LABORATORI NAZIONALI DI FRASCATI
SIS – Pubblicazioni

**LNF-03/17 (NT)**
**1 Ottobre 2003**

# TEST DI CONFIGURABILITA' E PRESTAZIONI DEL ROUTER JUNIPER

Franco Brasolin[1], Angelo Veloce[2]

*[1)]INFN-Sezione di Bologna V.le Berti-Pichat 6/2, I-40127 Bologna, Italy*
*[2)]INFN-Laboratori Nazionali di Frascati Via E. Fermi 40, I-00044 Frascati, Italy*

## Sommario

Questo documento illustra le modalità e i risultati dei test dei nuovi router Juniper della famiglia M5. Il lavoro si inserisce nelle attivita' del Netgroup, afferente alla Commissione Nazionale di Calcolo e Reti dell'INFN. L'obiettivo è verificare la configurabilità e le performance di questi apparati in previsione della sostituzione degli attuali router di accesso alla rete GARR.

## Abstract

This document shows procedures and tests of the new router Juniper of M5 family. This work is requested by the Netgroup belonging to the INFN National Commission of Network and Computing. The purpose is to verify how to set this Router and his performances. This is due to the future substitution of the INFN current Routers

# 1 INTRODUZIONE

L'infrastruttura della rete di accesso dell'INFN è basata su apparati di routing Cisco, che garantiscono la connettività IP dei diversi siti INFN alla rete GARR-B. Attualmente la rete sta evolvendo verso la nuova infrastruttura GARR-G, che realizza un backbone gibabit. L'accesso ai Giga-POP della futura rete IP sarà fornito dal GARR attraverso un insieme eterogeneo di apparati di rete, utilizzando prevalentemente router Cisco e Juniper.

Il Netgroup, in previsione del nuovo ambiente in cui andranno ad operare i Network Manager dell'INFN, ha ottenuto in prova due router Juniper della tipologia M5, che sono stati installati, configurati e testati in produzione presso la Sezione INFN di Bologna ed i Laboratori Nazionali di Frascati.

I router M5, pur essendo i modelli base del marchio Juniper, garantiscono ottime prestazioni e sono limitati solo nel numero di Physical Interface Cards che possono essere installate (al massimo quattro) e nel numero di alimentatori (uno, che non può quindi essere ridondato).

Il presente documento descrive la procedura di configurazione di un router Juniper adattata alle esigenze dei siti INFN e le prove di performance eseguite tra le sedi di LNF e Bologna. Particolare attenzione è stata rivolta al miglioramento delle prestazioni, ottenibile grazie all'implementazione in ASIC caratteristica dei router Juniper, verificato sia in ambiente di test (simulando un traffico molto elevato con Netperf e impostando Access-List particolarmente "pesanti") che durante un periodo di utilizzo in produzione come border router delle sedi di LNF e Bologna.

## 2 CARATTERISTICHE HARDWARE DEI ROUTER JUNIPER

Questi apparati di rete prevedono una divisione tra la componente di controllo denominata *Routing Engine* e la componente di forwarding denominata *Packet Forwarding Engine* (Fig. 1).

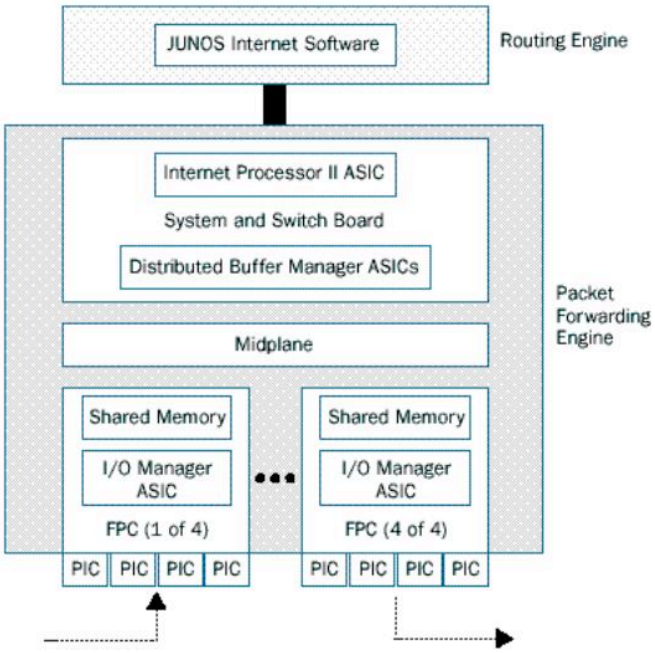



**Fig. 1**: Architettura Hardware

### 2.1 Routing Engine

Ha il compito di elaborare e mantenere la *Routing Table*, il *Network Management* attraverso il quale, ad esempio, i log sono inviati ad un server centrale.

### 2.2 Packet Forwarding Engine

L'unità è composta da una serie di *ASIC* che eseguono il forwarding dei pacchetti *IP* in hardware, in base alla *Routing Table* elaborata dalla *Routing Engine*. Tra i principali servizi offerti in *ASIC* a *wire-rate* ci sono:

- Advanced Packet Filtering (Access Control Lists), filtraggio dei pacchetti IP;
- Rate Limiting, limitazione di banda per tipologie di traffico;
- Packet Counting, conteggio di pacchetti;
- Sampling, campionamento di pacchetti IP;
- Port Mirroring, copiare il traffico del router su determinate porte.

È possibile applicare più servizi allo stesso flusso di traffico contemporaneamente; ad esempio eseguire un campionamento, limitare il traffico, incrementare contatori, eseguire un mirroring del traffico.

## 3 EQUIPAGGIAMENTO DEI ROUTER

### 3.1 Frascati:

Router Juniper M5 (Fig. 2):
- PIC 0: una interfaccia 1000 Base SX.
- PIC 1: quattro interfacce 100 Base TX.
- PIC 2: due interfacce ATM OC-3.
- PIC 3: una interfaccia VPN Tunnel.

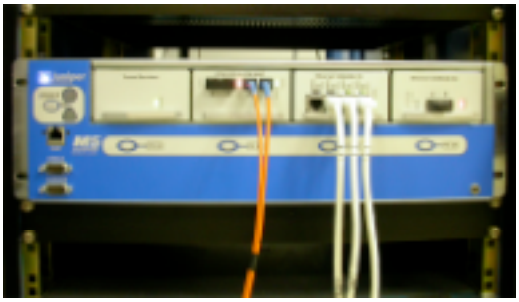


**Fig. 2**: Router Juniper M5 di Frascati

### 3.2 Bologna:

Router Juniper M5:
- PIC 0: quattro interfacce 100 Base TX.
- PIC 1: due interfacce ATM OC-3.

## 4 SOFTWARE

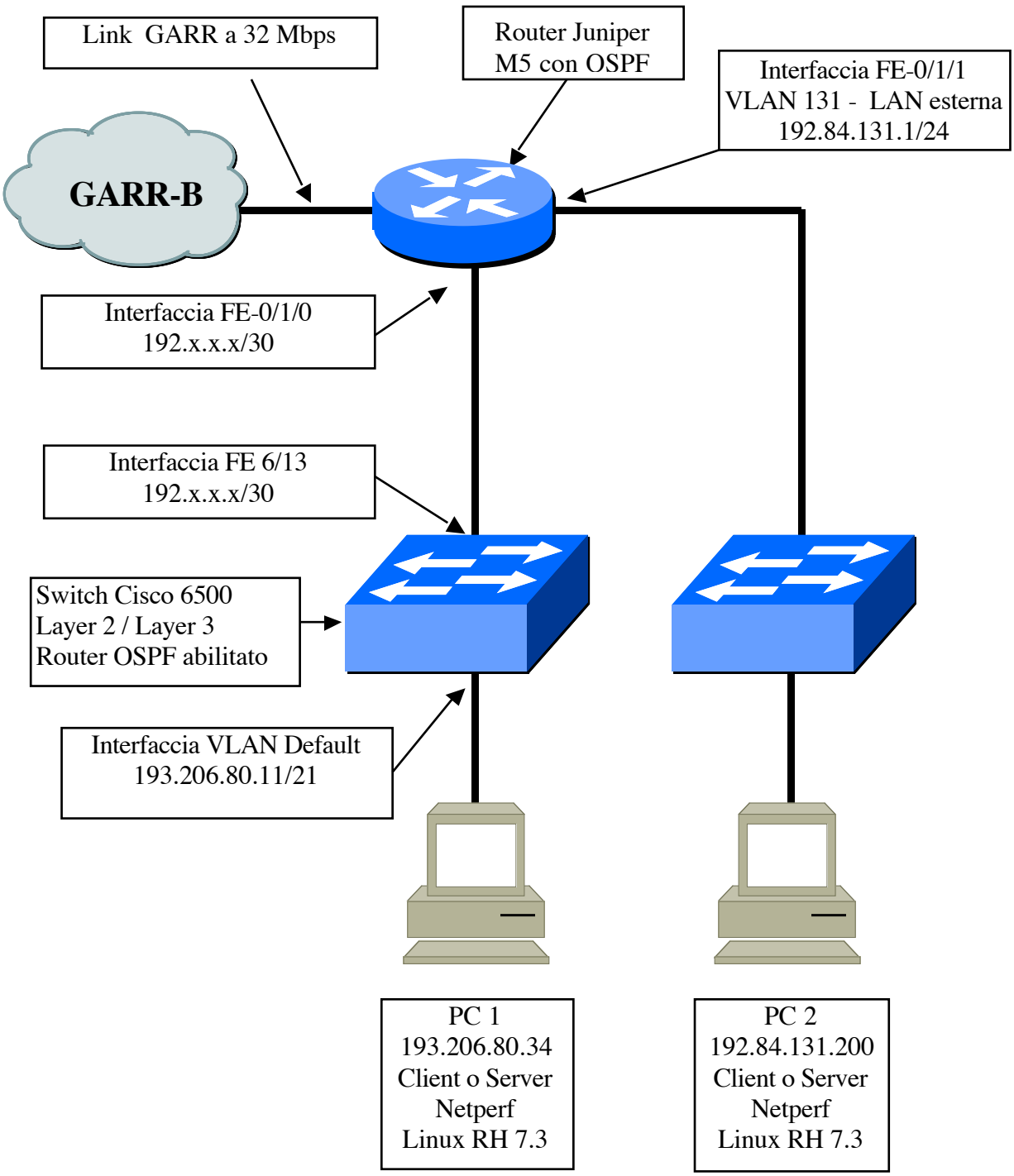
Per eseguire i test di performance è stato utilizzato il software Open-Source *Netperf*, versione 2.1 su piattaforma Linux. Ai LNF, inoltre, per verificare la configurazione del Port Mirroring, è stato utilizzato lo sniffer di rete EtherPeek della WildPackets per Windows 2000.

Il software dei router Juniper è basato su Unix BSD; le versioni utilizzate sono:

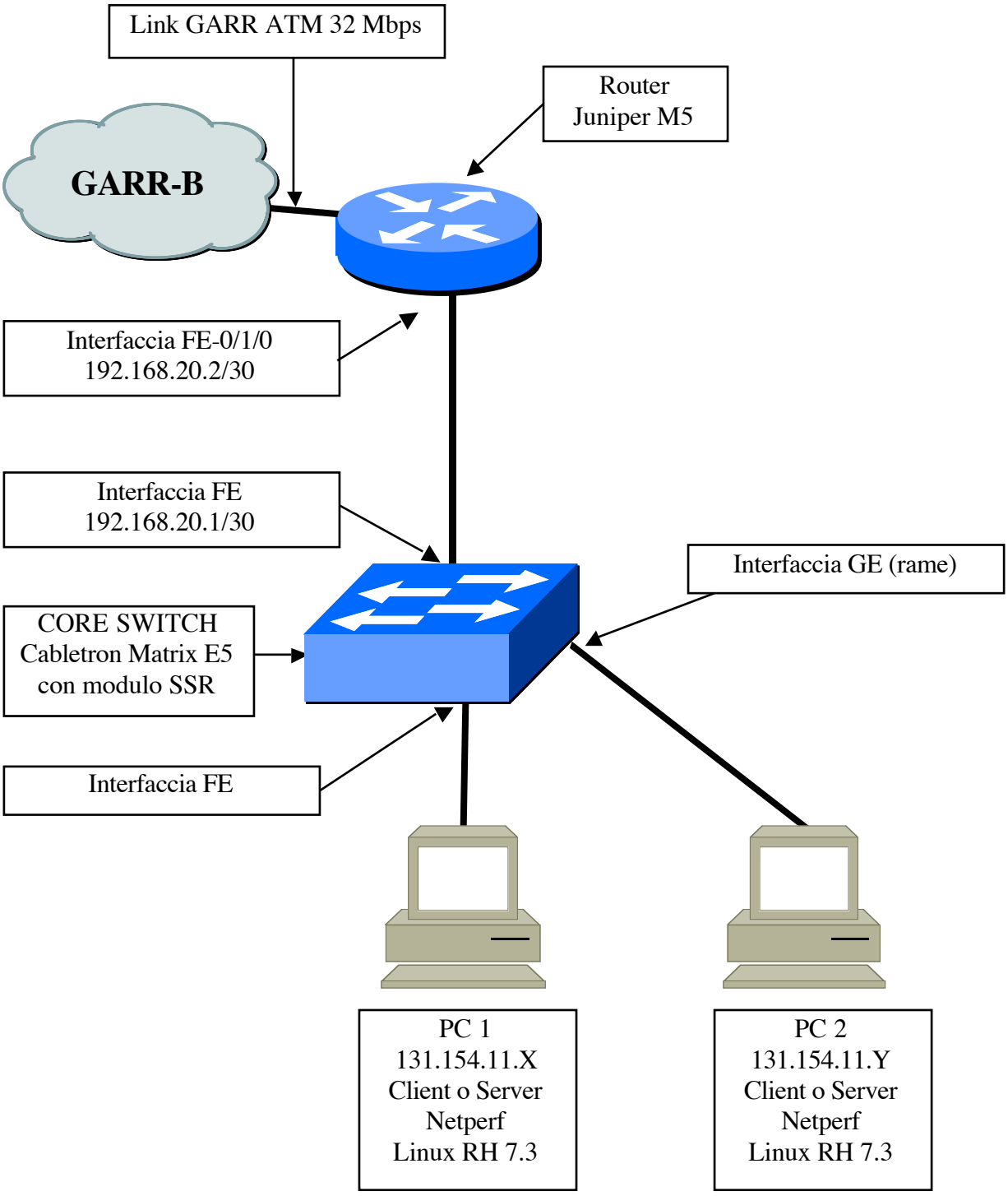
*LNF: JunOS 5.5*
*Bologna: JunOS 5.3*

# 5 INFRASTRUTTURA DI TEST

## 5.1 Frascati



### 5.2 Bologna


Link GARR ATM 32 Mbps
Router
Juniper M5
GARR-B
Interfaccia FE-0/1/0
192.168.20.2/30
Interfaccia FE
192.168.20.1/30
Interfaccia GE (rame)
CORE SWITCH
Cabletron Matrix E5
con modulo SSR
Interfaccia FE
PC 1
131.154.11.X
Client o Server
Netperf
Linux RH 7.3
PC 2
131.154.11.Y
Client o Server
Netperf
Linux RH 7.3

# 6 PARAMETRI MONITORATI DURANTE IL TEST

L'obiettivo dei test di performance era verificare l'effettivo forwarding in *ASIC* del traffico e monitorare il carico della CPU, simulando elevati flussi di traffico TCP e UDP con *Netperf*.

I router sono stati configurati con le tradizionali politiche di filtering tipiche delle sedi INFN (circa 70 righe di ACL a Bologna e 200 ai LNF; definite come "*termini"* nel linguaggio JunOS). L'entry relativa al permesso di passaggio al software *Netperf* sulla porta 12865 è stata collocata in modo da mettere in crisi il più possibile il firewall definito nel router. Nel caso specifico le CPU da monitorare erano due: Routing Engine (RE) e Packet Forwarding Engine (PFE).

## 6.1 Routing Engine

È possibile visualizzare lo stato della CPU di questa unità con il comando:

```
Juniper> show chassis routing-engine

Routing Engine status:
    Temperature                 22 degrees C / 71 degrees F
    DRAM                       256 MB
    Memory utilization          19 percent
    CPU utilization:
      User                       0 percent
      Background                 0 percent
      Kernel                     0 percent
      Interrupt                  0 percent
      Idle                      99 percent
    Model                        RE-2.0
    Serial ID                    d10000078c0adf01
    Start time                   2003-05-13 13:36:29 UTC
    Uptime                       22 days, 1 hour, 42 minutes, 4seconds
    Load averages:               1 minute   5 minute  15 minute
                                     0.01       0.02       0.00
```

Durante i test è stata monitorata, attraverso il protocollo SNMP, la MIB relativa alla *CPU utilization* della Routing Engine.

## 6.2 Packet Forwarding Engine

Per capire quali sono i parametri da monitorare in questi apparati è utile descriverne le parti fondamentali. La Packet Forwarding Engine è composta da:

- Midplane: ha il compito di distribuire l'alimentazione, di trasferire dati e segnali tra le diverse componenti;
- Physical Interface Cards (PICs): sono moduli che permettono la connettività alle diverse interfacce fisiche. Ad esempio: Fast Ethernet in fibra ottica, Gigabit Ethernet in fibra ottica, OC-12/STM-4, ecc;
- Flexible PIC Concentrators (FPCs): questa unità è semplicemente il contenitore delle PICs sopra indicate. Nel router M5 è possibile installare al massimo 4 PICs mentre nel router M10 possono essere installate fino ad otto PICs;
- Forwarding Engine Board (FEB): esegue il filtering e l'instradamento per tutti i

pacchetti in base alla tabella di forwarding, frutto dell'elaborazione della Routing Engine.

Quindi, monitorando lo stato del Forwarding Engine Board (FEB) è possibile avere una misura del carico del Packet Forwarding Engine:

```
Juniper> show chassis feb

FEB status:
  Temperature                 22 degrees C / 71 degrees F
  CPU utilization              2 percent
  Interrupt utilization       11 percent
  Heap utilization            17 percent
  Buffer utilization          49 percent
  Total CPU DRAM              64 MB
  Internet Processor II          Version 1, Foundry IBM, Part number 9
  Start time:                    2003-05-13 13:38:08 UTC
  Uptime:                        22 days, 1 hour, 40 minutes, 34 seconds
```

Durante i test sono state monitorate, attraverso il protocollo SNMP, le MIB relative ai seguenti parametri:

- *CPU Utilization*: percentuale di CPU utilizzata nel processore della FEB;
- *Interrupt Utilization*: percentuale di interrupts utilizzati;
- *Heap Utilization*: percentuale di memoria dinamica usata nel processore della FEB;
- *Buffer Utilization*, percentuale di spazio buffer usato nel processore FEB per il buffering dei messaggi interni.

### 6.3 Produzione grafici

Per ottenere i grafici dell'andamento dell'occupazione di CPU dei due router Juniper durante i test è stato utilizzato un PC linux RedHat 7.3 con:

- snmpwalk (rpm: ucd-snmp-utils-4.2.5-7.73.0)
- rrdtools (rpm: rrdtool-1.0.39-1.7.2)

Da *crontab* uno script interroga via *snmpwalk* i due router utilizzando le apposite MIB. I dati ottenuti vengono memorizzati in un database in formato *RRD* e utilizzati per creare i grafici tramite l'applicativo *rrdtool*.

## 7 TEST ESEGUITI CON NETPERF

I test sono stati eseguiti tra la Sezione INFN di Bologna e i Laboratori Nazionali di Frascati. Sono state utilizzate due stream contemporanee che hanno coinvolto quattro elaboratori (PC Linux RedHat 7.3): un Server Netperf e un Client Netperf sia a Bologna che a Frascati.

### 7.1 Stream TCP

Sono stati eseguiti dei test di stream TCP con durata 3 minuti, 6 minuti e 9 minuti. Durante queste prove sono state monitorati i carichi di CPU del Routing Engine e del Packet Forwarding Engine.

### 7.2 Stream UDP

Le misure successive sono state stream UDP con diverse dimensioni di pacchetti pari a:

- 1024 Bytes
- 2048 Bytes
- 10240 Bytes
- 20480 Bytes
- 50000 Bytes
- 60000 Bytes

**7.3 Grafico dei parametri relativi alle CPU monitorate sul router di LNF (Fig. 3) durante le simulazioni di traffico precedentemente indicate e relativo andamento del traffico sull'interfaccia GARR (Fig. 4):**

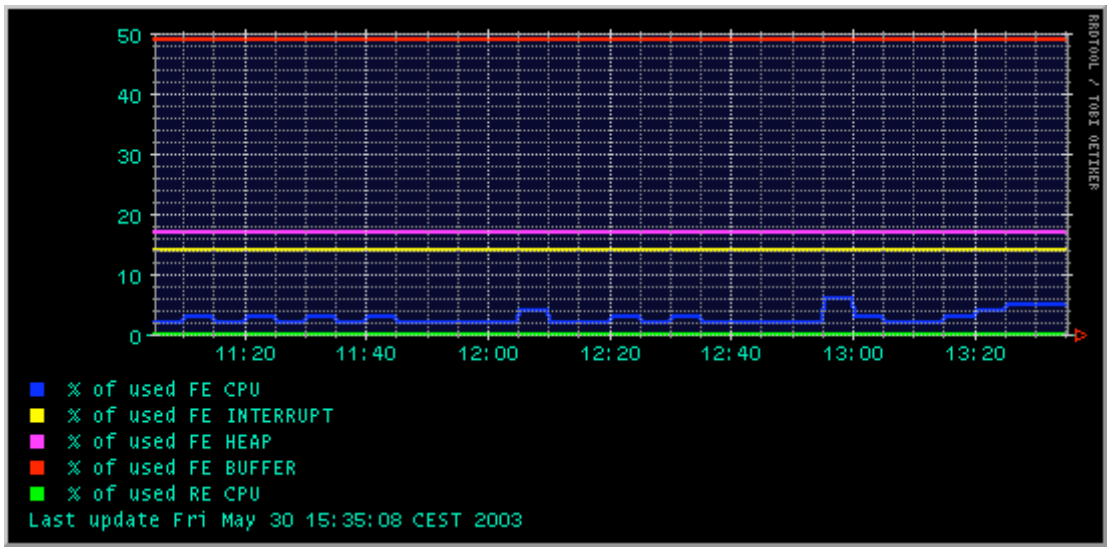



**Fig.3**: Monitoraggio CPU router Frascati

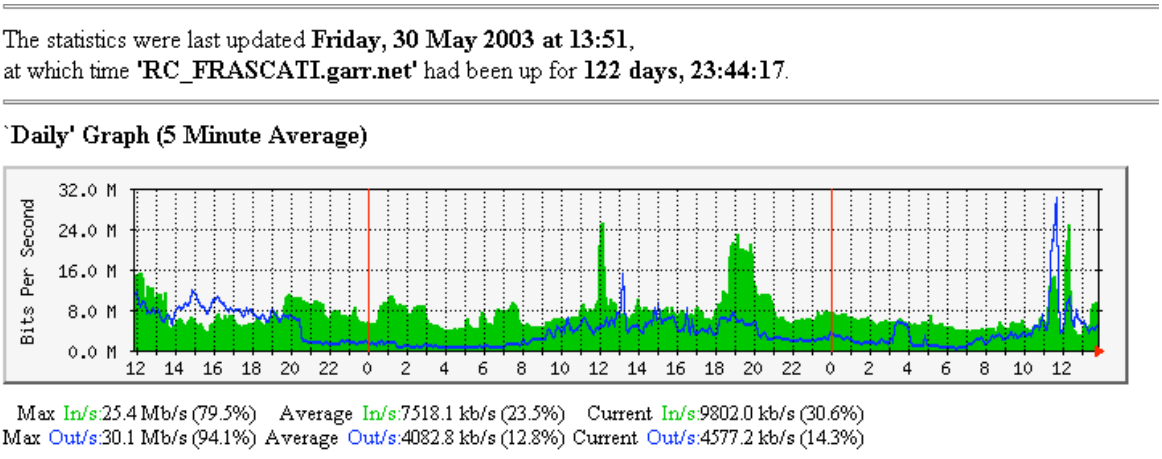



**Fig.4**: Traffico con il POP di Frascati

**7.4 Grafico dei parametri relativi alle CPU monitorate sul router di Bologna (Fig. 5) durante le simulazioni di traffico precedentemente indicate e relativo andamento del traffico sull'interfaccia GARR (Fig. 6):**

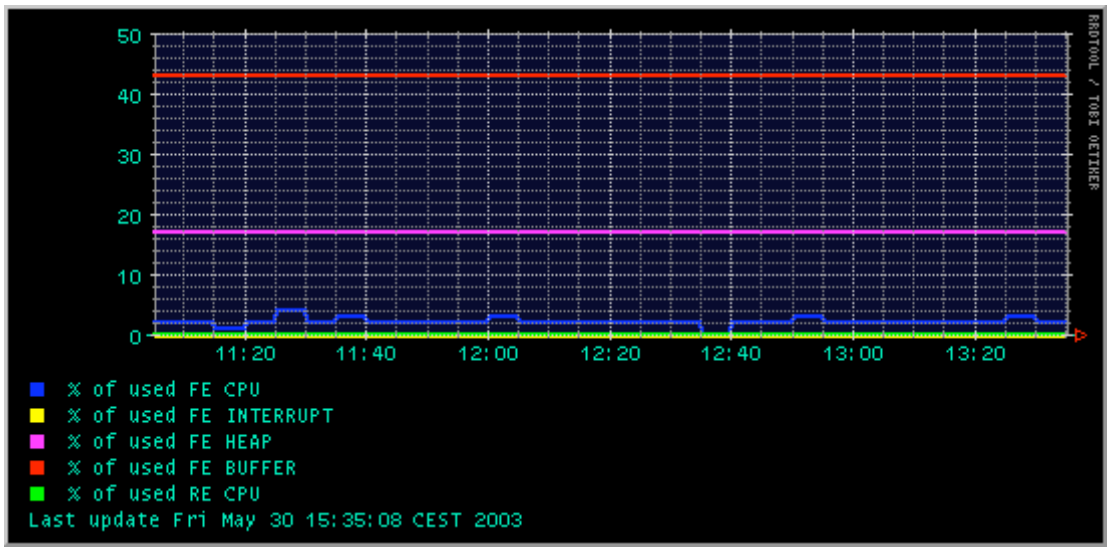



**Fig.5**: Monitoraggio CPU router Bologna

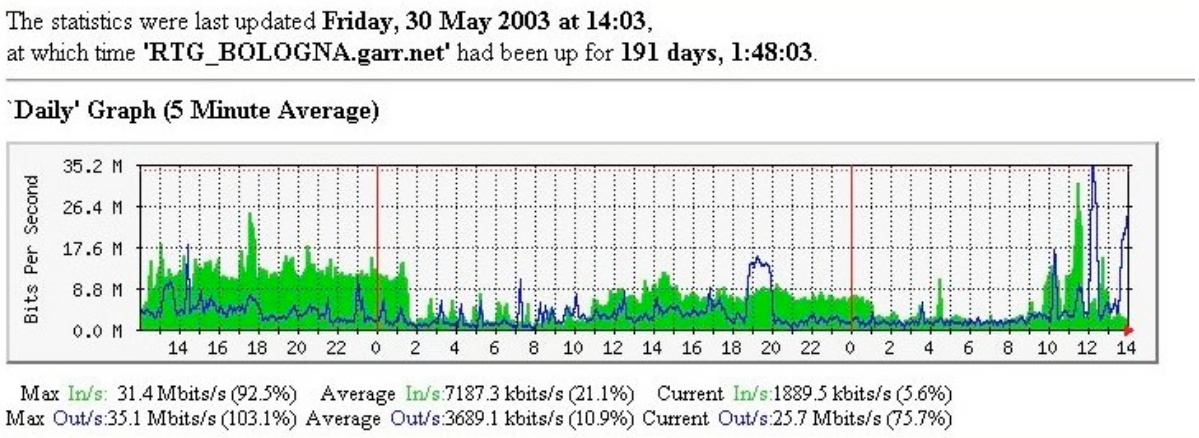



**Fig.6**: Traffico con il POP di Bologna

# 8 RISULTATI DEI TEST

Si può facilmente rilevare dai grafici sopra riportati che durante le simulazioni i due router non hanno risentito delle stream TCP e UDP, confermando quindi l'effettiva attività in ASIC nel forwarding di pacchetti IP. Questo di fatto garantisce ai router Juniper di poter mantenere la massima funzionalità avendo le CPU libere per altre attività come routing, logging, ecc, indipendentemente dal traffico in transito.

# 9 FUNZIONALITÀ EVOLUTE OFFERTE IN ASIC

## 9.1 Sampling

Il *Sampling* permette di esaminare e memorizzare una percentuale di pacchetti che rispondono a determinati requisiti. Questa funzionalità è stata provata sul router dei LNF, campionando i pacchetti che violano le regole di spoofing.

```
forwarding-options {
    sampling {
        input {
            /* rate 1 = 100% traffico */
            family inet {
                rate 1;
            }
        }
        output {
            file filename Spoofing size 2m world-readable;
        }
    }

firewall {
    /* Filtro per anti-spoofing - 12-05-2003 */
    filter INFN-Out {
        term AntiSpoofing {
            from {
                source-address {
                    193.206.80.0/21;
                    192.135.25.0/24;
                    192.135.26.0/24;
                    192.84.128.0/22;
                    193.206.131.58/32;
                    193.206.136.206/32;
                }
            }
            then {
                count Conta-Traffico-OK;
                accept;
            }
        }
        term Default {
            then {
                count Conta-Accessi-Negati;
                log;
                sample;
                discard;
            }
        }
```

Il file prodotto da questo campionamento, si dimostra utile perché ci fornisce in maniera immediata l'elenco degli host che hanno violato l'*antispoofing*:

```
# Jun 19 09:02:35
#           Dest             Src  Dest   Src Proto  TOS   Pkt  Intf    IP   TCP
#           addr            addr  port  port               len   num  frag flags

  192.84.134.75 192.168.160.206  7003  7001    17  0x0    93     4   0x0   0x0
  141.108.3.252 192.168.160.206  7003  7001    17  0x0    60     4   0x0   0x0
    131.154.1.7 192.168.160.206  7003  7001    17  0x0    60     4   0x0   0x0
 192.84.128.121    216.12.72.38    80 10722     6  0x80   43     7   0x0   0x14
  192.84.128.30     80.15.220.4    80 26129     6  0x0    40     7   0x0   0x4
  192.84.128.30     80.15.220.4    80 26399     6  0x0    40     7   0x0   0x4
 192.84.128.128  211.203.90.164    80  3531     6  0x80  1460    7   0x4000   0x10
 192.84.128.215   213.88.133.65    80 33519     6  0x0    40     7   0x0   0x14
 192.84.128.225  211.58.236.190    80 24033     6  0x80   40     7   0x0   0x4
 192.84.128.108  211.203.90.164    80  3451     6  0x80 1460     7   0x4000   0x10
 192.84.128.239  65.202.139.145    80  4636     6  0x80   40     7   0x0   0x4
 192.84.128.239  65.202.139.145    80  4636     6  0x80   40     7   0x0   0x4
 192.84.128.239  65.202.139.145    80  4636     6  0x80   40     7   0x0   0x4
  192.84.128.73   213.150.58.51    80  3363     6  0x80   40     7   0x0   0x4
  192.84.128.73   213.150.58.51    80  3363     6  0x80   40     7   0x0   0x4
 192.84.128.152     12.17.11.87    80 35012     6  0x80   43     7   0x0   0x14
  192.84.128.20  209.181.92.204    80  1586     6  0x80   43     7   0x0   0x14
  192.84.128.37   200.99.80.130    80 35197     6  0x80   40     7   0x0   0x4
  192.84.128.37   200.99.80.130    80 35197     6  0x80   40     7   0x0   0x4
 192.84.128.109 211.203.146.254    80  3866     6  0x80  1500    7   0x4000   0x10
 192.84.128.109 211.203.146.254    80  3866     6  0x80   40     7   0x0   0x4
 192.84.128.109 211.203.146.254    80  3866     6  0x80   40     7   0x0   0x4
 192.84.128.109 211.203.146.254    80  3866     6  0x80   40     7   0x0   0x4
```

## 9.2 Rate Limiting

Con il rate limiting è possibile limitare la quantità di traffico e il rate di picco (*burst size*) per determinate categorie di traffico. In particolare, con il termine *Bandwidth-limit* si indica il valor medio dei bit per secondo permessi, mentre con il termine *burst-size-limit* si indicano i picchi, espressi in byte, permessi oltre la *Bandwidth-limit* per limitati intervalli di tempo. Si utilizza l'algoritmo *token-bucket* che applica un limite sulla banda media mentre permette bursts fino ad uno specifico valore.

Impostando questa funzionalità non abbiamo notato diminuzioni di capacità di forwarding sul router, rispettando quindi i prerequisiti di operatività in ASIC.

## 9.3 Rate Limiting ICMP

Un tipo di attacco molto diffuso, il *ping storming*, può essere limitato impostando il rate limiting sul protocollo ICMP.

```
firewall {
    policer LimitaICMP {
        if-exceeding {
            bandwidth-limit 200k;
            burst-size-limit 50k;
        }
        then discard;
    }
```

Con questo termine, in caso di traffico superiore ai 200 Kbps e con burst superiori di 50 KB, i pacchetti vengono scartati. Una volta stabilita la policy di rate limiting ICMP, questa viene applicata al termine corrispondente nell'access list.

```
term T46 {
     from {
        protocol icmp;
          }
     then {
        policer LimitaICMP;
        log;
        accept;
          }
    }
```

### 9.4 Rate Limiting del traffico Peer to Peer

Limitare questo tipo di traffico è importante per evitare che la banda a disposizione di una sezione o laboratorio INFN sia utilizzata in modo illecito.

```
firewall {

    policer LimitaPeer-to-Peer {
        if-exceeding {
            bandwidth-limit 2m;
            burst-size-limit 64k;
        }
        then discard;
    }
```

Questo termine è stato applicato sul filtro del traffico in uscita.

```
term GnutellaOUT {
       from {
           port [ 6346 6347 6348 1214 6699 7730 41000-41900 4661 4662 ];
            }
       then {
                policer LimitaPeer-to-Peer;
                syslog;
                accept;
            }
        }
```

Molto apprezzata è la possibilità di usare il termine port che permette di catturare pacchetti che usano il protocollo TCP o UDP e che hanno indifferentemente un source o destination port indicati nella lista. I principali programmi filtrati sono stati:

- Gnutella sulle porte 6346, 6347, 6348;
- Morpheus sulla porta 1214;
- WinMX sulle porte 6699, 7730;
- Audiogalaxy nel range di porte 41000-41900;
- Edonkey sulle porte 4661 4662;

Da questa attività di limitazione del traffico *peer-to-peer* sono stati riscontrati benefici, nell'ordine dei 2 Mbps, nella banda utilizzata ai LNF. Rimane comunque il pericolo che gli utenti modifichino le porte di default utilizzate da questi programmi, vanificando i tentativi di limitazione.

### 9.5 Port Mirroring

Questo servizio offre la possibilità di copiare una serie di pacchetti su una porta di monitoring dove è attestato un analizzatore di traffico. È possibile indirizzare flussi di traffico specifici sui quali eseguire il monitoring.

Nel nostro test è utilizzata questa funzionalità per copiare tutto il traffico in uscita dai LNF sulla porta `fe`-0/1/2, monitorando tale traffico con lo sniffer di rete EtherPeek

```
forwarding-options {
    sampling {
        input {
            /* rate 1 = 100% traffico */
            family inet {
                rate 1;
            }
        }
        output {
            port-mirroring {
                interface fe-0/1/2.0;
                next-hop 1.1.1.1;
            }
        }
    }
}

interfaces {
fe-0/1/2 {
        unit 0 {
            family inet {
                address 1.1.1.2/30 {
                    arp 1.1.1.1 mac 00:01:02:f3:62:e3;
                }
            }
        }
    }
```

### 9.6 Packet Counting

Questa funzionalità risulta molto utile per produrre statistiche di traffico. È stato applicato il *Packet Counting* sul filtro del traffico in uscita dai LNF come di seguito indicato:

```
/* Filtro per anti-spoofing - 12-05-2003 */
    filter INFN-Out {
        term GnutellaOUT {
            from {
                port [ 6346 6347 6348 1214 6699 7730 41000-41900 4662 ];
            }
            then {
                count Conta-traffico-Peer-to-Peer;
                policer LimitaPeer-to-Peer;
                syslog;
                accept;
            }
        }
        term AntiSpoofing {
            from {
                source-address {
                    193.206.80.0/21;
                    192.135.25.0/24;
                    192.135.26.0/24;
                    192.84.128.0/22;
                    193.206.131.58/32;
                    193.206.136.206/32;
                }
            }
            then {
                count Conta-Traffico-OK;
                sample;
                accept;
            }
        }
        term Default {
            then {
                count Conta-Accessi-Negati;
                log;
                syslog;
                discard;
            }
        }
    }
```

Con il seguente comando è possibile visualizzare lo stato dei contatori sopra predisposti:

```
Juniper> show firewall filter INFN-Out
Filter: INFN-Out
Counters:
Name                                                Bytes              Packets
Conta-traffico-Peer-to-Peer                   xxxxxxxxxxxx            xxxxxxxxx
Conta-Accessi-Negati                             xxxxxxxx               xxxxxx
Conta-Traffico-OK                             xxxxxxxxxxxx            xxxxxxxxx
Policers:
Name                                                Packets
LimitaPeer-to-Peer-GnutellaOUT                   xxxxxxxx
```

## 10 TRADUTTORE i2j IOS-JunOS

Per quanti debbano sostituire un router *Cisco* con un router *Juniper*, è disponibile un comodo software di traduzione da *IOS* a *JunOS*: *i2j*, fornito da Juniper (http://i2j.juniper.net).

Utilizza un'interfaccia Web (servono username/password da richiedere a Juniper Italia) e può tradurre singole righe di comando o anche l'intero file di configurazione *Cisco*. Nei test effettuati si è rivelato molto utile e notevolmente preciso. È comunque fortemente consigliabile verificare attentamente il risultato della traduzione prima di utilizzarla.

## 11 CONCLUSIONI

Nel corso dei test è stato possibile provare in maniera esaustiva e in produzione le caratteristiche di questi router, in particolare per quanto riguarda le necessità di una tipica Sezione o Laboratorio INFN. La possibilità di effettuare in *ASIC*, quindi in hardware, la parte più pesante del lavoro (*Packet Filtering, Rate Limiting, Packet Counting, Sampling*) permette a queste macchine di lavorare con la *CPU* alleggerita e di non avere problemi di sovraccarico, dovuto al traffico o ad attacchi dall'esterno, che impedirebbero altrimenti qualsiasi forma di attività di controllo e management dell'apparato nei momenti più critici.

Il software di queste macchine è di fatto un sistema operativo Unix *BSD*, ottimizzato per rispondere alle esigenze di rete. Questo permette a chi vuole cimentarsi, e ne abbia la necessità, di poter operare direttamente a livello di sistema operativo: esaminare i log, copiare file from/to host remoti o qualsiasi altra operazione *unix-like* diventa possibile (operazioni comunque possibili anche lavorando al livello superiore, con interfaccia JunOS). Durante i nostri test per esempio è stato compilato e installato un demone SSHD per potersi connettere in modo sicuro al router da remoto.

La parte relativa alla configurazione dei router si è dimostrata particolarmente semplice: si basa su una struttura ad albero attraverso cui è possibile accedere ai vari sotto-livelli per esaminare e/o modificare i vari parametri. Le dieci configurazioni precedenti vengono sempre salvate ed è possibile ripristinarle velocemente, sia in caso di test di nuove funzionalità che di problemi sulle nuove versioni. Per esempio, è possibile provare una nuova configurazione per un intervallo di tempo definito, dopodiché il router ripristina automaticamente la versione precedente, evitando eventualmente di creare disservizi.

Juniper fornisce inoltre ottima documentazione, tra cui un manuale in italiano con le istruzioni fondamentali per installare e configurare da zero queste macchine.

Nel complesso quindi la nostra opinione è senz'altro positiva: le prestazioni di questi router nelle sedi coinvolte nel test sono state ottime; restano però da valutare l'affidabilità hardware, la qualità e velocità dell'assistenza e, non ultime, le offerte economiche che si potranno ottenere per queste macchine.

# A APPENDICE

Vengono qui riportati un esempio di ACL, alcuni comandi utili, le configurazioni dei due router di Frascati e Bologna, le *MIB* per interrogare i parametri di occupazione CPU dei router Juniper e la lista degli acronimi.

## A.1 Alcune annotazioni importanti riguardanti le ACL

- Le ACL sono riportate a titolo di esempio, per avere una indicazione della sintassi da utilizzare. Anche se possono corrispondere a quelle di una tipica Sezione o Laboratorio INFN, non si vuole in questo documento fornire un elenco completo ed esaustivo dei filtri da implementare per avere un buon livello di sicurezza.
- Si ricorda che anche nei router *Juniper*, come nei router *Cisco*, le ACL vengono interpretate nell'ordine in cui sono scritte. Il controllo del pacchetto finisce al primo *match* che viene soddisfatto, ignorando le righe successive.
- I *termini* (regole) che compongono le ACL hanno un nome che può essere per esempio: *T1, T2 T3* ecc.: questa numerazione non ha nessuna valenza per stabilire l'ordine con cui vengono interpretate; vale solo l'ordine sequenziale con cui sono scritti. I termini possono essere spostati di posizione più in alto o più in basso, secondo le esigenze. Ad ogni *termine* si può applicare l'opzione *"log"* per loggare l'evento sul router e/o l'opzione *"syslog"* per inviare l'informazione ad un syslog server remoto.
- Per evitare interruzioni nei servizi di rete, è consigliabile implementare le ACL un po' per volta e non tutte contemporaneamente, controllando il logging e verificando con gli utenti eventuali malfunzionamenti.

## A.2 Semplicità di configurazione: un esempio di ACL

In questo paragrafo si vuole mettere in evidenza la facilità di management delle Access-List, utilizzando come esempio il worm Blaster che utilizza le porte TCP 135, 139, 445, 593 e UDP 69, 135, 137, 138, 4444.

È stato configurato il *sampling* delle connessioni aperte dai nodi interni ai Laboratori Nazionali di Frascati utilizzando le porte sopra menzionate, per ottenere la lista dei nodi che probabilmente sono stati infettati dal worm Blaster.

Non viene riportata la configurazione completa del *sampling* da eseguire sulle *forwarding-options* perché già precedentemente spiegata (par. 9.1):

```
[edit firewall filter INFN-Out term W32.Blaster]
Juniper> show
from {
    protocol [ tcp udp ];
    source-port [ 135 139 445 593 137 138 69 4444 ];
}
then {
    sample;
    accept;
}
```

Questo termine controlla il traffico in uscita e viene posto alla fine del filtro INFN-Out. Per posizionarlo all'interno dei termini che compongono la nostra ACL usiamo il seguente comando:

```
[edit firewall filter INFN-Out]
Juniper> insert term W32.Blaster before term AntiSpoofing
```

Il risultato è abbastanza intuitivo e comporta il posizionamento del termine W32.Blaster prima del termine AntiSpoofing. Il nuovo filtro INFN-Out risulta quindi:

[edit firewall filter INFN-Out]

```
juniper> show

term cert_cisco {
    from {
        protocol [ 53 55 77 103 ];
    }
    then {
        count vulnerabilita_cisco;
        discard;
    }
}
term GnutellaOUT {
    from {
        port [ 6346 6347 6348 1214 6699 7730 41000-41900 4662 ];
    }
    then {
        count Conta-traffico-Peer-to-Peer;
        policer LimitaPeer-to-Peer;
        syslog;
        accept;
    }
}
term PCATEMMI {
    from {
        source-address {
            193.x.x.x/32;
        }
    }
    then discard;
}
term W32.Blaster {
    from {
        protocol [ tcp udp ];
        source-port [ 135 139 445 593 137 138 69 4444 ];
    }
    then {
        sample;
        accept;
    }
}
term AntiSpoofing {
    from {
        source-address {
            x.x.x.x/21;
            x.x.x.0/24;
            x.x.x.0/24;
            x.x.x.0/22;
             ……
        }
    }

    then {
        count Conta-Traffico-OK;
        sample;
        accept;
    }
}
term Default {
    then {
        count Conta-Accessi-Negati;
        log;
        syslog;
        discard;
    }
}
```

## A.3 Comandi utili: commit

Un comando molto comodo è il *commit*, che può essere anche condizionato:

```
Juniper> commit confirmed
commit confirmed will be automatically rolled back in 10 minutes unless
confirmed
```

In questo modo la nuova versione caricata deve essere confermata entro dieci minuti, altrimenti il sistema ricarica la precedente. Questo permette di rimettere in funzione il router nel caso la nuova configurazione contenga errori gravi che ne pregiudicano il buon funzionamento.

Il router Juniper è in grado di mantenere le ultime dieci configurazioni: in particolare il file di configurazione in esercizio è denominato *juniper.conf*. Gli ultimi tre precedentemente utilizzati sono: *juniper.conf.1, juniper.conf.2, juniper.conf.3* e sono mantenuti nella *flash memory* del router, localizzata nella directory */config*.

Le configurazioni utilizzate precedentemente (*juniper.conf.4* - *juniper.conf.9*) sono memorizzate nell'hard disk del router, nella directory */var/db/config*.

Una funzione molto utile è il *rollback* che permette di ripristinare una delle precedenti configurazioni:

```
Juniper> rollback ?
Possible completions:
  <[Enter]>            Execute this command
  <number>             Numeric argument
  0                    2003-09-10 08:57:49 UTC by veloce via cli
  1                    2003-09-10 08:57:25 UTC by veloce via cli commit
confirmed
  2                    2003-09-10 08:42:07 UTC by veloce via cli
  3                    2003-09-08 14:11:31 UTC by veloce via cli
  4                    2003-09-08 14:11:12 UTC by veloce via cli
  5                    2003-09-04 15:40:12 UTC by veloce via cli
  6                    2003-09-04 09:57:35 UTC by veloce via cli
  7                    2003-09-03 09:50:57 UTC by veloce via cli
  8                    2003-09-03 09:48:15 UTC by veloce via cli
  9                    2003-09-02 08:18:34 UTC by veloce via cli
  |                    Pipe through a command
[edit]
```

Una volta ricaricata una delle precedenti configurazioni, questa dovrà essere confermata con il comand *commit*.

## A.4 Altri comandi utili

- Halt del sistema:

  ```
  request system halt
  ```

- Reboot del sistema:

  ```
  request system reboot
  ```

- Entrare in shell (per terminare exit):

  ```
  start shell
  ```

- Salvare il file di configurazione su host remoto via ssh o ftp:
  - entrare in modalità "conf"
  - assicurarsi di essere al "top level" (altrimenti verrà salvata la configurazione parziale del livello in cui si è posizionati).
    - SSH:

      ```
      save scp://user@host/directory/subdirectory/file.conf
      ```

    - FTP:

      ```
      save ftp://user@host/directory/subdirectory/file.conf
      ```

## A.5 Configurazione router LNF

```
version 5.5R2.3;
system {
    host-name lnfgw;
    domain-name lnf.infn.it;
    ports {
        console type vt100;
    }
    inactive: root-authentication {
        encrypted-password "xxxxxxxxxxxxxxxxxxxxxxxxx";
    }
    name-server {
        193.x.x.x;
        193.x.x.x;
    }
    login {                    # Blocco dove sono indicati gli utenti che
                               # hanno accesso al router Juniper
        user infn1 {
            uid x;
            class read-only;
            authentication {
                encrypted-password "xxxxxxxxxxxxxxxxxxxxxxxxxx";
            }
        }
        user infn2 {
            uid x;
            class super-user;
            authentication {
                encrypted-password "xxxxxxxxxxxxxxxxxxxxxxxxxxx";
            }
        }
        user infn3 {
            uid x;
            class superuser;
            authentication {
                encrypted-password "xxxxxxxxxxxxxxxxxxxxxxxxxxx";
            }
        }
    }
    services {                   # Tipologie di accessi agli
        ftp;                     # utenti sopra indicati
        ssh;
        telnet;
    }
    syslog {                     # Configurazione del logserver
        host 193.x.x.x {
            any error;
            firewall any;
            pfe notice;
            facility-override local7;
        }
        file messages {
            any notice;
            authorization info;
        }
    }
}
```

```
chassis {
    alarm {
        management-ethernet {
            link-down ignore;
        }
    }
}
interfaces {                    # Collegamento switch centrale layer 2 / 3
    fe-0/1/0 {
        description "Link verso SWCALC1";
        enable;
        no-keepalives;
        unit 0 {
            family inet {
                filter {
                    output 105;
                }
                address 192.x.x.x/30;
            }
        }
    }
    fe-0/1/1 {                          # Interfaccia che gestisce
                                        # VLAN degli ospiti
        description "LAN Esterna";
        unit 0 {
            family inet {
                address x.x.x.x/24 {
                    preferred;
                }
                address x.x.x.x/24;
            }
        }
    }
    fe-0/1/2 {          # Porta dello switch sulla quale viene eseguito
                        # il mirroring di tutto il traffico
        description "Porta di Mirroring";
        unit 0 {
            family inet {
                address 1.1.1.2/30 {
                    arp 1.1.1.1 mac 00:01:02:f3:62:e3;
                }
            }
        }
    }
    at-0/2/0 {          # Configurazione del link ATM verso il GARR
        atm-options {
            vpi x{
                maximum-vcs 2045;
            }
            vpi x{
                maximum-vcs 2045;
            }
        }
        unit 4 {
            description "PVC 8.8M LNF-RM1-PonteRadio";
            encapsulation atm-snap;
            point-to-point;
            vci x.y;
            shaping {
                vbr peak 8800000 sustained 8800000 burst 1;
            }
            family inet {
                address 193.x.x.x/30;
            }
        }
```

```
        unit 5 {
            description "PVC 34M LNF-GARRB-Telecom";
            encapsulation atm-snap;
            point-to-point;
            vci x.y;
            shaping {
                vbr peak 35333000 sustained 35333000 burst 1;
            }
            family inet {
                filter {
                    input 103;
                    output INFN-Out;
                }
                address 193.x.x.x/30;
            }
        }
    }
    lo0 {
        unit 0 {
            family inet {
                filter {
                    inactive: input Accessi-router;
                }
                address x.x.x.x/32;
            }
        }
    }
}
forwarding-options {
    sampling {
        input {
            /* rate 1 = 100% traffico */
            family inet {
                rate 1;
            }
        }
        output {
            port-mirroring {
                interface fe-0/1/2.0;
                next-hop 1.1.1.1;
            }
        }
    }
    helpers {               # Inoltro richieste DHCP dalla VLAN degli
                            # ospiti verso le VLAN interne LNF
        bootp {
            server x.x.x.x;
        }
    }
}
snmp {                      # Configurazione SNMP
    community xxxx {
        authorization read-write;
    }
    community xxxx {
        authorization read-only;
    }
}
```

```
routing-options {           # configurazione route statica verso il GARR
    static {
        route 0.0.0.0/0 {
            next-hop x.x.x.x;
            retain;
        }
    }
}
protocols {                 # configurazione Routing OSPF verso
                            # i router interni ai LNF
    ospf {
        export ospf-redistributes;
        area 0.0.0.0 {
            authentication-type md5;
            interface fe-0/1/0.0 {
                authentication-key "xxxxxxxxxxxxxxxxxxxxxxxx" key-id xx;
            }
            interface fe-0/1/1.0 {
                passive;
            }
            interface at-0/2/0.5 {
                passive;
            }
            interface lo0.0 {
                passive;
            }
        }
    }
}
policy-options {            # Ridistribuzione della informazione
                            # di route statica in OSPF
    policy-statement ospf-redistributes {
        term Red-Static {
            from protocol static;
            then accept;
        }
    }
}
firewall {                  # Configurazione Rate Limiting
    policer LimitaICMP {
        if-exceeding {
            bandwidth-limit 200k;
            burst-size-limit 50k;
        }
        then discard;
    }
    policer LimitaPeer-to-Peer {
        if-exceeding {
            bandwidth-limit 2m;
            burst-size-limit 64k;
        }
        then discard;
    }
```

## Configurazione Access List LNF

```
/* Filtro per anti-spoofing - 12-05-2003 */
filter INFN-Out {
    term GnutellaOUT {     # Conto e limito il traffico peer-to-peer
        from {
            port [ 6346 6347 6348 1214 6699 7730 41000-41900 4662 ];
        }
        then {
            count Conta-traffico-Peer-to-Peer;
            policer LimitaPeer-to-Peer;
            syslog;
            accept;
        }
    }
    term AntiSpoofing {    # Autorizzo e conto il solo traffico
                           # delle network LNF
        from {
            source-address {
                x.x.x.x/21;
                x.x.x.x/24;
                ……
            }
        }
        then {
            count Conta-Traffico-OK;
            sample;
            accept;
        }
    }
    term Default {      # Blocco e conto il traffico non autorizzato
        then {
            count Conta-Accessi-Negati;
            log;
            syslog;
            discard;
        }
    }
}

filter Accessi-router {    # Filtro che permette l'accesso al router   #
                           # solo alle network LNF
    term Accessi-Ammessi {
        from {
            source-address {
                x.x.x.x/32;
                ……
            }
            protocol tcp;
            destination-port [ telnet ssh ];
        }
        then {
            syslog;
            accept;
        }
    }
    term Filtra-SSH-TELNET {
        from {
            protocol tcp;
            destination-port [ telnet ssh ];
        }
        then {
            count Conta-SSH-TELNET-Negati;
```

```
            syslog;
            discard;
        }
    }

    term Others {
        then accept;
    }
}

filter 103 {
    term Gnutella {          # Termine che "cattura" il traffico
                             # Peer-To-Peer per limitarlo
      from {
       port [ 6346 6347 6348 1214 6699 7730 41000-41900 4662 4661 ];
        }
        then {
            policer LimitaPeer-to-Peer;
            syslog;
            accept;
        }
    }

    }
    term T2 {                # Termine che permette il traffico gia'
                             # stabilito dai nodi interni
        from {
            destination-address {
                x.x.x.x/21;
                x.x.x.x/24;
                ……
            }
            protocol tcp;
            tcp-established;
        }
        then accept;
    }
    term BULL {          # Termine di accesso ai sistemisti BULL
                         # per l'informatizzazione amministrazione
        from {
            source-address {
                138.x.0.0/16;
            }
            destination-address {
                x.x.x.x/32;
                x.x.x.x/32;
            }
        }
        then {
            log;
            syslog;
            accept;
        }
    }
    term T4 {              # Termine di accesso al DNS primario
        from {
            destination-address {
                x.x.x.x/32;
            }
            protocol tcp;
            destination-port domain;
        }
        then {
```

```
        log;
        syslog;
        accept;
    }
}
term T5 {             # Termine di accesso al DNS primario
    from {
        destination-address {
            x.x.x.x/32;
        }
        protocol udp;
        destination-port domain;
    }
    then {
        log;
        syslog;
        accept;
    }
}
term T6 {                 # Termine di accesso al Server
                          # di posta secondario
    from {
        destination-address {
            x.x.x.x/32;
        }
        protocol tcp;
        destination-port smtp;
    }
    then {
        log;
        syslog;
        accept;
    }
}
term T7 {              # Termine di accesso al DNS secondario
    from {
        destination-address {
            x.x.x.x/32;
        }
        protocol tcp;
        destination-port domain;
    }
    then {
        log;
        syslog;
        accept;
    }
}
term T8 {              # Termine di accesso al DNS secondario
    from {
        destination-address {
            x.x.x.x/32;
        }
        protocol udp;
        destination-port domain;
    }
    then {
        log;
        syslog;
        accept;
    }
}
```

```
term T9 {              # Termine di accesso al Server
                       # di posta primario
    from {
        destination-address {
            x.x.x.x/32;
        }
        protocol tcp;
        destination-port smtp;
    }
    then {
        log;
        syslog;
        accept;
    }
}
term T10 {                # Accesso in SSH sulle macchine
                          # centrali del Servizio di Calcolo
    from {
        destination-address {
            x.x.x.x/32;
            x.x.x.x/32;
            ……..
        }
        protocol tcp;
        destination-port 22;
    }
    then {
        log;
        syslog;
        accept;
    }
}
term T11 {             # Accesso ai Server WEB LNF e INFN in HTTP
    from {
        destination-address {
            x.x.x.x/32;
            x.x.x.x/32;
            ……..
        }
        protocol tcp;
        destination-port http;
    }
    then {
        log;
        syslog;
        accept;
    }
}
term T12 {            # Accesso ai Server WEB LNF e INFN in HTTPS
    from {
        destination-address {
            x.x.x.x/32;
            x.x.x.x/32;
            ……..
        }
        protocol tcp;
        destination-port 443;
    }
    then {
        log;
        syslog;
        accept;
    }
}
```

```
term T13 {           # Accesso al Server WEB-MAIL
    from {
        destination-address {
            x.x.x.x/32;               }
        protocol udp;
        destination-port 443;
    }
    then {
        log;
        syslog;
        accept;
    }
}
term T14 {           # Accesso al Server WEB-MAIL
    from {
        destination-address {
            x.x.x.x/32;
        }
        protocol tcp;
        destination-port 443;
    }
    then {
        log;
        syslog;
        accept;
    }
}
term T25 {               # Permesso di accesso verso la
                         # cella AFS di Frascati
    from {
        destination-address {
            x.x.x.x/32;
            x.x.x.x/32;
            …….
        }
        protocol tcp;
        destination-port 7000-7009;
    }
    then {
        log;
        syslog;
        accept;
    }
}
term "Call-Back AFS" {   # Permesso any to any per le callbacks
                         # delle cache dei client AFS
    from {
        protocol tcp;
        destination-port 7001;
    }
    then {
        log;
        syslog;
        accept;
    }
}
```

```
term "Autenticazione afsserver INFN" { # autenticazione AFS
                                       # per Client Windows
    from {
        destination-address {
            x.x.x.x/32;
            x.x.x.x/32;
            ……
        }
        protocol udp;
        destination-port 750;
    }
    then {
        log;
        syslog;
        accept;
    }
}
term "NTP Server" {                # Permesso di sincronizzazione
                                   # del Network Time Protocol
    from {
        destination-address {
            x.x.x.x/32;
            x.x.x.x/32;
            ……
        }
        protocol udp;
        source-port ntp;
        destination-port ntp;
    }
    then {
        log;
        syslog;
        accept;
    }
}
term "NTP Server Traffico negato" {
    from {                     # Traffico NTP non permesso
                               # sulle porte diverse dal default
        destination-address {
            x.x.x.x/32;
            x.x.x.x/32;
            ……
        }
        protocol udp;
        destination-port ntp;
    }
    then {
        log;
        syslog;
        discard;
    }
}
term "Tunnel Appletalk" {          # Permesso al Tunnel AppleTalk
    from {
        destination-address {
            x.x.x.x/32;
        }
        protocol gre;
    }
    then {
        log;
        syslog;
        accept;
    }
}
```

```
term "Accesso GARR al Telnet" {     # Permesso di accesso al
                                    # router dal GARR
    from {
        source-address {
            x.x.x.x/32;
        }
        destination-address {
            x.x.x.x/32;
        }
        protocol tcp;
        destination-port telnet;
    }
    then {
        log;
        syslog;
        accept;
    }
}
term "FTP Dirpers" {                # Permesso verso FTP
                                    # Server autorizzati
    from {
        destination-address {
            x.x.x.x/32;
        }
        protocol tcp;
        destination-port [ ftp-data ftp ];
    }
    then {
        log;
        syslog;
        accept;
    }
}
term "Tunnel su IP" {               # Permesso al Tunnel per i
                                    # Client VPN Cisco

    from {
        destination-address {
            x.x.x.x/32;
            x.x.x.x/32;
        }
        protocol 50;
    }
    then {
        log;
        syslog;
        accept;
    }
}
term "Tunnel VPN-LNF" {             # Permesso al Tunnel per il
                                    # Server VPN LNF
    from {
        destination-address {
            x.x.x.x/32;
        }
        protocol gre;
    }
    then {
        log;
        syslog;
        accept;
    }
}
```

```
term VPN-LNF {                          # Permesso al Tunnel per il
                                        # Server VPN LNF
    from {
        destination-address {
            x.x.x.x/32;
        }
        protocol tcp;
        destination-port 1723;
    }
    then {
        log;
        syslog;
        accept;
    }
}
term "Divieto di tutte le porte TCP" {  # Blocco di tutte le
                                        #rimanenti porte TCP
    from {
        protocol tcp;
    }
    then {
        log;
        syslog;
        discard;
    }
}
term "Blocco porte UDP per NFS e MYSQL" {
                                        # Blocco porte UDP pericolose
    from {
        protocol udp;
        destination-port [ 2049 3306 ];
    }
    then {
        log;
        syslog;
        discard;
    }
}
term "Blocco porta UDP del Font Server" {
                                        # Blocco porte UDP pericolose
    from {
        destination-address {
            x.x.x.x/32;
        }
        protocol udp;
        destination-port 7000;
    }
    then {
        log;
        syslog;
        discard;
    }
}
term "Blocco porte UDP Font Server Webmin e worm MS-SQL Server" {
                                        # Blocco porte UDP pericolose
    from {
        protocol udp;
        destination-port [ 7100 10000 1434 ];
    }
    then {
        log;
        syslog;
        discard;
    }
}
```

```
    term "Permesso porte UDP sopra 1024" { # Permesso al traffico
                                           # UDP sopra la porta 1024
        from {
            protocol udp;
            destination-port 1025-65535;
        }
        then {
            log;
            syslog;
            accept;
        }
    }
    term "Blocco tutte le porte UDP" {     # Blocco del traffico UDP
                                           # sotto la porta 1024
        from {
            protocol udp;
        }
        then {
            syslog;
            discard;
        }
    }
    term "Permesso ICMP" {             # Permesso al traffico ICMP
        from {
            protocol icmp;
        }
        then {
            log;
            syslog;
            accept;
        }
    }
    term "Blocco tutto il traffico rimanente" {
                                       # Blocco del traffico residuo
        then {
            log;
            syslog;
            discard;
        }
    }
}

 # Filtro che protegge la LAN dei LNF vista sulla fe-0/1/0, dalla
 # VLAN degli ospiti ruotata sulla fe-0/1/1

filter 105 {
    term OK-DHCP {      # Permesso di accesso al Server DHCP dalla
                        # VLAN degli ospiti
        from {
            source-address {
                x.x.x.x/32;
            }
            destination-address {
                x.x.x.x/32;
            }
            protocol udp;
            source-port 67;
            destination-port 67;
        }
        then {
            log;
            syslog;
            accept;
        }
    }
```

```
term OK-OSPF {       # Permesso di accesso ai pacchetti di
                     # gestione OSPF
    from {
        protocol ospf;
    }
    then {
        log;
        syslog;
        accept;
    }
}
term T2 {            # Termine che permette il traffico già
                     # stabilito dai nodi interni
    from {
        destination-address {
            x.x.x.x/21;
            x.x.x.x/24;
            ……
        }
        protocol tcp;
        tcp-established;
    }
    then accept;
}
term T4 {              # Termine di accesso al DNS primario
    from {
        destination-address {
            x.x.x.x/32;
        }
        protocol tcp;
        destination-port domain;
    }
    then {
        log;
        syslog;
        accept;
    }
}

term T5 {              # Termine di accesso al DNS primario
    from {
        destination-address {
            x.x.x.x/32;
        }
        protocol udp;
        destination-port domain;
    }
    then {
        log;
        syslog;
        accept;
    }
}
   term T6 {             # Termine di accesso al Server di posta
                         # secondario
    from {
        destination-address {
            x.x.x.x/32;
        }
        protocol tcp;
        destination-port smtp;
    }
```

```
    then {
        log;
        syslog;
        accept;
    }
}
term T7 {              # Termine di accesso al DNS secondario
    from {
        destination-address {
            x.x.x.x/32;
        }
        protocol tcp;
        destination-port domain;
    }
    then {
        log;
        syslog;
        accept;
    }
}
term T8 {               # Termine di accesso al DNS secondario
    from {
        destination-address {
            x.x.x.x/32;
        }
        protocol udp;
        destination-port domain;
    }
    then {
        log;
        syslog;
        accept;
    }
}
term T9 {              # Termine di accesso al Server di posta
                       # primario
    from {
        destination-address {
            x.x.x.x/32;
        }
        protocol tcp;
        destination-port smtp;
    }
    then {
        log;
        syslog;
        accept;
    }
}
term T10 {              # Accesso in SSH sulle macchine centrali
                        # del Servizio di Calcolo
    from {
        destination-address {
            x.x.x.x/32;
            x.x.x.x/32;
            ……..
        }
        protocol tcp;
        destination-port 22;
    }
    then {
        log;
        syslog;
        accept;
    }
}
```

```
term T11 {            # Accesso ai Server WEB LNF e INFN in HTTP
    from {
        destination-address {
            x.x.x.x/32;
            x.x.x.x/32;
            ……..
        }
        protocol tcp;
        destination-port http;
    }
    then {
        log;
        syslog;
        accept;
    }
}
term T12 {           # Accesso ai Server WEB LNF e INFN in HTTPS
    from {
        destination-address {
            x.x.x.x/32;
            x.x.x.x/32;
            ……..
        }
        protocol tcp;
        destination-port 443;
    }
    then {
        log;
        syslog;
        accept;
    }
}
term T13 {           # Accesso al Server WEB-MAIL
    from {
        destination-address {
            x.x.x.x/32;               }
        protocol udp;
        destination-port 443;
    }
    then {
        log;
        syslog;
        accept;
    }
}
    term T14 {           # Accesso al Server WEB-MAIL
    from {
        destination-address {
            x.x.x.x/32;
        }
        protocol tcp;
        destination-port 443;
    }
    then {
        log;
        syslog;
        accept;
    }
}
```

```
term T25 {      # Permesso di accesso verso la cella
                # AFS di Frascati
    from {
        destination-address {
            x.x.x.x/32;
            x.x.x.x/32;
            …….
        }
        protocol tcp;
        destination-port 7000-7009;
    }
    then {
        log;
        syslog;
        accept;
    }
}
term "Call-Back AFS" {   # Permesso any to any per le callbacks
                         # delle cache dei client AFS
    from {
        protocol tcp;
        destination-port 7001;
    }
    then {
        log;
        syslog;
        accept;
    }
}
term "Autenticazione afsserver INFN" { # autenticazione AFS
                                       # per Client Windows
    from {
        destination-address {
            x.x.x.x/32;
            x.x.x.x/32;
            ……
        }
        protocol udp;
        destination-port 750;
    }
    then {
        log;
        syslog;
        accept;
    }
}

term "NTP Server" {           # Permesso di sincronizzazione
                                  # del Network Time Protocol
    from {
        destination-address {
            x.x.x.x/32;
            x.x.x.x/32;
            ……
        }
        protocol udp;
        source-port ntp;
        destination-port ntp;
    }
    then {
        log;
        syslog;
        accept;
    }
}
```

```
term "NTP Server Traffico negato" {
    from {                      # Traffico NTP non permesso
                                # sulle porte diverse dal default
        destination-address {
            x.x.x.x/32;
            x.x.x.x/32;
            ……
        }
        protocol udp;
        destination-port ntp;
    }
    then {
        log;
        syslog;
        discard;
    }
}
term "Tunnel Appletalk" {           # Permesso al Tunnel AppleTalk
    from {
        destination-address {
            x.x.x.x/32;
        }
        protocol gre;
    }
    then {
        log;
        syslog;
        accept;
    }
}
term "Accesso GARR al Telnet" {     # Permesso di accesso
                                    # al router dal GARR
    from {
        source-address {
            x.x.x.x/32;
        }
        destination-address {
            x.x.x.x/32;
        }
        protocol tcp;
        destination-port telnet;
    }
    then {
        log;
        syslog;
        accept;
    }
}
term "FTP Dirpers" {                # Permesso verso FTP Server
                                    # autorizzati
    from {
        destination-address {
            x.x.x.x/32;
        }
        protocol tcp;
        destination-port [ ftp-data ftp ];
    }
    then {
        log;
        syslog;
        accept;
    }
}
```

```
term "Tunnel su IP" {          # Permesso al Tunnel per i
                               # Client VPN Cisco
    from {
        destination-address {
            x.x.x.x/32;
            x.x.x.x/32;
        }
        protocol 50;
    }
    then {
        log;
        syslog;
        accept;
    }
}
term "Tunnel VPN-LNF" {        # Permesso al Tunnel per il
                               # Server VPN LNF
    from {
        destination-address {
            x.x.x.x/32;
        }
        protocol gre;
    }
    then {
        log;
        syslog;
        accept;
    }
}
term VPN-LNF {                 # Permesso al Tunnel per il
                               # Server VPN LNF
    from {
        destination-address {
            x.x.x.x/32;
        }
        protocol tcp;
        destination-port 1723;
    }
    then {
        log;
        syslog;
        accept;
    }
}
term "Divieto di tutte le porte TCP" {  # Blocco di tutte le
                                        # rimanenti porte TCP
    from {
        protocol tcp;
    }
    then {
        log;
        syslog;
        discard;
    }
}
term "Blocco porte UDP per NFS e MYSQL" {
                                    # Blocco porte UDP pericolose
    from {
        protocol udp;
        destination-port [ 2049 3306 ];
    }
```

```
    then {
        log;
        syslog;
        discard;
    }
}
term "Blocco porta UDP del Font Server" {
                                    # Blocco porte UDP pericolose
    from {
        destination-address {
            x.x.x.x/32;
        }
        protocol udp;
        destination-port 7000;
    }
    then {
        log;
        syslog;
        discard;
    }
}
term "Blocco porte UDP Font Server Webmin e worm MS-SQL Server" {
                                   # Blocco porte UDP pericolose

    from {
        protocol udp;
        destination-port [ 7100 10000 1434 ];
    }
    then {
        log;
        syslog;
        discard;
    }
}
term "Permesso porte UDP sopra 1024" { # Permesso al traffico
                                       # UDP sopra la porta 1024
    from {
        protocol udp;
        destination-port 1025-65535;
    }
    then {
        log;
        syslog;
        accept;
    }
}
term "Blocco tutte le porte UDP" {     # Blocco del traffico UDP
                                       # sotto la porta 1024
    from {
        protocol udp;
    }
    then {
        syslog;
        discard;
    }
}
term "Permesso ICMP" {             # Permesso al traffico ICMP
    from {
        protocol icmp;
    }
    then {
        log;
        syslog;
        accept;
    }
}
```

```
term "Blocco tutto il traffico rimanente" {
                                                # Blocco del traffico residuo
            then {
                log;
                syslog;
                discard;
            }
        }
    }
```

## A.6 Configurazione router di Bologna

```
version 5.3R1.2;

system {
    host-name junbo;
    domain-name xx.infn.it;
    time-zone Europe/Rome;
    name-server {
        x.x.x.x;
        x.x.x.x;
    }
    login {                              # configurazione utenti
        user xxx {                       # che hanno accesso al router
            uid 2000;
            class superuser;
            authentication {
                encrypted-password "xxxxxxxxxxxxxxxxxx"; # SECRET-DATA
            }
        }
    }
    services {                           # Servizi disponibili per gli
        ftp {                            # utenti e loro limitazioni
            connection-limit 1;
            rate-limit 5;
        }
        ssh {
            protocol-version v2;
            connection-limit 5;
            rate-limit 5;
        }
        telnet {
            connection-limit 2;
            rate-limit 5;
        }
    }
    syslog {                                 # configurazione LogServer
        host x.x.x.x {
            any any;
            facility-override local4;
        }
        file messages {
            any any;
        }
    }
}
interfaces {                                 # configurazione interfaccia
    fe-0/1/0 {                               # FastEthernet verso la LAN
        description FE-INFN;
        unit 0 {
            family inet {
                address x.x.x.x/y;
            }
        }
    }
```

```
    at-0/2/0 {                              # configurazione interfaccia
        atm-options {                       # collegamento GARR
            vpi 133 maximum-vcs 2045;
            vpi 150 maximum-vcs 2045;
        }
        t3-options {
            no-payload-scrambler;
        }
        unit 1 {
            description "INFN-GARR";
            encapsulation atm-snap;
            point-to-point;
            vci 133.203;
            shaping {
                vbr peak 108544000 sustained 108544000 burst 1;
            }
            family inet {
                filter {
                    input 103;                  # Filtro in ingresso
                    output 104;                 # Filtro in uscita
                }
                address x.x.x.x/yy;
            }
        }
    }
    lo0 {
        unit 0 {
            family inet {
                address 127.0.0.1/32;
            }
        }
    }
}
snmp {                                          # configurazione SNMP
    description "Juniper M5 - Bologna";
    location "Bologna - sala macchine INFN";
    community xxxxxx {
        authorization read-write;
    }
    community yyyyyy {
        authorization read-only;
    }
}
accounting-options;                     # route statiche verso GARR
routing-options {                       # route statiche sede secondaria
    static {                            # route statiche Backdoor Cnaf
        route 0.0.0.0/0 {
            next-hop x.x.x.x;
            retain;
        }
        route x.x.x.x/yy next-hop k.k.k.k;
        route h.h.h.h/yy next-hop j.j.j.j;

    }
}
```

```
firewall {

    filter 103 {                          # Filtro in ingresso GARR
       term T1   {                        # permette monitor dal Garr
            from {
                source-address {
                    193.206.128.0/24
                }
            }
            then {
                syslog;
                accept;
            }
        }


        term T2 {                         # permette connessioni
            from {                        # established
                protocol tcp;
                tcp-established;
            }
            then accept;
        }


        term T3 {                         # Antispoofing: blocca nostre
            from {                        # network e network riservate
                source-address {
                    131.x.x.x/24;
                    131.y.y.y/24;
                    0.0.0.0/32;
                    127.0.0.0/8;
                    10.0.0.0/8;
                    172.16.0.0/12;
                    192.168.0.0/16;
                    213.215.166.83/32;
                    192.65.185.43/32;
                }
            }
            then {
                log;
                syslog;
                discard;
            }
        }

        term T4 {                         # blocca i seguenti host
            from {                        # locali completamente
                destination-address {
                    x.x.x.x/32;
                }
            }
            then {
                log;
                syslog;
                discard;
            }
        }
```

```
term T5 {                           # blocca i seguenti host
    from {                          # remoti completamente
        source-address {
            x.x.x.x/yy;
            k.k.k.k/yy;
        }
    }
    then {
        count T5-counter;           # conta pacchetti scartati
        log;
        syslog;
        discard;
    }
}

term T6 {                           # permetto da network remota
    from {                          # a host locale su intervallo
        source-address {            # porte definite
            x.x.x.0/24;
        }
        destination-address {
            y.y.y.y/32;
        }
        protocol tcp;
        destination-port aaaa-bbbb;
    }
    then {
        syslog;
        accept;
    }
}

term T7 {                                   # blocca porte 1-20
    from {                                  # per tutti tcp-udp
        protocol [tcp udp];
        destination-port 1-20;
    }
    then {
        log;
        syslog;
        discard;
    }
}

term T8  {                                  # permette accesso FTP
    from {                                  # per autorizzati
        source-address {
            x.x.x.x/32;
            y.y.y.y/32;
        }
        destination-address {
            k.k.k.k/32;
        }
        protocol tcp;
        destination-port ftp;
    }
    then {
        syslog;
        accept;
    }
}
```

```
 term T9  {                          # blocca FTP
    from {                           # per tutti tcp-udp
        protocol [tcp udp];
        destination-port ftp;
    }
    then {
        log;
        syslog;
        discard;
    }
}

term T10 {                          # blocca porta 22 verso host
  from {                            # locali con versioni SSH non
        destination-address {       # sicure
            x.x.x.x/yy;
            h.h.h.h/yy;
        }
        protocol [tcp udp];
        destination-port 22;
    }
    then {
        syslog;
        discard;
    }
}


term T11 {                                  # permette telnet solo
    from {                                  # autorizzati
        source-address {
            x.x.x.x/yy;
            h.h.h.h/yy;
        }
        destination-address {
            k.k.k.k/yy;
        }
        protocol tcp;
        destination-port telnet;
    }
    then {
        syslog;
        accept;
    }
}
term T12 {                                  # blocca porte 23-24
    from {                                  # per tutti tcp-udp
        protocol [tcp udp];
        destination-port 23-24;
    }
    then {
        log;
        syslog;
        discard;
    }
}
```

```
term T13 {                          # permette porta 25
    from {                          # solo verso mailserver
        destination-address {
            x.x.x.x/yy;
            y.y.y.y/yy;
        }
        protocol tcp;
        destination-port smtp;
    }
    then accept;
}

term T14 {                              # blocca porte 25-52
    from {                              # per tutti tcp-udp
        protocol [tcp udp];
        destination-port 25-52;
    }
    then {
        log;
        syslog;
        discard;
    }
}

term T15 {                              # permette porta 53
    from {                              # solo per DNS Server
        destination-address {
            x.x.x.x/yy;
            k.k.k.k/yy;
        }
        protocol [tcp udp];
        destination-port domain;
    }
    then accept;
}

term T16 {                              # blocca porte 53-79
    from {                              # per tutti tcp-udp
        protocol [tcp udp];
        destination-port 53-79;
    }
    then {
        log;
        syslog;
        discard;
    }
}


term T17 {                          # permette porta 80 solo
    from {                          # per WWW server autorizzati
        destination-address {
            x.x.x.x/yy;
            k.k.k.k/yy;
        }
        protocol tcp;
        destination-port http;
    }
    then accept;
}
```

```
term T18 {                      # blocca porte 80-109
    from {                      # per tutti tcp-udp
        protocol [tcp udp];
        destination-port 80-109;
    }
    then {
        log;
        syslog;
        discard;
    }
}

term T19 {                          # permette porta 110 solo per
    from {                          # Pop Server autorizzati
        destination-address {
            x.x.x.x/yy;
        }
        protocol tcp;
        destination-port pop3;
    }
    then accept;
}

term T20 {                          # blocca porte 110-136
    from {                          # per tutti tcp-udp
        protocol [tcp udp];
        destination-port [ 110-136 ];
    }
    then {
        log;
        syslog;
        discard;
    }
}

term T21 {                      # permette porte 137-139 Netbios
    from {                      # solo per autorizzati
        source-address {
            x.x.x.x/yy;
            y.y.y.y/yy;
        }
        destination-address {
            k.k.k.k/yy;
        }
        protocol [tcp udp];
        destination-port 137-139;
    }
    then accept;
}

term T22 {                              # blocca porte 137-142
    from {                              # per tutti tcp-udp
        protocol [tcp udp];
        destination-port 137-142;
    }
    then {
        log;
        syslog;
        discard;
    }
}
```

```
term T23 {                          # permette porta 143 solo
    from {                          # per IMAP server autorizzati
        destination-address {
            x.x.x.x/yy;
            h.h.h.h/yy;
        }
        protocol tcp;
        destination-port 143;
    }
    then accept;
}

term T24 {                              # blocca porte 143-169
    from {                              # per tutti tcp-udp
        protocol [tcp udp];
        destination-port 143-169;
    }
    then {
        log;
        syslog;
        discard;
    }
}

term T25 {                          # permette porta 170 printsrv
    from {                          # per network autorizzate
        source-address {
            x.x.x.0/yy;
        }
        destination-address {
            h.h.h.h/yy;
            y.y.y.y/yy;
        }
        protocol tcp;
        destination-port 170;
    }
    then accept;
}

term T26 {                              # blocca porte 170-442
    from {                              # per tutti tcp-udp
        protocol [tcp udp];
        destination-port 170-442;
    }
    then {
        log;
        syslog;
        discard;
    }
}

term T27 {                          # permette porta 443 HTTPS
    from {                          # solo per autorizzati
        destination-address {
            x.x.x.x/yy;
            k.k.k.k/yy;
        }
        protocol tcp;
        destination-port 443;
    }
    then accept;
}
```

```
 term T28 {                              # blocca porte 443-444
    from {                               # per tutti tcp-udp
        protocol [tcp udp];
        destination-port 443-444;
    }
    then {
        log;
        syslog;
        discard;
    }
}

term T29 {                          # permette porta 445 Microsoft DS
    from {                          # solo per autorizzati
        source-address {
            x.x.x.x/yy;
            h.h.h.h/yy;
        }
        destination-address {
            k.k.k.k/yy;
        }
        protocol [ tcp udp ];
        destination-port 445;
    }
    then accept;
}

term T30 {                              # blocca porte 445-448
    from {                              # per tutti tcp-udp
        protocol [tcp udp];
        destination-port 445-448;
    }
    then {
        log;
        syslog;
        discard;
    }
}
term T31 {                          # permette porta 449 JavaScript
    from {                          # solo per host locali autorizzati
        source-address {
            x.x.x.x/yy;
            h.h.h.h/yy;
        }
        destination-address {
            k.k.k.k/yy;
        }
        protocol tcp;
        destination-port 449;
    }
    then accept;
}
term T32 {                              # blocca porte 449-499
    from {                              # per tutti tcp-udp
        protocol [tcp udp];
        destination-port 449-499;
    }
    then {
        log;
        syslog;
        discard;
    }
}
```

```
term T33 {                          # permette porta 500 VPN solo
    from {                          # per host locali autorizzati
        destination-address {
            x.x.x.x/yy;
            h.h.h.h/yy;
        }
        protocol udp;
        destination-port 500;
    }
    then accept;
}

term T34 {                              # blocca porte 500-514
    from {                              # per tutti tcp-udp
        protocol [tcp udp];
        destination-port 500-514;
    }
    then {
        log;
        syslog;
        discard;
    }
}

term T35 {                          # permette porta 515 lpd
    from {                          # per network autorizzate
        source-address {
            x.x.x.0/yy;
        }
        destination-address {
            h.h.h.h/yy;
            k.k.k.k/yy;
        }
        protocol tcp;
        destination-port 515;
    }
    then accept;
}

term T36 {                              # blocca porte 515-970
    from {                              # per tutti tcp-udp
        protocol [tcp udp];
        destination-port 515-970;
    }
    then {
        log;
        syslog;
        discard;
    }
}

term T37 {                          # permette porta 993 IMAP-SSL
    from {                          # solo host locali autorizzati
        destination-address {
            x.x.x.x/yy;
            h.h.h.h/yy;
        }
        protocol tcp;
        destination-port 993;
    }
    then accept;
}
```

```
term T38 {                              # blocca porta 993 per
    from {                              # tutti gli altri tcp-udp
        protocol [tcp udp];
        destination-port 993;
    }
    then {
        log;
        syslog;
        discard;
    }
}

term T39 {                              # blocca porta 1080 IRC
    from {                              # per tutti tcp-udp
        protocol [tcp udp];
        destination-port 1080;
    }
    then {
        log;
        syslog;
        discard;
    }
}

term T40 {                              # blocca porta 1115 ardus
    from {                              # per tutti tcp-udp
        protocol [tcp udp];
        destination-port 1115;
    }
    then {
        log;
        syslog;
        discard;
    }
}

term T41 {                              # blocca porta 1214 Kaaza
    from {                              # per tutti tcp-udp
        protocol [tcp udp];
        destination-port 1214;
    }
    then {
        log;
        syslog;
        discard;
    }
}

term T42 {                      # blocca porte 1433-1434 MS-SQL
    from {                      # per tutti tcp-udp
        protocol [tcp tcp];
        destination-port 1433-1434;
    }
    then {
        log;
        syslog;
        discard;
    }
}
```

```
term T43 {                              # blocca porta 1993 Cisco
    from {                              # per tutti tcp-udp
        protocol [tcp udp];
        destination-port 1993;
    }
    then {
        log;
        syslog;
        discard;
    }
}

term T44 {                              # blocca porta 2002 SSL
    from {                              # per tutti tcp-udp
        protocol [tcp udp];
        destination-port 2002;
    }
    then {
        log;
        syslog;
        discard;
    }
}

term T45 {                          # blocca porta 2049 NFS
    from {                          # per tutti tcp-udp
        protocol [tcp udp];
        destination-port 2049;
    }
    then {
        log;
        syslog;
        discard;
    }
}

term T46 {                          # blocca porte 2773-2774
    from {                              # sub-seven trojan
        protocol [tcp udp];             # per tutti tcp-udp
        destination-port 2773-2774;
    }
    then {
        log;
        syslog;
        discard;
    }
}

term T47 {                      # blocca porte 4600-4700 eDonkey
    from {                      # per tutti tcp-udp
        protocol [tcp udp];
        destination-port 4600-4700;
    }
    then {
        log;
        syslog;
        discard;
    }
}
```

```
term T48 {                          # blocca porte 6200-6300 WinMX
    from {                          # per tutti tcp-udp
        protocol [tcp udp];
        destination-port 6200-6300;
    }
    then {
        log;
        syslog;
        discard;
    }
}

term T49 {                      # blocca porte 6300-6400 Gnutella
    from {                      # per tutti tcp-udp
        protocol [tcp udp];
        destination-port 6300-6400;
    }
    then {
        log;
        syslog;
        discard;
    }
}

term T50 {                          # blocca porta 6667 IRC
    from {                          # per tutti tcp-udp
        protocol [tcp udp];
        destination-port 6667;
    }
    then {
        log;
        syslog;
        discard;
    }
}

term T52 {                          # blocca porte 6600-6800 WinMX
    from {                          # per tutti tcp-udp
        protocol [tcp udp];
        destination-port 6600-6800;
    }
    then {
        log;
        syslog;
        discard;
    }
}

term T53 {                          # blocca porta 27374 WormRamen
    from {                          # per tutti tcp-udp
        protocol [tcp udp];
        destination-port 27374;
    }
    then {
        log;
        syslog;
        discard;
    }
}
```

```
    term T54 {                          # blocca porta 43981 NetWare
        from {                          # per tutti tcp-udp
            protocol [tcp udp];
            destination-port 43981;
        }
        then {
            log;
            syslog;
            discard;
        }
    }


    term T55 {                          # Attenzione, questa deve
        then accept;                    # essere l'ultima regola:
    }                                   # tutto quello che non viene
}                                       # filtrato deve PASSARE


filter 104 {                            # Filtro in uscita GARR
    term T1 {                           # blocca host locali in uscita
        from {
            source-address {
                x.x.x.x/yy;
                h.h.h.h/yy;
            }
        }
        then {
            log;
            syslog;
            discard;
        }
    }

    term T2 {                               # blocca porta 1214
        from {                              # per tutti tcp-udp
            protocol [tcp udp];
            destination-port 1214;
        }
        then {
            log;
            syslog;
            discard;
        }
    }

    term T3 {                               # blocca porte 1433-1434
        from {                              # per tutti tcp-udp
            protocol [tcp udp];
            destination-port 1433-1434;
        }
        then {
            log;
            syslog;
            discard;
        }
    }
```

```
term T4 {                           # blocca porta 2002
    from {                          # per tutti tcp-udp
        protocol [tcp udp];
        destination-port 2002;
    }
    then {
        log;
        syslog;
        discard;
    }
}

term T5 {                           # blocca porte 4600-4700
    from {                          # per tutti tcp-udp
        protocol [tcp udp];
        destination-port 4600-4700;
    }
    then {
        log;
        syslog;
        discard;
    }
}

term T6 {                           # blocca porte 6346-6347
    from {                          # per tutti tcp-udp
        protocol [tcp udp];
        destination-port 6346-6347;
    }
    then {
        log;
        syslog;
        discard;
    }
}

term T7 {                           # blocca porte 6600-6800
    from {                          # per tutti tcp-udp
        protocol [ tcp udp ];
        destination-port 6600-6800;
    }
    then {
        log;
        syslog;
        discard;
    }
}

term T8 {                           # blocca porta 6667
    from {                          # per tutti tcp-udp
        protocol [tcp udp];
        destination-port 6667;
    }
    then {
        log;
        syslog;
        discard;
    }
}
```

```
        term T9 {                           # blocca porta 27374
            from {                          # per tutti tcp-udp
                protocol [tcp udp];
                destination-port 27374;
            }
            then {
                log;
                syslog;
                discard;
            }
        }

        term T10 {                          # Antispoofing su network locali
            from {
                source-address {
                    x.x.x.0/yy;
                }
            }
            then accept;
        }
        term T16 {                          # permette monitoring (ping)
            from {                          # dal GARR
                destination-address {
                    x.x.x.x/yy;
                }
            }
            then {
                syslog;
                accept;
            }
        }

        term T17 {                      # ATTENZIONE: tutto il resto viene
            then {                      # BLOCCATO!
                log;
                syslog;
                discard;
            }
        }
    }
}
```

## A.7 MIB

Vengono qui riportate le *MIB* utilizzate per l'interrogazione remota dei *Router Juniper M5* via *snmp* dei parametri monitorati durante i test:

- Forwarding Engine - CPU .1.3.6.1.4.1.2636.3.1.13.1.8.6.1.0
- Forwarding Engine - Interrupt Util. .1.3.6.1.4.1.2636.3.1.13.1.9.6.1.0.0
- Forwarding Engine - Heap Util. .1.3.6.1.4.1.2636.3.1.13.1.12.6.1.0.0
- Forwarding Engine - Buffer Util. .1.3.6.1.4.1.2636.3.1.13.1.11.6.1.0
- Routing Engine – CPU .1.3.6.1.4.1.2636.3.1.13.1.8.9.1.0.0

## A.8 Lista Acronimi

| | |
|---|---|
| ACL | Access Control List; *termini* o *regole* nel linguaggio JunOS |
| ASIC | Application Specific Integrated Circuit |
| ATM | Asyncronous Transfer Mode |
| BSD | Berkeley Software Distribution |
| CPU | Central Processor Unit |
| GARR | *Consortium* per la gestione delle Reti dell'Università e della Ricerca Scientifica Italiana |
| ICMP | Internet Control Message Protocol |
| IOS | Internetworking Operating System (Cisco) |
| JUNOS | Juniper Operating System |
| IP | Internet Protocol |
| MIB | Management Information Base |
| PIC | Physical Interface Card (Juniper) |
| PoP | Point of Presence |
| RRD | Round Robin Database |
| SNMP | Simple Network Management Protocol |
| SSHD | Secure Shell Daemon |
| TCP | Transmission Control Protocol |
| UDP | User Datagram Protocol |
| VPN | Virtual Private Network |