Traffic Shaping

Realizzazione di un traffic shaper di Sezione con un Linux Box

Problemi

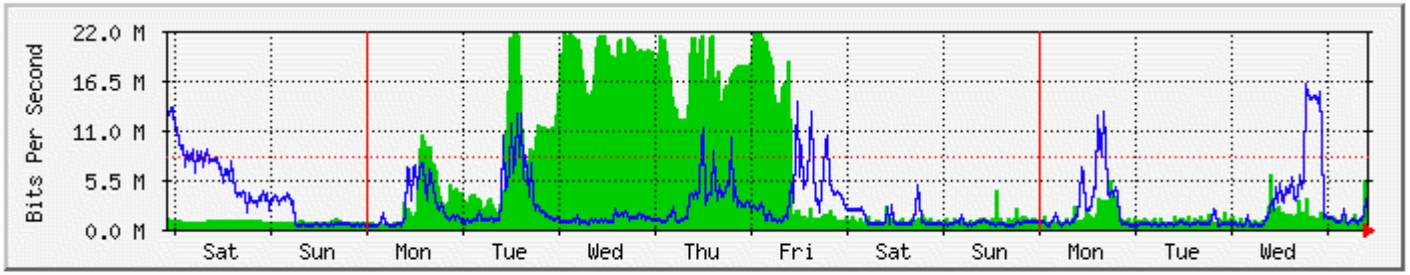
- L'accesso a Internet è una risorsa limitata e costosa
- Un'eccessiva congestione di un link può portare le applicazioni a non rispondere nei tempi prestabiliti (Applicazioni Real-Time)
- I grossi trasferimenti di dati AFS tendono a saturare la banda
- Spesso ad impegnare la banda sono applicazioni P2P per filesharing

Obiettivi

- Dare una priorità al traffico delle diverse applicazioni che comunicano tramite Internet
  - Applicazioni Real-Time come il VoIP, le Videoconferenze e le sessioni interattive (SSH) devono avere massima priorità
  - L'accesso al Web deve risultare il più fluido possibile
  - I grossi trasferimenti di dati (AFS, FTP, SMTP, ...) che in genere non necessitano di latenza bassa devono avere bassa priorità
- Limitare la banda disponibile per applicazioni non fondamentali (per es. alcuni tipi di P2P per filesharing)

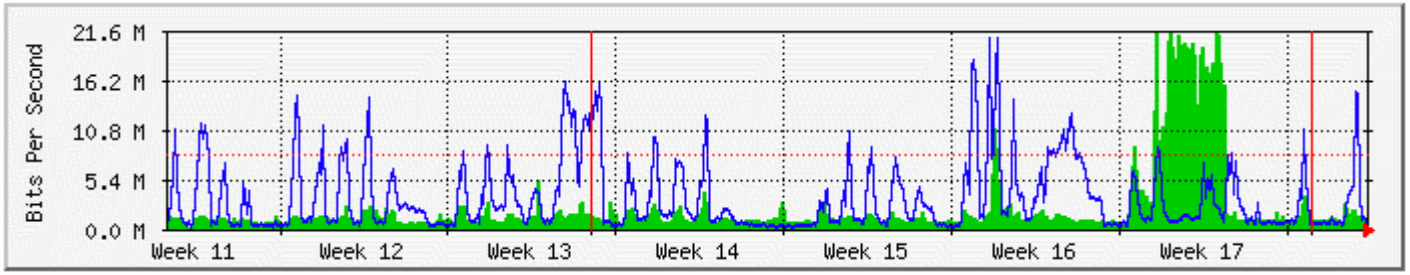
Esempio di Traffico P2P

`Weekly' Graph (30 Minute Average)



	Max	Average	Current
In/s:	21.8 Mb/s (271.9%)	5208.0 kb/s (65.1%)	2602.9 kb/s (32.5%)
Out/s:	16.0 Mb/s (200.1%)	2557.8 kb/s (32.0%)	3424.3 kb/s (42.8%)

`Monthly' Graph (2 Hour Average)



	Max	Average	Current
In/s:	21.4 Mb/s (267.5%)	2207.5 kb/s (27.6%)	1075.8 kb/s (13.4%)
Out/s:	20.6 Mb/s (257.8%)	3232.6 kb/s (40.4%)	817.3 kb/s (10.2%)

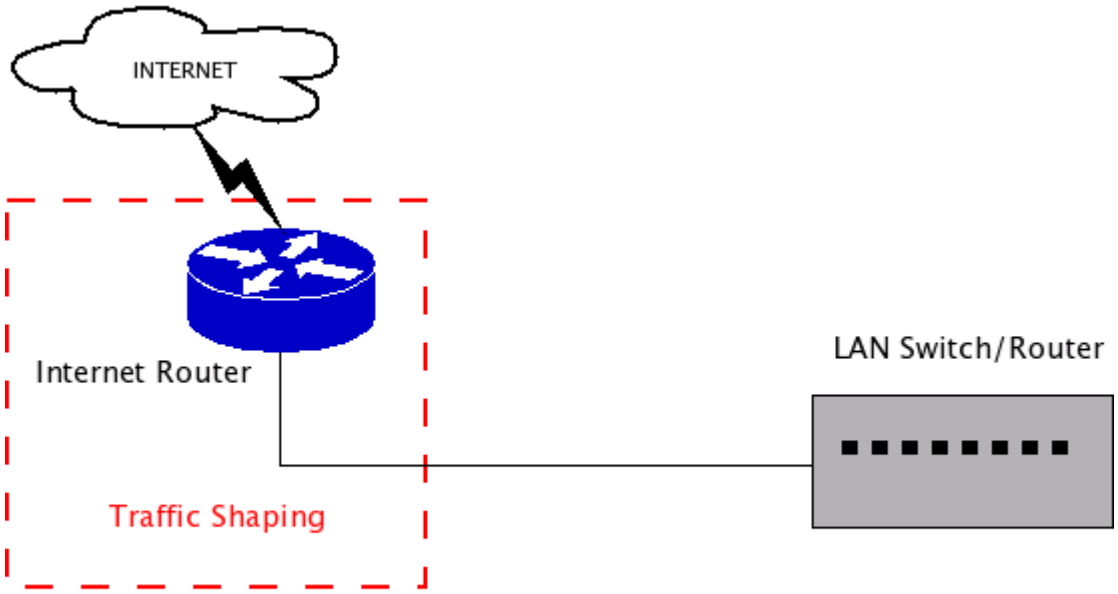
Obiettivi più in dettaglio

Applicazione	**Priorità**	**Banda Garantita**	**Banda Massima**
SIP, H323, MSN Messenger, Skype	Alta	4Mbit/s	-
SSH	Alta	512Kbit/s	-
HTTP	Media	512Kbit/s	-
Default	Media	512Kbit/s	-
AFS, FTP, SMTP	Bassa	512Kbit/s	-
P2P (eMule,EDonkey,Kademlia,KaZaA,FastTrack, Gnutella,BitTorrent, Direct Connect)	Bassa	-	512Kbit/s

Possibili Soluzioni

1. Applicare il traffic shaping sul router di accesso ad Internet
2. Applicare il QoS sugli switch/router della LAN
3. Applicare il traffic shaping su di un bridge o router Linux posto tra il router di accesso a Internet e il router della LAN

Soluzione 1



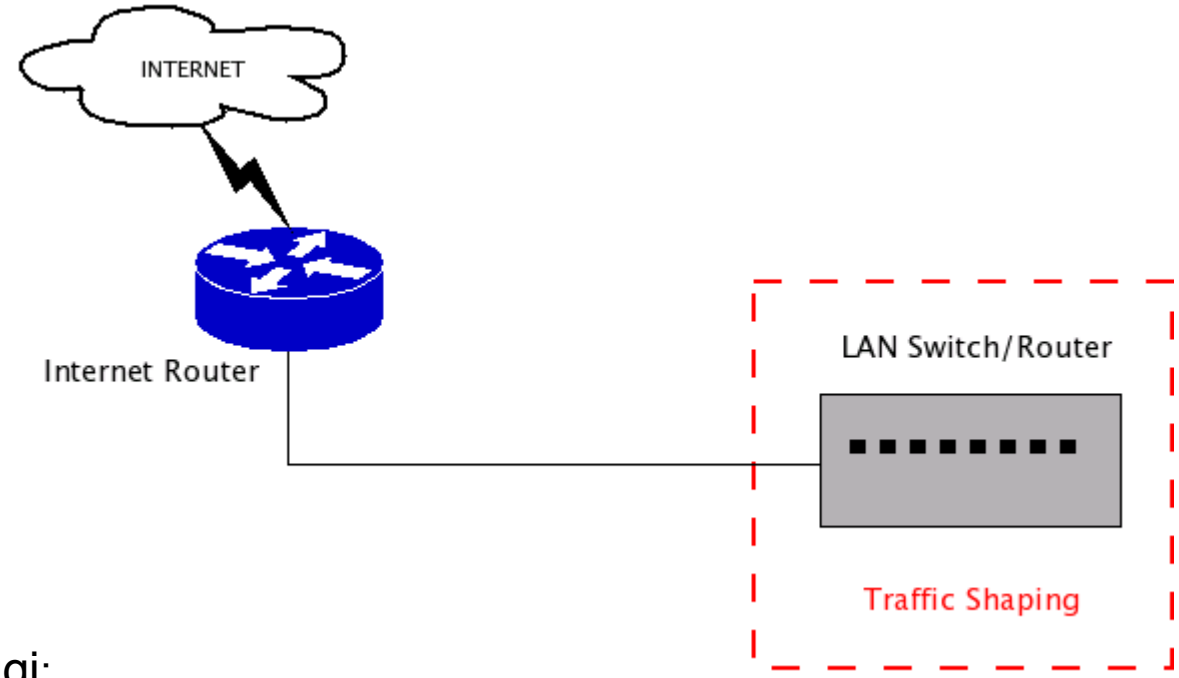
Vantaggi:

- Non è necessario ulteriore hardware e quindi non si introducono ulteriori punti di failure

Svantaggi:

- Poca flessibilità nella classificazione del traffico. Spesso i parametri di classificazione sono solo gli indirizzi IP e le porte TCP/UDP

Soluzione 2



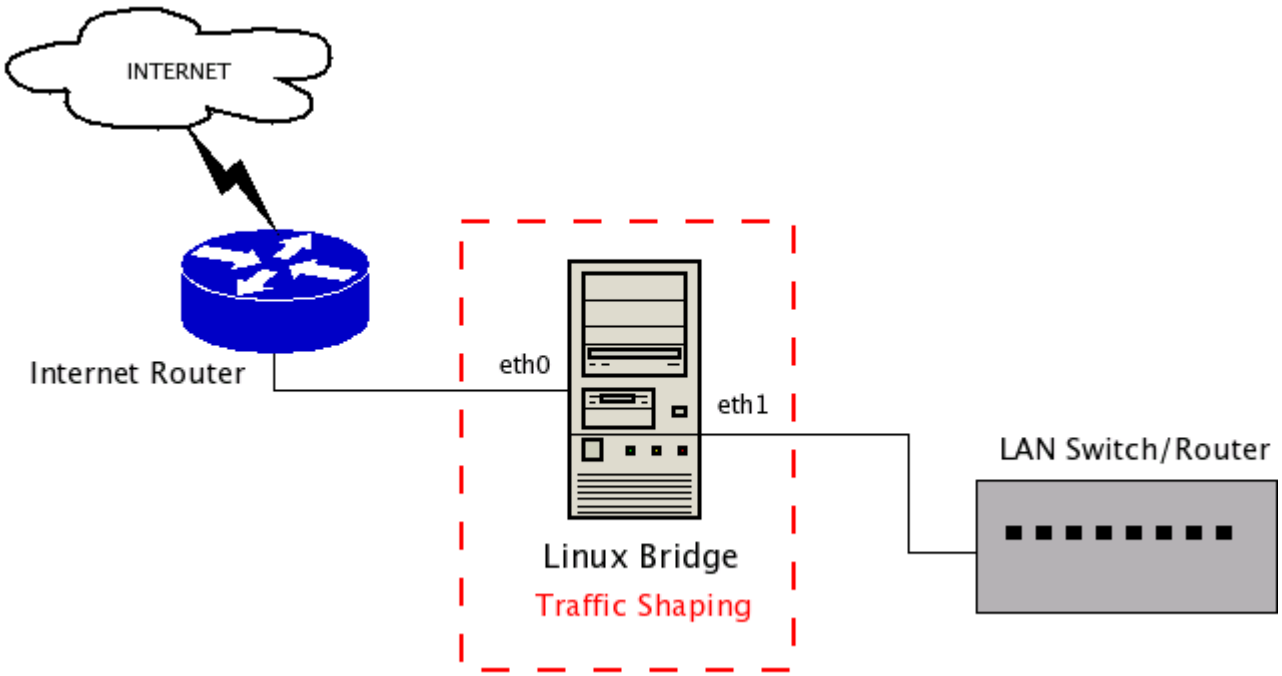
Vantaggi:

- Non è necessario ulteriore hardware e quindi non si introducono ulteriori punti di failure
- E' possibile impostare regole di QoS per comunicazioni che avvengono tra host della LAN
- Il traffic shaping non carica la CPU dello Switch/Router poiché il tutto è gestito tramite ASIC

Svantaggi:

- Poca flessibilità nella classificazione del traffico. Spesso i parametri di classificazione sono solo le porte fisiche, gli indirizzi IP e le porte TCP/UDP

Soluzione 3


INTERNET
Internet Router
eth0
eth1
Linux Bridge
Traffic Shaping
LAN Switch/Router

Vantaggi e svantaggi della soluzione Linux Bridge

- Vantaggi
  - Elevata flessibilità e programmabilità
    - Ampia scelta di discipline di traffic shaping e prioritizzazione (FIFO, PRIO, CBQ, HTB, ...)
    - Classificatori di traffico molto completi e flessibili
    - E' possibile utilizzare iptables per classificare
      - Iptables di dispone di filtri layer 7 (l7-filter e IPP2P)
      - Iptables permette di classificare il traffico anche in funzione dell'orario e del giorno della settimana
  - E' possibile installare software di monitoring del traffico come per esempio ntop e iptraf
- Svantaggi
  - L'introduzione di ulteriore hardware aumenta la probabilità che si verifichi un guasto
  - E' necessario verificare che il Bridge Linux non diventi un collo di bottiglia

Routing o Transparent Bridging

- Le QDisc si agganciano direttamente alle interfacce di rete e lavorano a livello di datalink
  - La conseguenza di ciò è che tutti i concetti e le tecniche di Traffic Shaping sono validi sia nel caso che il box Linux faccia da Router che da Bridge
- Si è preferito il bridging perché è trasparente dal punto di vista della configurazione IP del router di accesso a Internet e dello Switch/Router della LAN
  - In caso di guasto (o reboot) del bridge Linux è sufficiente bypassarlo con un cavo di rete che collega direttamente i due router preesistenti
  - E' possibile ridondare il Linux Bridge utilizzando lo Spanning Tree Protocol che assicurerà che un solo bridge sia attivo per volta.

Traffic Shaping solo in uscita

- Linux applica politiche di traffic shaping solo sul traffico uscente da un'interfaccia di rete
  - Il motivo di ciò è che su un pacchetto in ingresso l'unica cosa che si potrebbe fare è scartarlo prima che entri nel prerouting del Linux Box. Ma ciò avrebbe poco senso, visto che tanto ormai quel pacchetto ha già occupato il link
- Per controllare il flusso entrante da Internet è necessario perciò agire sul traffico uscente dall'interfaccia che si connette al router della LAN

QDisc HTB (Hierarchical Token Bucket)

La Queuing Discipline HTB è stata scelta perché:

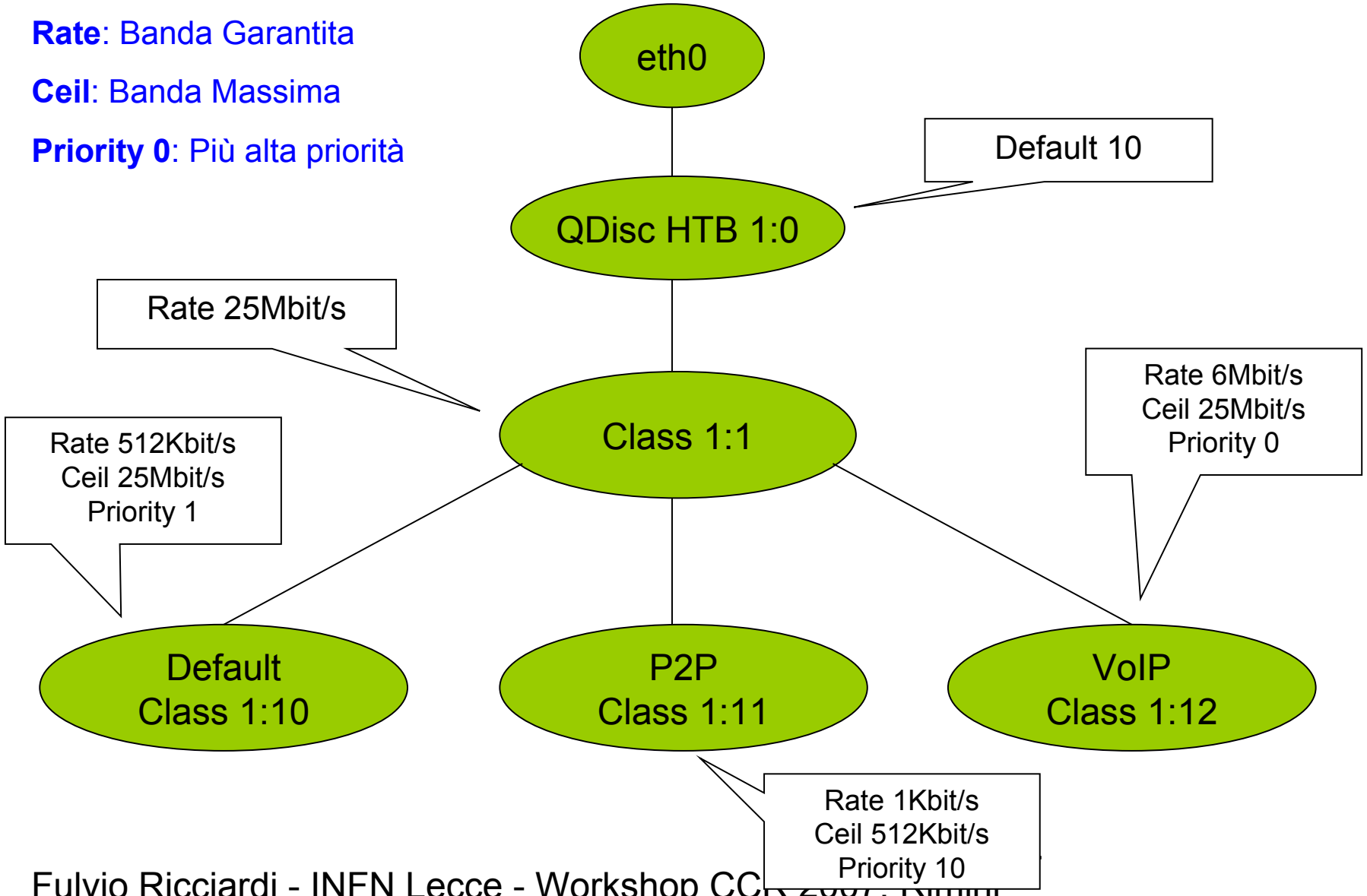
- Permette la suddivisione del traffico in classi disposte gerarchicamente
- Per ogni classe è possibile assegnare la **Banda Garantita**
- Per ogni classe è possibile assegnare la **Banda Massima**
- Tra classi dello stesso livello è possibile stabilire la **Priorità**
- HTB è stata inclusa nel Kernel di Linux ed è automaticamente supportata dal comando tc (Traffic Control) di iproute2
- E' semplice da usare

Struttura della QDisc HTB

Rate: Banda Garantita

Ceil: Banda Massima

Priority 0: Più alta priorità



Esempio di impostazione di HTB

- tc qdisc del dev eth0 root
- tc qdisc add dev eth0 root handle 1:0 htb default 10
- tc class add dev eth0 parent 1:0 classid 1:1 htb rate 25Mbit
- tc class add dev eth0 parent 1:1 classid 1:10 htb rate 512Kbit ceil 25Mbit prio 1
- tc class add dev eth0 parent 1:1 classid 1:11 htb rate 1Kbit ceil 0.5Mbit prio 10
- tc class add dev eth0 parent 1:1 classid 1:12 htb rate 6Mbit ceil 25Mbit prio 0

- tc qdisc del dev eth1 root
- tc qdisc add dev eth1 root handle 1:0 htb default 10
- tc class add dev eth1 parent 1:0 classid 1:1 htb rate 25Mbit
- tc class add dev eth1 parent 1:1 classid 1:10 htb rate 512Kbit ceil 25Mbit prio 1
- tc class add dev eth1 parent 1:1 classid 1:11 htb rate 1Kbit ceil 0.5Mbit prio 10
- tc class add dev eth1 parent 1:1 classid 1:12 htb rate 6Mbit ceil 25Mbit prio 0

Classificatori

Classificatore u32

- tc filter add dev eth0 protocol ip parent 1:0 prio 1 u32 match ip dport 22 0xffff flowid 1:12
- tc filter add dev eth0 parent 1:0 protocol ip prio 1 u32 match ip dst 192.168.0.1/32 flowid 1:11

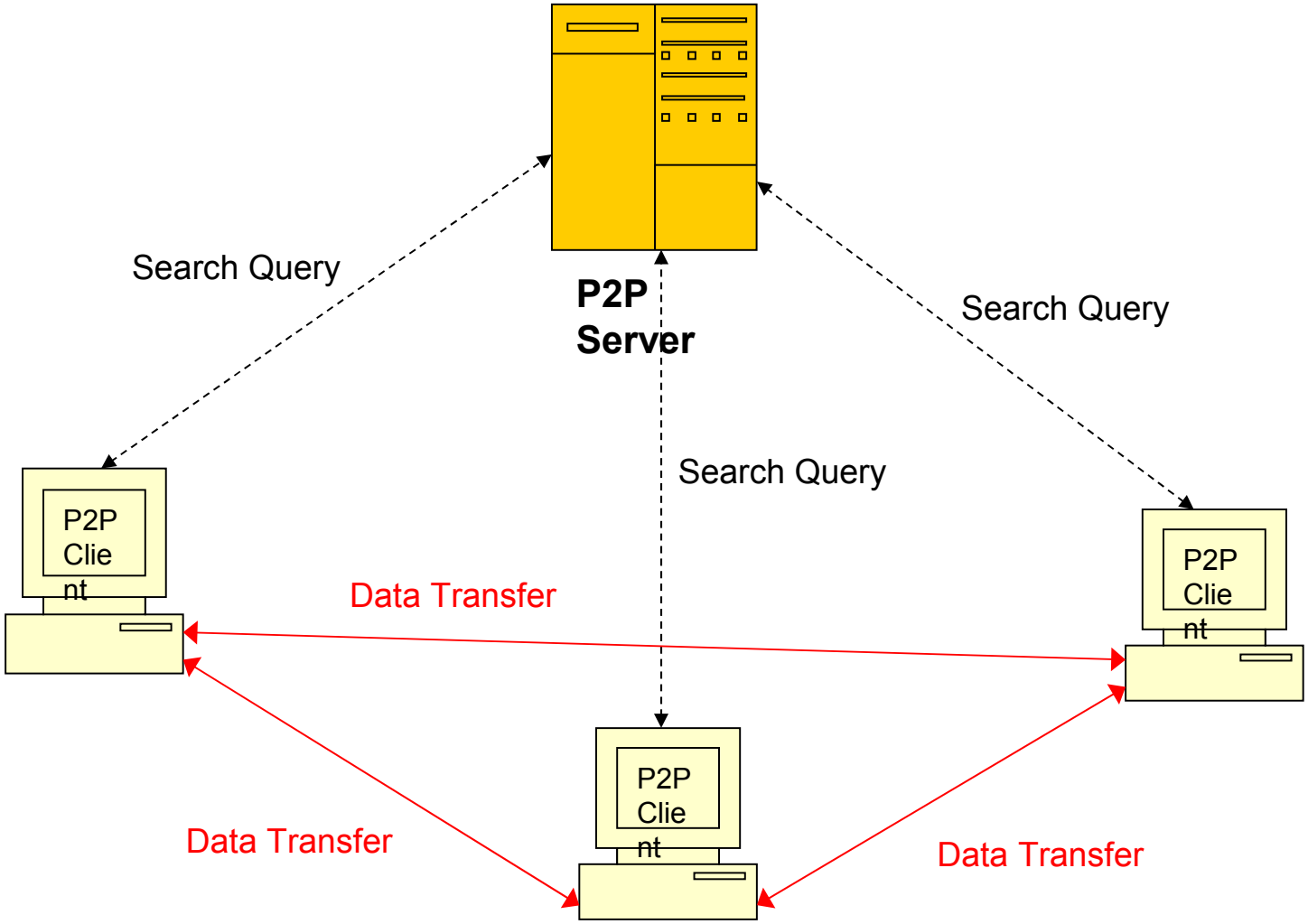
Classificatore fwmark

- tc filter add dev eth1 protocol ip parent 1:0 prio 1 handle 11 fw flowid 1:11
- tc filter add dev eth0 protocol ip parent 1:0 prio 1 handle 11 fw flowid 1:11
- tc filter add dev eth1 protocol ip parent 1:0 prio 1 handle 12 fw flowid 1:12
- tc filter add dev eth0 protocol ip parent 1:0 prio 1 handle 12 fw flowid 1:12

Classificazione del Traffico

- Il problema più grosso quando si vuole implementare il Traffic Shaping è riuscire a classificare il traffico, poiché alcuni protocolli non utilizzano porte TCP/UDP fisse
- Spesso non si può classificare neanche per indirizzo IP poiché i flussi di dati non sono indirizzati verso dei server predicibili, ma avvengono tra host che cambiano velocemente (P2P)

Modello Peer to Peer di prima generazione



Filtri Layer 7

- Una soluzione al problema della classificazione del traffico sono i filtri a livello applicativo (Layer 7 del modello OSI)
- A questo livello non si guarda agli indirizzi IP e alle porte TCP/UDP ma al payload dei pacchetti
  - Anche se un programma cambia dinamicamente le porte di connessione o utilizza porte di servizi standard (HTTP, FTP, ...) viene comunque individuato correttamente

Filtri Layer 7 utilizzati

- L7-filter (http://l7-filter.sourceforge.net/)
  - Sono un modulo aggiuntivo del NetFilter di Linux e quindi vengono impostati tramite iptables
  - Le signature per l'individuazione del traffico sono delle normali Regular Expression contenute all'interno di file ASCII
    - I pattern sono personalizzabili
    - Possono essere aggiornate online scaricando un tar file
  - Utilizzano automaticamente il sistema di Connection Tracking di Linux
- IPP2P (http://www.ipp2p.org/)
  - E' una patch del NetFilter di Linux
  - Individuano soltanto traffico di tipo Peer to Peer per filesharing
  - Non includono internamente la gestione del Connection Tracking

Esempi di utilizzo di L7-filter

Filtri VoIP

- iptables -t mangle -A FORWARD -m layer7 --l7proto h323 -j MARK --set-mark 12
- iptables -t mangle -A FORWARD -m layer7 --l7proto sip -j MARK --set-mark 12
- iptables -t mangle -A FORWARD -m layer7 --l7proto msnmessenger -j MARK --set-mark 12
- iptables -t mangle -A FORWARD -m layer7 --l7proto skypetoskype -j MARK --set-mark 12
- iptables -t mangle -A FORWARD -m layer7 --l7proto skypeout -j MARK --set-mark 12

Filtri P2P

- iptables -t mangle -A FORWARD -m layer7 --l7proto edonkey -j MARK --set-mark 11
- iptables -t mangle -A FORWARD -m layer7 --l7proto bittorrent -j MARK --set-mark 11
- iptables -t mangle -A FORWARD -m layer7 --l7proto napster -j MARK --set-mark 11
- iptables -t mangle -A FORWARD -m layer7 --l7proto fasttrack -j MARK --set-mark 11
- iptables -t mangle -A FORWARD -m layer7 --l7proto gnutella -j MARK --set-mark 11
- iptables -t mangle -A FORWARD -m layer7 --l7proto directconnect -j MARK --set-mark 11

Esempi di utilizzo di IPP2P

- IPP2P diversamente da L7-filter non gestisce internamente il **Connection Tracking**

  - iptables -t mangle -A FORWARD -j CONNMARK --restore-mark
  - iptables -t mangle -A FORWARD -m mark ! --mark 0 -j ACCEPT
  - iptables -t mangle -A FORWARD -m ipp2p --debug --ipp2p -j MARK --set-mark 11
  - iptables -t mangle -A FORWARD -m mark --mark 11 -j CONNMARK --save-mark

Compilazione del Kernel

- cd /root
- tar xvfz netfilter-layer7-v2.9.tar.gz
- cd /usr/src/kernels
- tar xvfj linux-2.6.19.7.tar.bz2
- cd /usr/src/kernels/linux-2.6.19.7/
- patch -p1 < /root/netfilter-layer7-v2.9/kernel-2.6.18-2.6.19-layer7-2.9.patch
- cp /usr/src/kernels/2.6.9-42.0.10.EL-x86_64/.config .
- make oldconfig (accettare i default)
- make menuconfig
  - CONFIG_NET_SCH_HTB=m
  - CONFIG_BRIDGE=m
  - CONFIG_NETFILTER_XTABLES=m (abilitare anche tutti i moduli correlati)
  - CONFIG_IP_NF_CONNTRACK=m
  - CONFIG_IP_NF_CT_ACCT=m
  - CONFIG_IP_NF_FTP=m
  - CONFIG_IP_NF_IRC=m
  - CONFIG_IP_NF_PPTP=m
  - CONFIG_IP_NF_H323=m
  - CONFIG_IP_NF_SIP=m
  - CONFIG_IP_NF_IPTABLES=m
  - CONFIG_IP_NF_MATCH_LAYER7=m
- make && make modules_install && make install

Ricompilazione di IPTABLES

- rpm -e iptables
- wget ftp://ftp.netfilter.org/pub/iptables/iptables-1.3.7.tar.bz2
- tar xvfj iptables-1.3.7.tar.bz2
- cd iptables-1.3.7
- patch -p1 < /root/netfilter-layer7-v2.9/iptables-layer7-2.9.patch
- chmod 755 extensions/.layer7-test
- make KERNEL_DIR=/usr/src/kernels/linux-2.6.19.7/
- make install KERNEL_DIR=/usr/src/kernels/linux-2.6.19.7/

Installazione dei Pattern Protocol

- Le signature vengono aggiornate periodicamente e spesso sono il frutto della collaborazione degli utilizzatori di L7-Filter
  - wget http://downloads.sourceforge.net/l7-filter/l7-protocols-2007-01-14.tar.gz?modtime=1168818775&big_mirror=0
  - cd /etc
  - tar xvfz /root/l7-protocols-2007-01-14.tar.gz
  - mv l7-protocols-2007-01-14 l7-protocols
- Le signature vengono suddivise nelle directory
  - /etc/l7-protocols/protocols
  - /etc/l7-protocols/file_types
  - /etc/l7-protocols/malware
  - /etc/l7-protocols/extra

Esempio di Signature Layer 7

```
# SIP - Session Initiation Protocol - Internet telephony - RFC 3261
# Pattern attributes: ok fast fast
# Protocol groups: voip ietf_proposed_standard
# Wiki: http://www.protocolinfo.org/wiki/SIP
#
# This pattern has been tested with the Ubiquity SIP user agent.
#
# Thanks to Ankit Desai for this pattern.
#
# This pattern is based on SIP request format as per RFC 3261. I'm not
# sure about the version part. The RFC doesn't say anything about it, so
# I have allowed version ranging from 0.x to 2.x.

#Request-Line  =  Method SP Request-URI SP SIP-Version CRLF
sip
^(invite|register|cancel) sip[\x09-\x0d -~]*sip/[0-2]\.[0-9]
```

Configurazione dell'interfaccia Bridge

- yum install bridge-utils

- brctl addbr br0
- brctl addif br0 eth0
- brctl addif br0 eth1
- ifconfig br0 10.10.254.252 netmask 255.255.255.248

- E' comodo avere una terza interfaccia di rete collegata alla LAN per facilitare l'accesso remoto

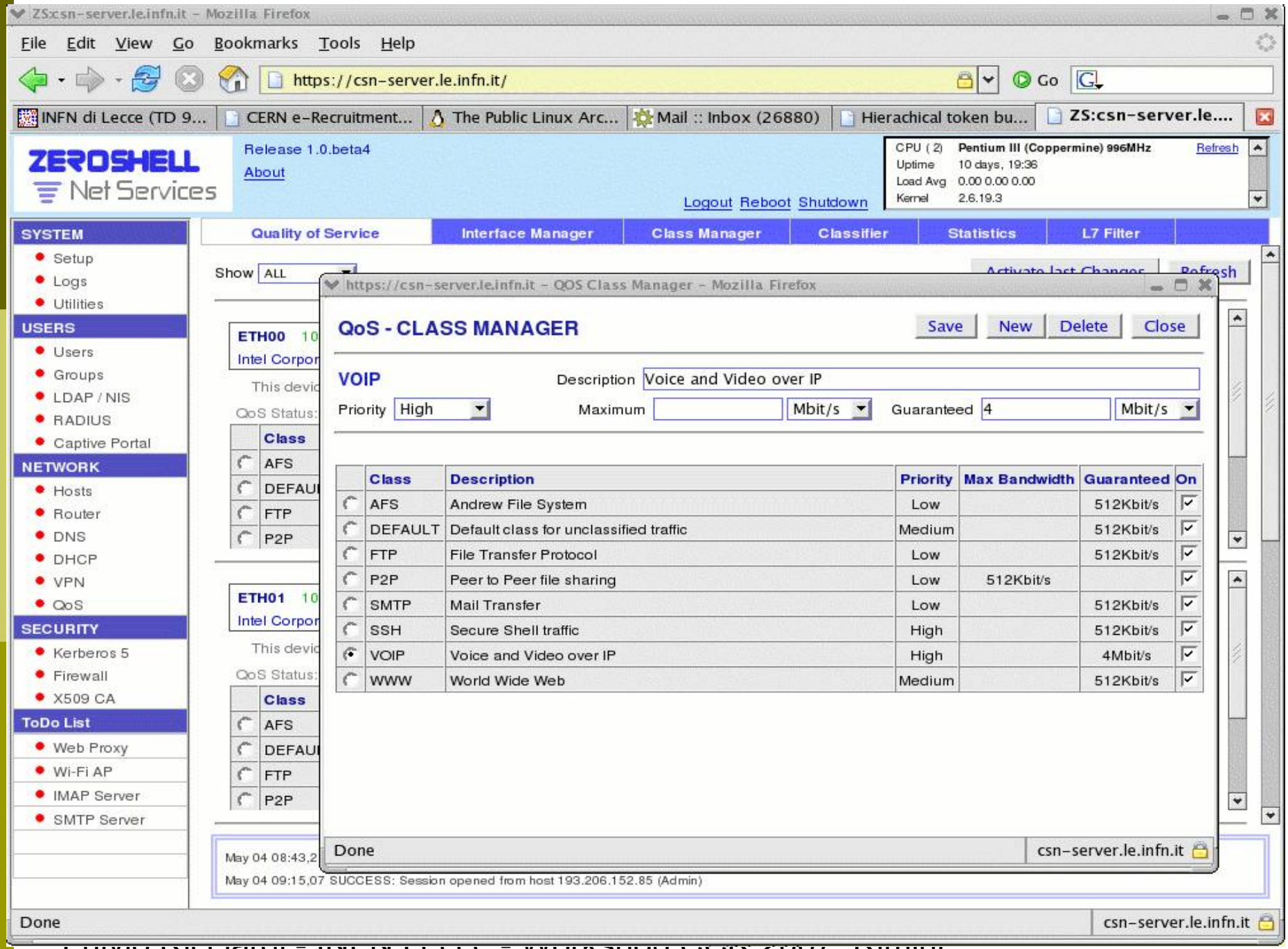
Alcune GUI per la gestione del traffic shaping

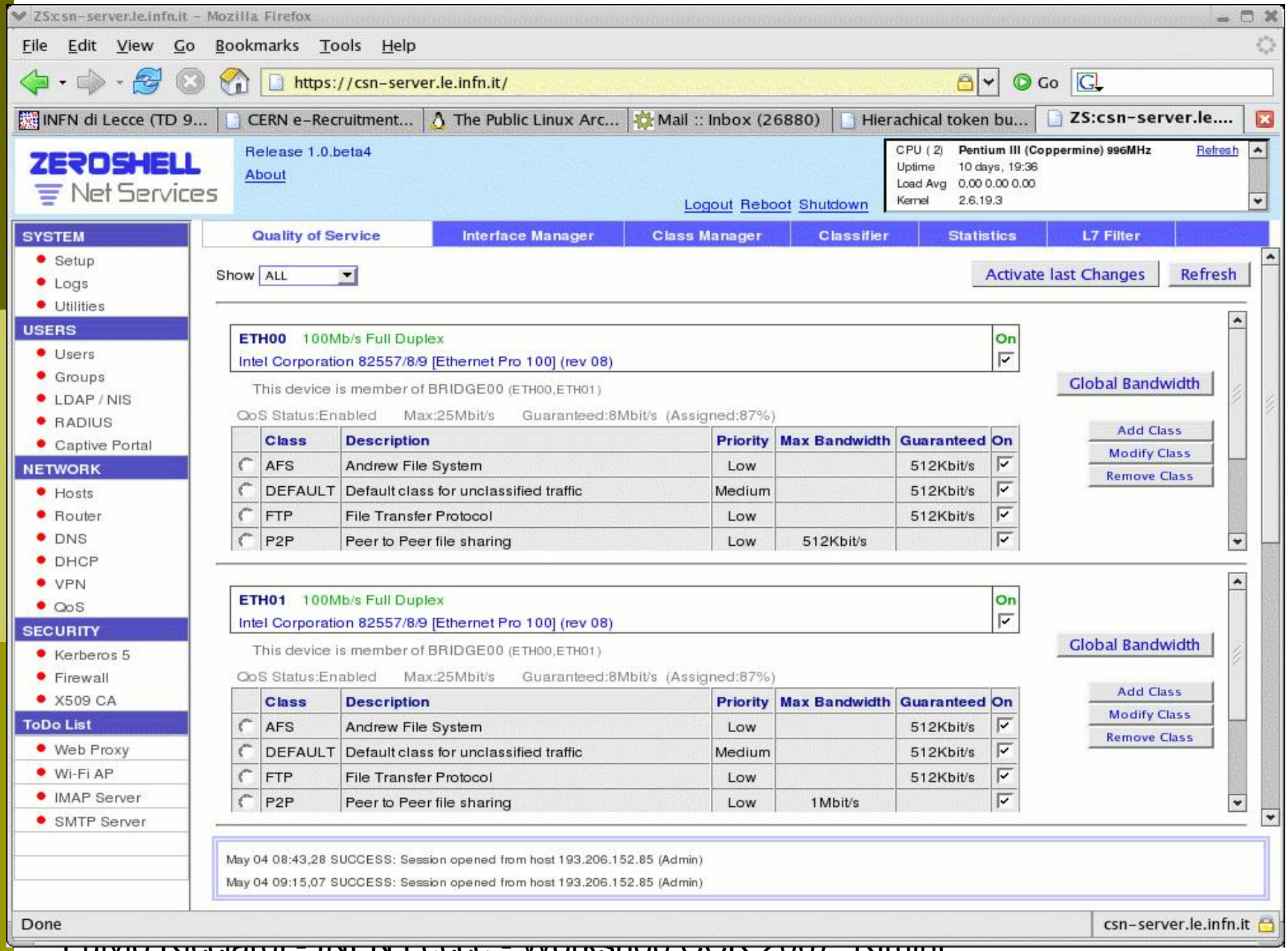
Dal sito di L7-Filter

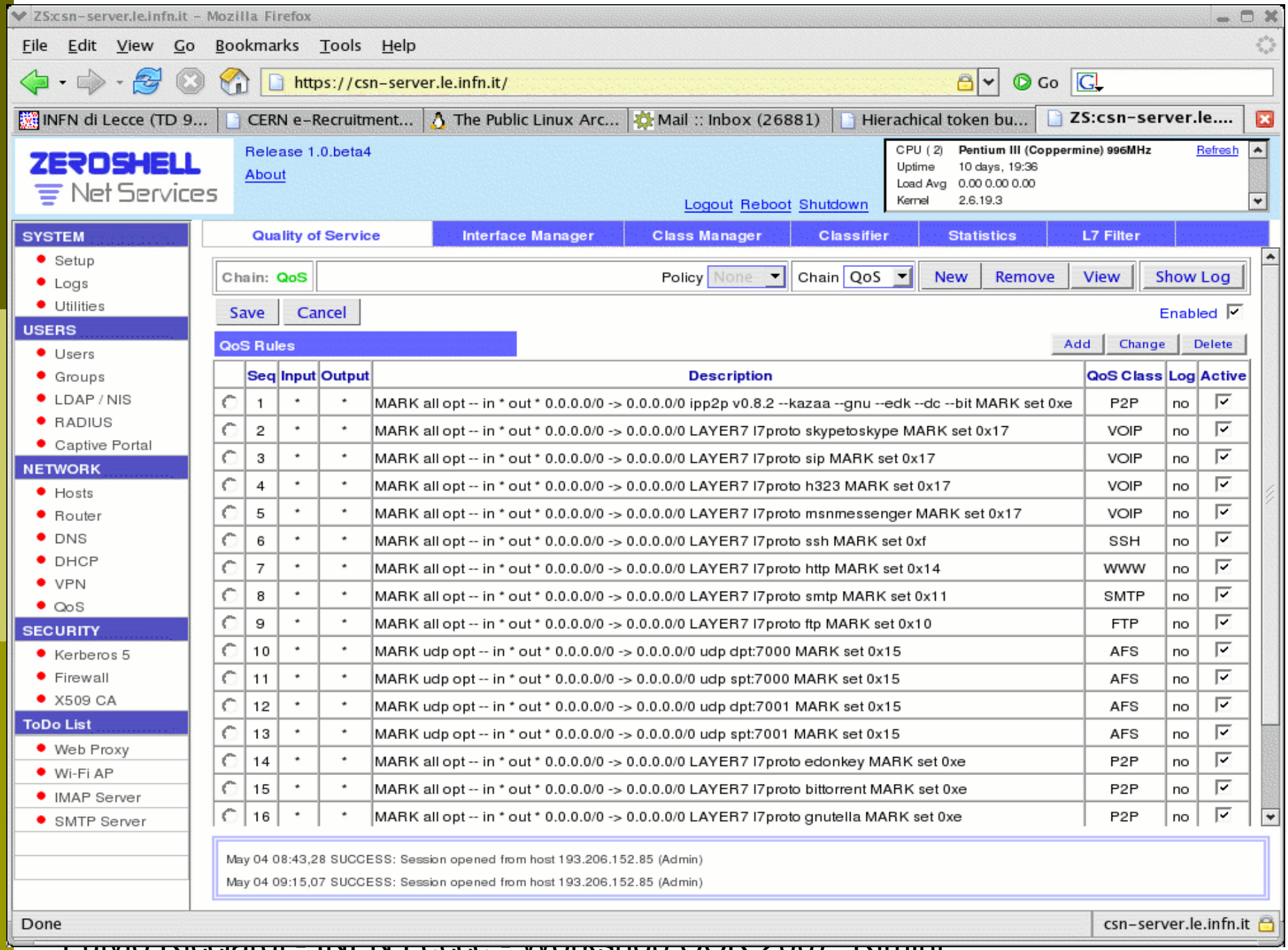
- ZeroShell
- QOS-L7
- NuFace
- MasterShaper
- k-shaper
- DD-WRT

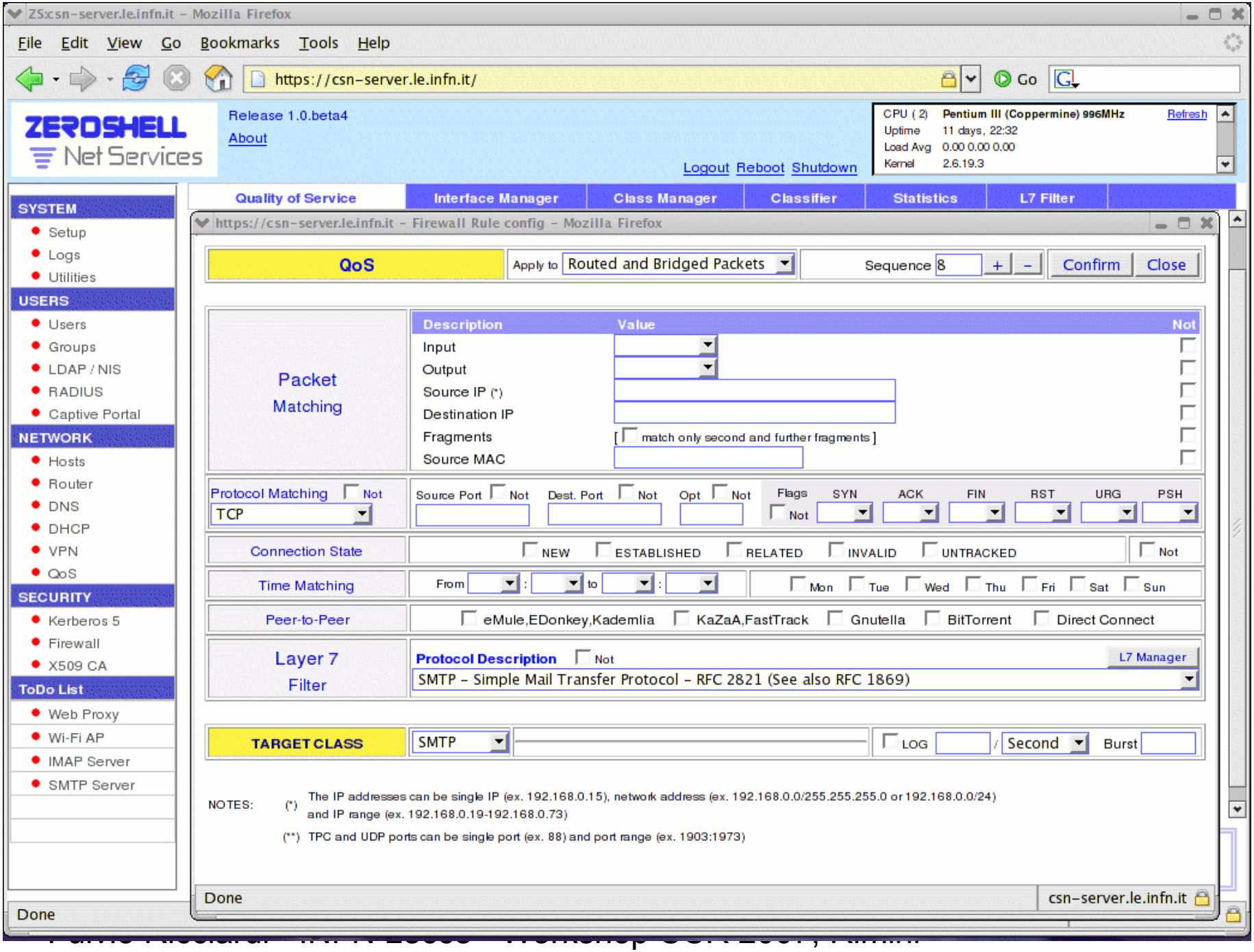
Traffic Shaping utilizzando ZeroShell

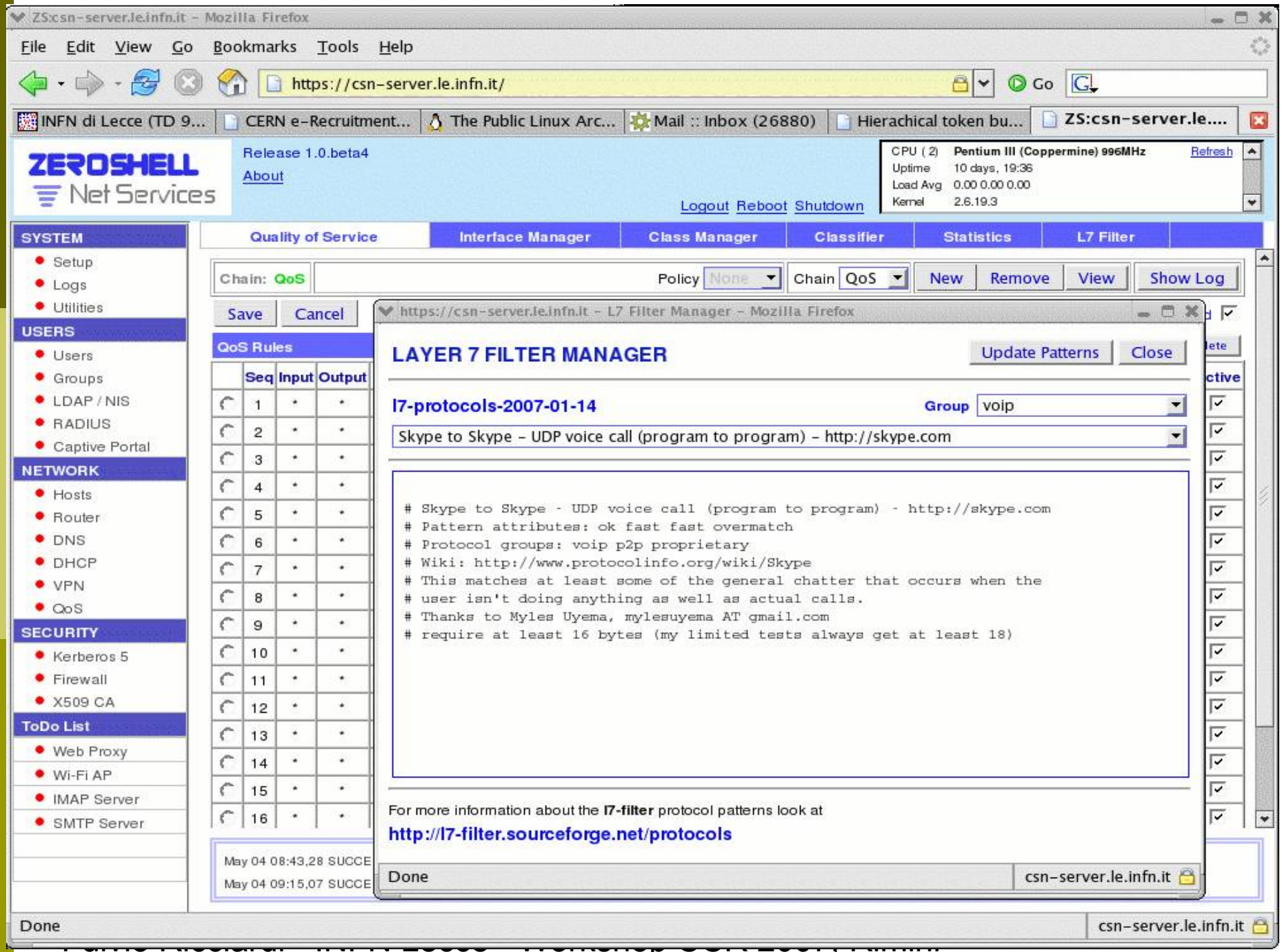
- ZeroShell è un sistema Linux disponibile nel formato di Live CD e CompactFlash
- E' amministrabile completamente via Web Interface
- E' orientato ai Server ed Embedded Device che forniscono Servizi di Rete
- Contiene solo il software indispensabile a fornire tali servizi, infatti occupa meno di 100MB
- E' disponile all'URL http://www.zeroshell.net

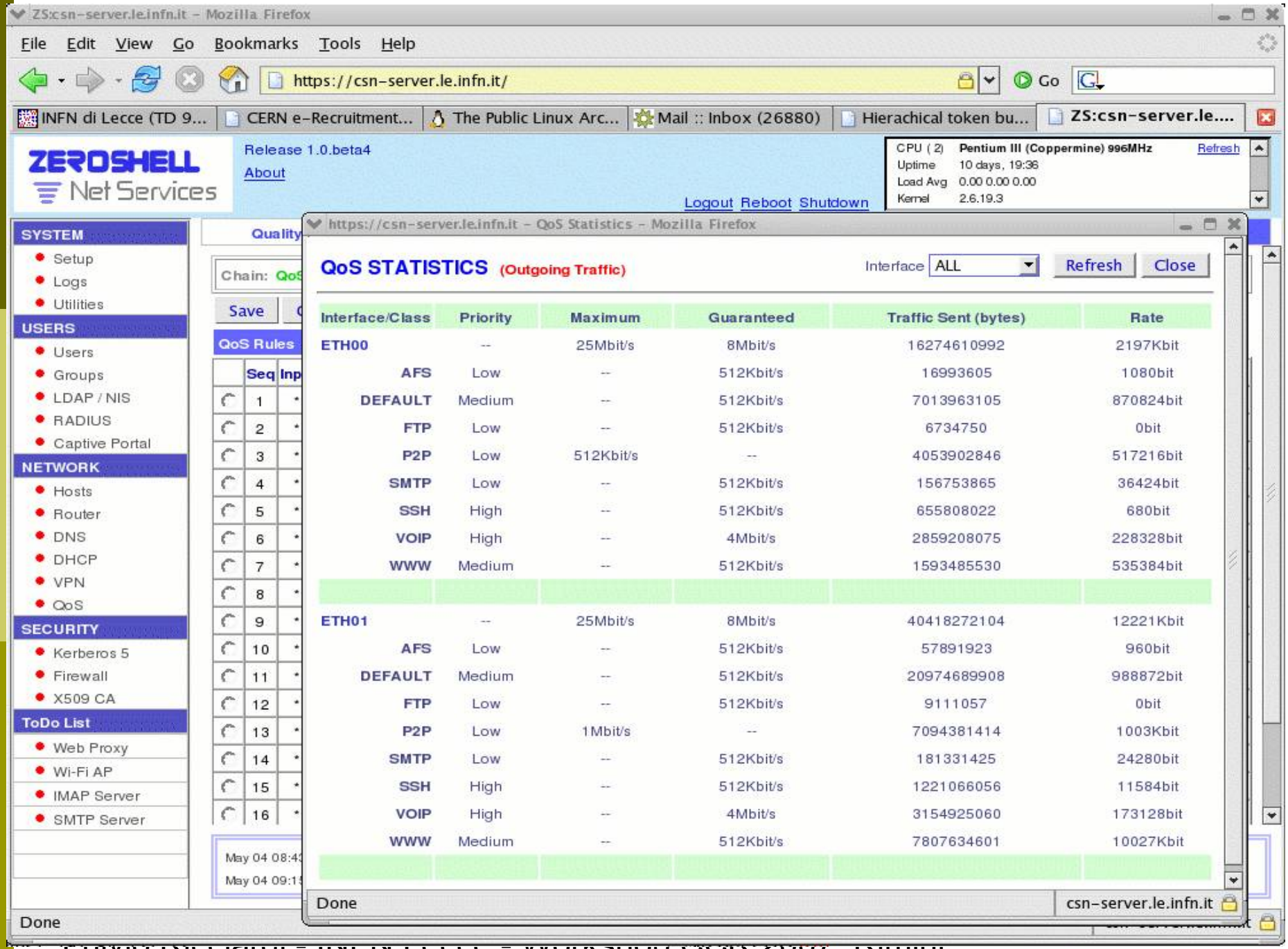

ZS:csn-server.le.infn.it - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
https://csn-server.le.infn.it/
Go
INFN di Lecce (TD 9...
CERN e-Recruitment...
The Public Linux Arc...
Mail :: Inbox (26880)
Hierachical token bu...
ZS:csn-server.le....
ZEROSHELL
Net Services
Release 1.0.beta4
About
Logout Reboot Shutdown
CPU (2) Pentium III (Coppermine) 996MHz
Refresh
Uptime 10 days, 19:36
Load Avg 0.00 0.00 0.00
Kernel 2.6.19.3
SYSTEM
Setup
Logs
Utilities
USERS
Users
Groups
LDAP / NIS
RADIUS
Captive Portal
NETWORK
Hosts
Router
DNS
DHCP
VPN
QoS
SECURITY
Kerberos 5
Firewall
X509 CA
ToDo List
Web Proxy
Wi-Fi AP
IMAP Server
SMTP Server
Quality of Service
Interface Manager
Class Manager
Classifier
Statistics
L7 Filter
Show ALL
Activate last Changes
Refresh
ETH00 10
Intel Corpor
This devic
QoS Status:
Class
AFS
DEFAU
FTP
P2P
ETH01 10
Intel Corpor
This devic
QoS Status:
Class
AFS
DEFAU
FTP
P2P
May 04 08:43,2
May 04 09:15,07 SUCCESS: Session opened from host 193.206.152.85 (Admin)
Done
csn-server.le.infn.it
https://csn-server.le.infn.it - QOS Class Manager - Mozilla Firefox
QoS - CLASS MANAGER
Save
New
Delete
Close
VOIP
Description Voice and Video over IP
Priority High
Maximum
Mbit/s
Guaranteed 4
Mbit/s
Class
Description
Priority
Max Bandwidth
Guaranteed
On
AFS Andrew File System Low 512Kbit/s
DEFAULT Default class for unclassified traffic Medium 512Kbit/s
FTP File Transfer Protocol Low 512Kbit/s
P2P Peer to Peer file sharing Low 512Kbit/s
SMTP Mail Transfer Low 512Kbit/s
SSH Secure Shell traffic High 512Kbit/s
VOIP Voice and Video over IP High 4Mbit/s
WWW World Wide Web Medium 512Kbit/s
Done
csn-server.le.infn.it
Done
csn-server.le.infn.it


ZS:csn-server.le.infn.it - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
https://csn-server.le.infn.it/
Go
INFN di Lecce (TD 9...
CERN e-Recruitment...
The Public Linux Arc...
Mail :: Inbox (26880)
Hierachical token bu...
ZS:csn-server.le....
ZEROSHELL
Net Services
Release 1.0.beta4
About
Logout Reboot Shutdown
CPU (2) Pentium III (Coppermine) 996MHz
Refresh
Uptime 10 days, 19:36
Load Avg 0.00 0.00 0.00
Kernel 2.6.19.3
SYSTEM
Setup
Logs
Utilities
USERS
Users
Groups
LDAP / NIS
RADIUS
Captive Portal
NETWORK
Hosts
Router
DNS
DHCP
VPN
QoS
SECURITY
Kerberos 5
Firewall
X509 CA
ToDo List
Web Proxy
Wi-Fi AP
IMAP Server
SMTP Server
Quality of Service
Interface Manager
Class Manager
Classifier
Statistics
L7 Filter
Show ALL
Activate last Changes
Refresh
ETH00 100Mb/s Full Duplex
Intel Corporation 82557/8/9 [Ethernet Pro 100] (rev 08)
On
This device is member of BRIDGE00 (ETH00,ETH01)
Global Bandwidth
QoS Status:Enabled Max:25Mbit/s Guaranteed:8Mbit/s (Assigned:87%)
Add Class
Modify Class
Remove Class
Class Description Priority Max Bandwidth Guaranteed On
AFS Andrew File System Low 512Kbit/s
DEFAULT Default class for unclassified traffic Medium 512Kbit/s
FTP File Transfer Protocol Low 512Kbit/s
P2P Peer to Peer file sharing Low 512Kbit/s
ETH01 100Mb/s Full Duplex
Intel Corporation 82557/8/9 [Ethernet Pro 100] (rev 08)
On
This device is member of BRIDGE00 (ETH00,ETH01)
Global Bandwidth
QoS Status:Enabled Max:25Mbit/s Guaranteed:8Mbit/s (Assigned:87%)
Add Class
Modify Class
Remove Class
Class Description Priority Max Bandwidth Guaranteed On
AFS Andrew File System Low 512Kbit/s
DEFAULT Default class for unclassified traffic Medium 512Kbit/s
FTP File Transfer Protocol Low 512Kbit/s
P2P Peer to Peer file sharing Low 1Mbit/s
May 04 08:43,28 SUCCESS: Session opened from host 193.206.152.85 (Admin)
May 04 09:15,07 SUCCESS: Session opened from host 193.206.152.85 (Admin)
Done
csn-server.le.infn.it


ZS:csn-server.le.infn.it - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
https://csn-server.le.infn.it/
Go
INFN di Lecce (TD 9...
CERN e-Recruitment...
The Public Linux Arc...
Mail :: Inbox (26881)
Hierachical token bu...
ZS:csn-server.le....
ZEROSHELL
Net Services
Release 1.0.beta4
About
Logout Reboot Shutdown
CPU (2) Pentium III (Coppermine) 996MHz
Refresh
Uptime 10 days, 19:36
Load Avg 0.00 0.00 0.00
Kernel 2.6.19.3
SYSTEM
Setup
Logs
Utilities
USERS
Users
Groups
LDAP / NIS
RADIUS
Captive Portal
NETWORK
Hosts
Router
DNS
DHCP
VPN
QoS
SECURITY
Kerberos 5
Firewall
X509 CA
ToDo List
Web Proxy
Wi-Fi AP
IMAP Server
SMTP Server
Quality of Service
Interface Manager
Class Manager
Classifier
Statistics
L7 Filter
Chain: QoS
Policy None
Chain QoS
New
Remove
View
Show Log
Save
Cancel
Enabled
QoS Rules
Add
Change
Delete
Seq Input Output Description QoS Class Log Active
1 * * MARK all opt -- in * out * 0.0.0.0/0 -> 0.0.0.0/0 ipp2p v0.8.2 --kazaa --gnu --edk --dc --bit MARK set 0xe P2P no
2 * * MARK all opt -- in * out * 0.0.0.0/0 -> 0.0.0.0/0 LAYER7 l7proto skypetoskype MARK set 0x17 VOIP no
3 * * MARK all opt -- in * out * 0.0.0.0/0 -> 0.0.0.0/0 LAYER7 l7proto sip MARK set 0x17 VOIP no
4 * * MARK all opt -- in * out * 0.0.0.0/0 -> 0.0.0.0/0 LAYER7 l7proto h323 MARK set 0x17 VOIP no
5 * * MARK all opt -- in * out * 0.0.0.0/0 -> 0.0.0.0/0 LAYER7 l7proto msnmessenger MARK set 0x17 VOIP no
6 * * MARK all opt -- in * out * 0.0.0.0/0 -> 0.0.0.0/0 LAYER7 l7proto ssh MARK set 0xf SSH no
7 * * MARK all opt -- in * out * 0.0.0.0/0 -> 0.0.0.0/0 LAYER7 l7proto http MARK set 0x14 WWW no
8 * * MARK all opt -- in * out * 0.0.0.0/0 -> 0.0.0.0/0 LAYER7 l7proto smtp MARK set 0x11 SMTP no
9 * * MARK all opt -- in * out * 0.0.0.0/0 -> 0.0.0.0/0 LAYER7 l7proto ftp MARK set 0x10 FTP no
10 * * MARK udp opt -- in * out * 0.0.0.0/0 -> 0.0.0.0/0 udp dpt:7000 MARK set 0x15 AFS no
11 * * MARK udp opt -- in * out * 0.0.0.0/0 -> 0.0.0.0/0 udp spt:7000 MARK set 0x15 AFS no
12 * * MARK udp opt -- in * out * 0.0.0.0/0 -> 0.0.0.0/0 udp dpt:7001 MARK set 0x15 AFS no
13 * * MARK udp opt -- in * out * 0.0.0.0/0 -> 0.0.0.0/0 udp spt:7001 MARK set 0x15 AFS no
14 * * MARK all opt -- in * out * 0.0.0.0/0 -> 0.0.0.0/0 LAYER7 l7proto edonkey MARK set 0xe P2P no
15 * * MARK all opt -- in * out * 0.0.0.0/0 -> 0.0.0.0/0 LAYER7 l7proto bittorrent MARK set 0xe P2P no
16 * * MARK all opt -- in * out * 0.0.0.0/0 -> 0.0.0.0/0 LAYER7 l7proto gnutella MARK set 0xe P2P no
May 04 08:43,28 SUCCESS: Session opened from host 193.206.152.85 (Admin)
May 04 09:15,07 SUCCESS: Session opened from host 193.206.152.85 (Admin)
Done
csn-server.le.infn.it


ZS:csn-server.le.infn.it - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
https://csn-server.le.infn.it/
Go
ZEROSHELL
Net Services
Release 1.0.beta4
About
Logout Reboot Shutdown
CPU (2) Pentium III (Coppermine) 996MHz Refresh
Uptime 11 days, 22:32
Load Avg 0.00 0.00 0.00
Kernel 2.6.19.3
SYSTEM
Setup
Logs
Utilities
USERS
Users
Groups
LDAP / NIS
RADIUS
Captive Portal
NETWORK
Hosts
Router
DNS
DHCP
VPN
QoS
SECURITY
Kerberos 5
Firewall
X509 CA
ToDo List
Web Proxy
Wi-Fi AP
IMAP Server
SMTP Server
Quality of Service
Interface Manager
Class Manager
Classifier
Statistics
L7 Filter
https://csn-server.le.infn.it - Firewall Rule config - Mozilla Firefox
QoS
Apply to Routed and Bridged Packets
Sequence 8 + -
Confirm Close
Packet Matching
Description Value Not
Input
Output
Source IP (*)
Destination IP
Fragments [match only second and further fragments]
Source MAC
Protocol Matching Not
TCP
Source Port Not
Dest. Port Not
Opt Not
Flags Not SYN ACK FIN RST URG PSH
Connection State
NEW ESTABLISHED RELATED INVALID UNTRACKED Not
Time Matching
From : to :
Mon Tue Wed Thu Fri Sat Sun
Peer-to-Peer
eMule,EDonkey,Kademlia KaZaA,FastTrack Gnutella BitTorrent Direct Connect
Layer 7 Filter
Protocol Description Not
L7 Manager
SMTP - Simple Mail Transfer Protocol - RFC 2821 (See also RFC 1869)
TARGET CLASS
SMTP
LOG / Second Burst
NOTES: (*) The IP addresses can be single IP (ex. 192.168.0.15), network address (ex. 192.168.0.0/255.255.255.0 or 192.168.0.0/24) and IP range (ex. 192.168.0.19-192.168.0.73)
(**) TPC and UDP ports can be single port (ex. 88) and port range (ex. 1903:1973)
Done
csn-server.le.infn.it
Done


ZS:csn-server.le.infn.it - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
https://csn-server.le.infn.it/
INFN di Lecce (TD 9...
CERN e-Recruitment...
The Public Linux Arc...
Mail :: Inbox (26880)
Hierachical token bu...
ZS:csn-server.le....
ZEROSHELL
Net Services
Release 1.0.beta4
About
Logout Reboot Shutdown
CPU (2) Pentium III (Coppermine) 996MHz
Refresh
Uptime 10 days, 19:36
Load Avg 0.00 0.00 0.00
Kernel 2.6.19.3
SYSTEM
Setup
Logs
Utilities
USERS
Users
Groups
LDAP / NIS
RADIUS
Captive Portal
NETWORK
Hosts
Router
DNS
DHCP
VPN
QoS
SECURITY
Kerberos 5
Firewall
X509 CA
ToDo List
Web Proxy
Wi-Fi AP
IMAP Server
SMTP Server
Quality of Service
Interface Manager
Class Manager
Classifier
Statistics
L7 Filter
Chain: QoS
Policy None
Chain QoS
New
Remove
View
Show Log
Save
Cancel
QoS Rules
Seq
Input
Output
May 04 08:43,28 SUCCE
May 04 09:15,07 SUCCE
https://csn-server.le.infn.it - L7 Filter Manager - Mozilla Firefox
LAYER 7 FILTER MANAGER
Update Patterns
Close
l7-protocols-2007-01-14
Group voip
Skype to Skype - UDP voice call (program to program) - http://skype.com
Skype to Skype - UDP voice call (program to program) - http://skype.com
Pattern attributes: ok fast fast overmatch
Protocol groups: voip p2p proprietary
Wiki: http://www.protocolinfo.org/wiki/Skype
This matches at least some of the general chatter that occurs when the
user isn't doing anything as well as actual calls.
Thanks to Myles Uyema, mylesuyema AT gmail.com
require at least 16 bytes (my limited tests always get at least 18)
For more information about the l7-filter protocol patterns look at
http://l7-filter.sourceforge.net/protocols
Done
csn-server.le.infn.it
Done
csn-server.le.infn.it


ZS:csn-server.le.infn.it - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
https://csn-server.le.infn.it/
Go
INFN di Lecce (TD 9...
CERN e-Recruitment...
The Public Linux Arc...
Mail :: Inbox (26880)
Hierachical token bu...
ZS:csn-server.le....
ZEROSHELL
Net Services
Release 1.0.beta4
About
Logout Reboot Shutdown
CPU (2) Pentium III (Coppermine) 996MHz
Refresh
Uptime 10 days, 19:36
Load Avg 0.00 0.00 0.00
Kernel 2.6.19.3
SYSTEM
Setup
Logs
Utilities
USERS
Users
Groups
LDAP / NIS
RADIUS
Captive Portal
NETWORK
Hosts
Router
DNS
DHCP
VPN
QoS
SECURITY
Kerberos 5
Firewall
X509 CA
ToDo List
Web Proxy
Wi-Fi AP
IMAP Server
SMTP Server
Quality
Chain: QoS
Save
QoS Rules
Seq
Inp
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
May 04 08:43
May 04 09:15
Done
https://csn-server.le.infn.it - QoS Statistics - Mozilla Firefox
QoS STATISTICS (Outgoing Traffic)
Interface ALL
Refresh
Close
Interface/Class | Priority | Maximum | Guaranteed | Traffic Sent (bytes) | Rate
ETH00 -- 25Mbit/s 8Mbit/s 16274610992 2197Kbit
AFS Low -- 512Kbit/s 16993605 1080bit
DEFAULT Medium -- 512Kbit/s 7013963105 870824bit
FTP Low -- 512Kbit/s 6734750 0bit
P2P Low 512Kbit/s -- 4053902846 517216bit
SMTP Low -- 512Kbit/s 156753865 36424bit
SSH High -- 512Kbit/s 655808022 680bit
VOIP High -- 4Mbit/s 2859208075 228328bit
WWW Medium -- 512Kbit/s 1593485530 535384bit
ETH01 -- 25Mbit/s 8Mbit/s 40418272104 12221Kbit
AFS Low -- 512Kbit/s 57891923 960bit
DEFAULT Medium -- 512Kbit/s 20974689908 988872bit
FTP Low -- 512Kbit/s 9111057 0bit
P2P Low 1Mbit/s -- 7094381414 1003Kbit
SMTP Low -- 512Kbit/s 181331425 24280bit
SSH High -- 512Kbit/s 1221066056 11584bit
VOIP High -- 4Mbit/s 3154925060 173128bit
WWW Medium -- 512Kbit/s 7807634601 10027Kbit
Done
csn-server.le.infn.it
Done

Riferimenti su Web

- http://l7-filter.sourceforge.net/
  - Sito ufficiale del progetto L7-Filter
- http://www.ipp2p.org/
  - Sito ufficiale della patch per iptables IPP2P
- http://lartc.org/howto/
  - Linux Advanced Routing & Traffic Control
- http://www.zeroshell.net/qos/
  - HowTo per la realizzazione di un Traffic Shaping Bridge utilizzando ZeroShell