Esempio di utilizzo di zeroshell quale firewall , proxi server, dhcp e backup

Configurazione hardware

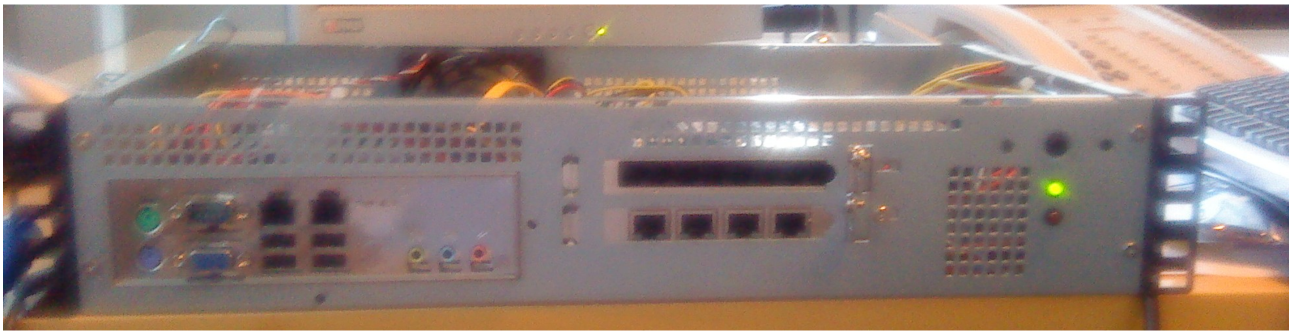
Utilizzando un case rack 19 pollici profondità 300 mm e 1,5 unità di altezza ho inserito :

- alimentatore integrato a 220 V ,
- una scheda Via Epia LT fanless,
- una ram da 512 mb ,
- un disco flash ide da 2 gb ,
- una scheda di rete con 4 porte lan prodotta da Soekris ,
- un adattatore per schede pcmcia

ho ottenuto un prodotto di ridotte dimensioni installabile all' interno degli armadi 19 pollici .

Le capacità complessive sono :

- 6 porte lan ETH0 sino a ETH5
- 1 slot per modem pcmcia umts , gprs



Architettura della rete

La architettura del sistema proposto come esempio per una piccola rete aziendale ricalca grosso modo la scelta base di IPCOP ovvero:

- ETH0 segmento wan (connessioni adsl verso interenet o connessioni esterne)
- ETH1 segmento server (area in cui si trovano tutti i server)
- ETH2 segmento utenza uffici (area uffici amministrativi e commerciali)
- ETH3 segmento utenza area tecnica e produzione (area uffici tecnici e produzione)
- ETH4 segmento access point x connessione wifi (connesione portatili)
- ETH5 segmento spare ((utilizzabile per suddividere i server interni da quelli accessibili da wan

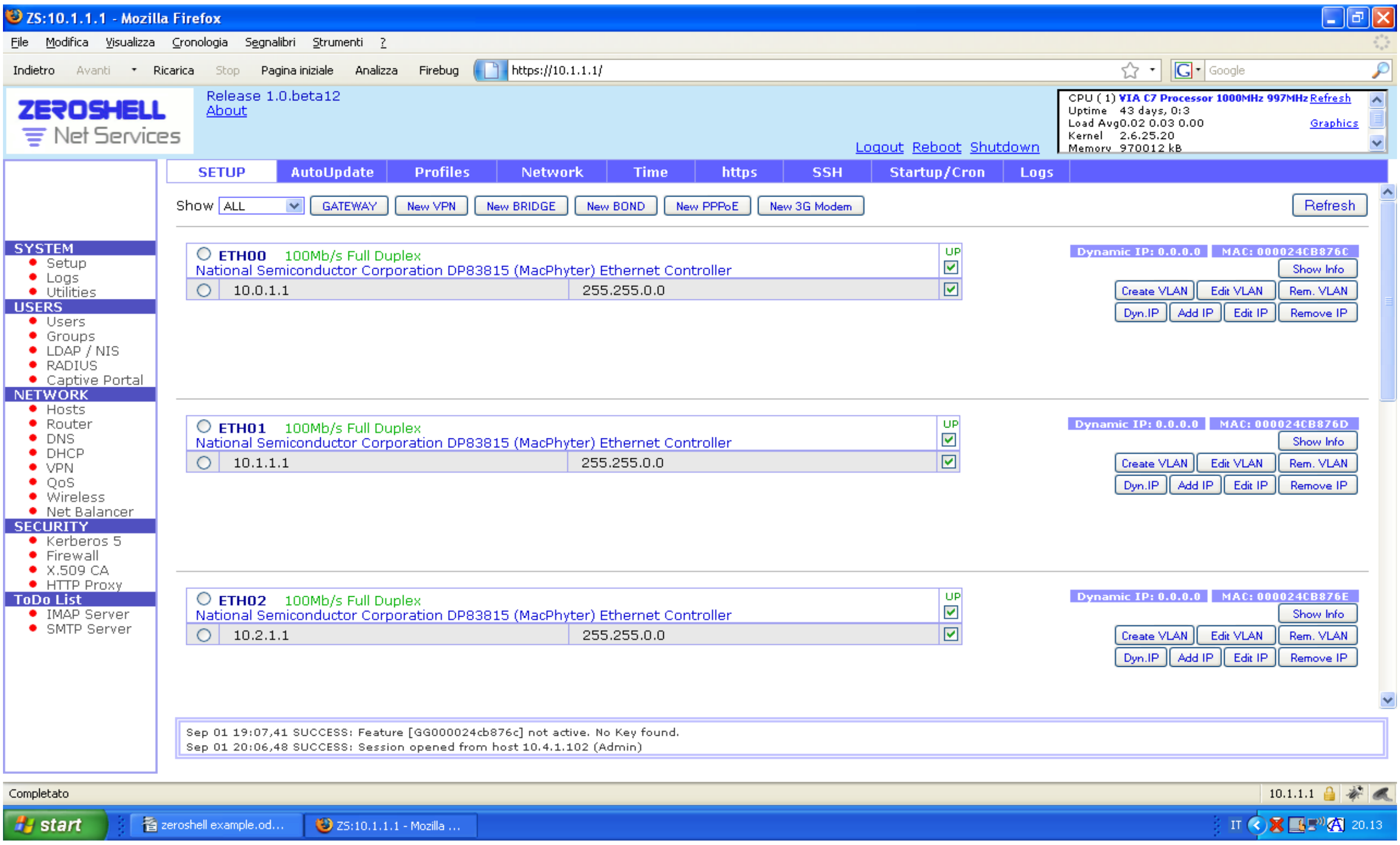
Configurazione Zeroshell

Network

A tutte le varie porte lan è stato assegnato un indirizzo ip secondo la tabella seguente:

- ETH0 10.0.1.1
- ETH1 10.1.1.1
- ETH2 10.2.1.1
- ETH3 10.3.1.1
- ETH4 10.4.1.1
- ETH5 nessun indirizzo

definisco le mask a 255.255.0.0



```
CPU ( 1) VIA C7 Processor 1000MHz 997MHz
Uptime    43 days, 0:3
Load Avg0.02 0.03 0.00
Kernel    2.6.25.20
Memory  970012 kB
```

○ ETH00 100Mb/s Full Duplex
National Semiconductor Corporation DP83815 (MacPhyter) Ethernet Controller ☑

○	10.0.1.1	255.255.0.0	☑

Dynamic IP: 0.0.0.0 MAC: 000024CB876C

○ ETH01 100Mb/s Full Duplex
National Semiconductor Corporation DP83815 (MacPhyter) Ethernet Controller ☑

○	10.1.1.1	255.255.0.0	☑

Dynamic IP: 0.0.0.0 MAC: 000024CB876D

○ ETH02 100Mb/s Full Duplex
National Semiconductor Corporation DP83815 (MacPhyter) Ethernet Controller ☑

○	10.2.1.1	255.255.0.0	☑

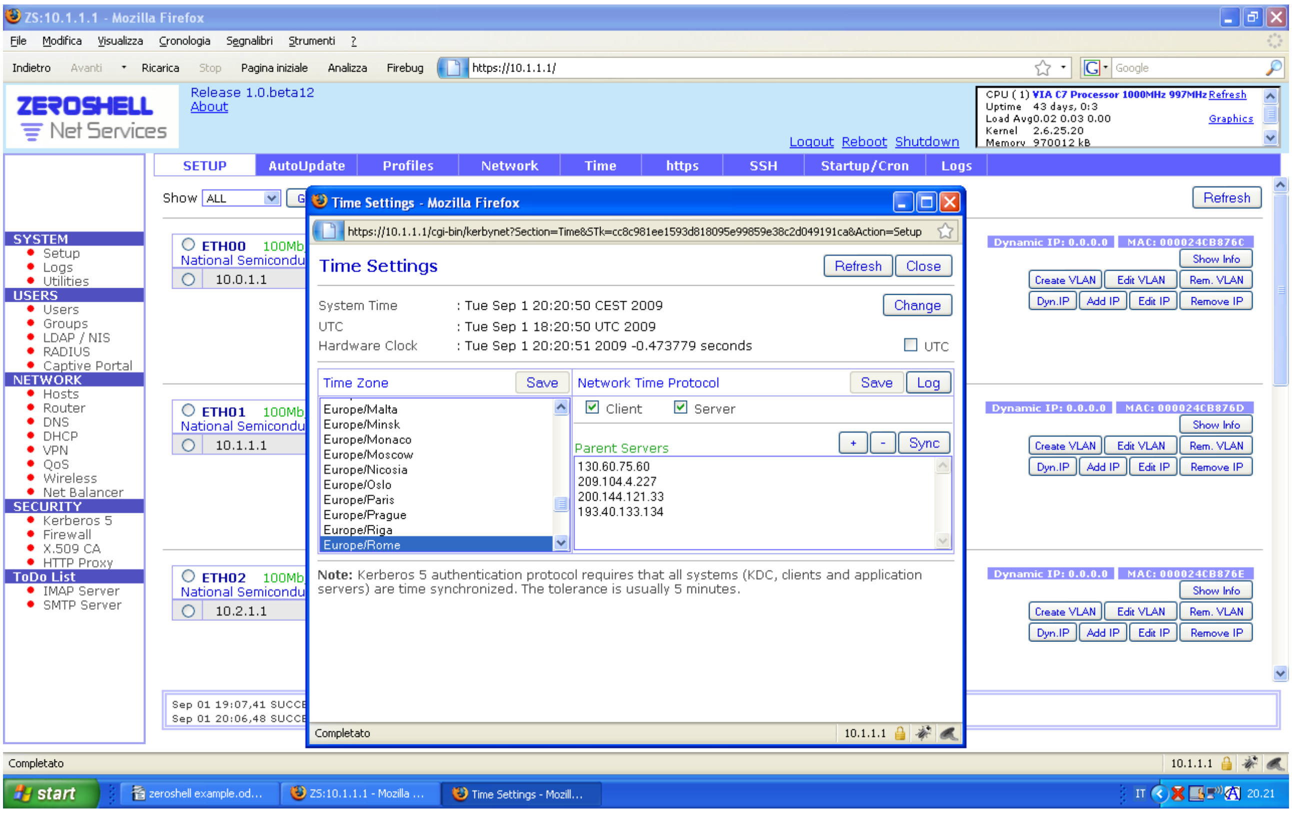
Dynamic IP: 0.0.0.0 MAC: 000024CB876E

```
Sep 01 19:07,41 SUCCESS: Feature [GG000024cb876c] not active. No Key found.
Sep 01 20:06,48 SUCCESS: Session opened from host 10.4.1.102 (Admin)
```

10.1.1.1

NTP

Definisco il server ntp per distribuire la data e l'ora



https://10.1.1.1/cgi-bin/kerbynet?Section=Time&STk=cc8c981ee1593d818095e99859e38c2d049191ca&Action=Setup

Time Settings Refresh Close

System Time : Tue Sep 1 20:20:50 CEST 2009 Change

UTC : Tue Sep 1 18:20:50 UTC 2009

Hardware Clock : Tue Sep 1 20:20:51 2009 -0.473779 seconds □ UTC

Time Zone Save

Europe/Malta
Europe/Minsk
Europe/Monaco
Europe/Moscow
Europe/Nicosia
Europe/Oslo
Europe/Paris
Europe/Prague
Europe/Riga
Europe/Rome

Network Time Protocol Save Log

☑ Client ☑ Server

Parent Servers + - Sync

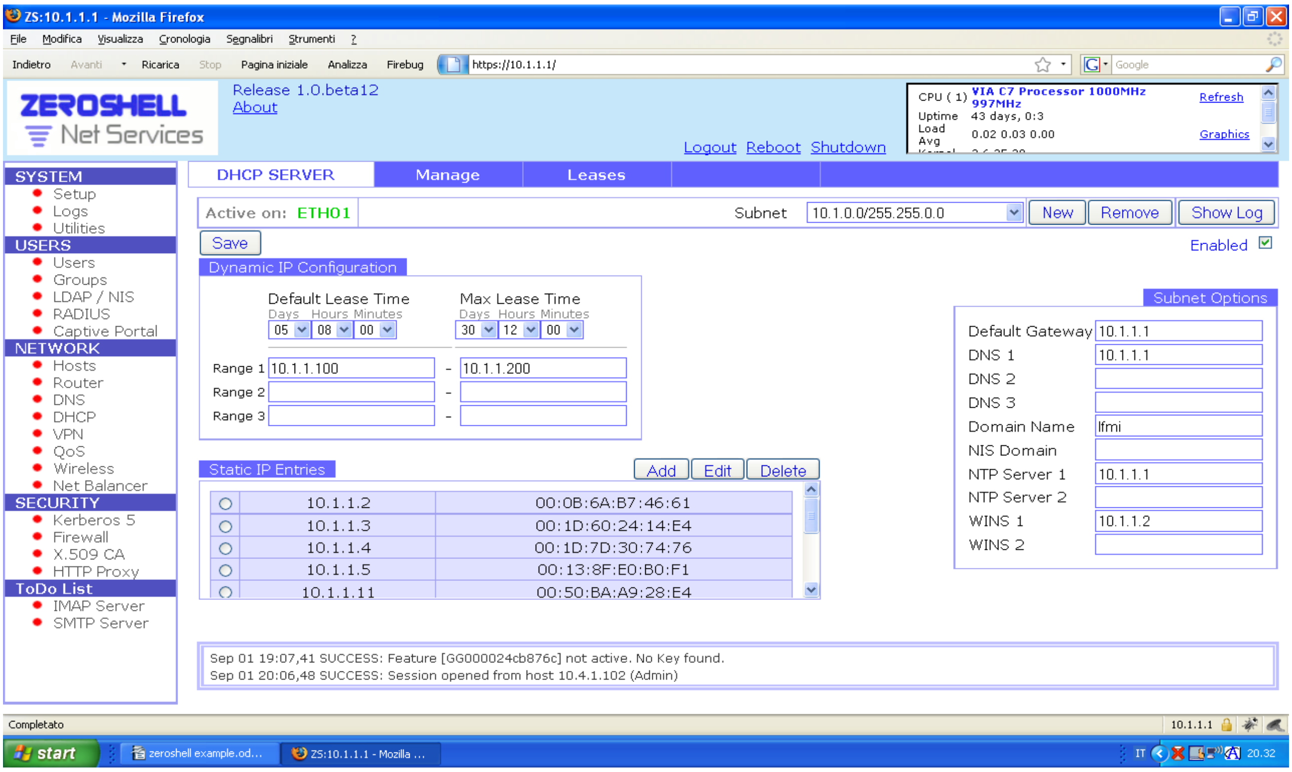
130.60.75.60
209.104.4.227
200.144.121.33
193.40.133.134

Note: Kerberos 5 authentication protocol requires that all systems (KDC, clients and application servers) are time synchronized. The tolerance is usually 5 minutes.

DHCP

Configuro una area di assegnazione automatica degli indirizzi per ogni porta lan stabilisco che le seguenti aree di indirizzamento valide per tutte le sotto reti:

- 10.x.1.1 default gateway
- 10.x.1.2 sino a 10.x.1.99 area per indirizzi statici
- 10.x.1.100 sino a 10.x.1.200 ara di assegnazione dinamica dhcp
- stabilisco inoltre che per semplificare la configurazione dei vari sistemi anche per le componenti di rete che necessitano indirizzi statici utilizzerò la tecnica di assegnazione dell indirizzo attraverso il dhcp mappando il relativo mac address



CPU (1) VIA C7 Processor 1000MHz 997MHz
Uptime 43 days, 0:3
Load Avg 0.02 0.03 0.00

Active on: ETH01

Subnet 10.1.0.0/255.255.0.0

Enabled ☑

Dynamic IP Configuration

	Days	Hours	Minutes
Default Lease Time	05	08	00
Max Lease Time	30	12	00

Range 1	10.1.1.100	-	10.1.1.200
Range 2		-	
Range 3		-	

Static IP Entries

○	10.1.1.2	00:0B:6A:B7:46:61
○	10.1.1.3	00:1D:60:24:14:E4
○	10.1.1.4	00:1D:7D:30:74:76
○	10.1.1.5	00:13:8F:E0:B0:F1
○	10.1.1.11	00:50:BA:A9:28:E4

Subnet Options

Default Gateway	10.1.1.1
DNS 1	10.1.1.1
DNS 2	
DNS 3	
Domain Name	lfmi
NIS Domain	
NTP Server 1	10.1.1.1
NTP Server 2	
WINS 1	10.1.1.2
WINS 2	

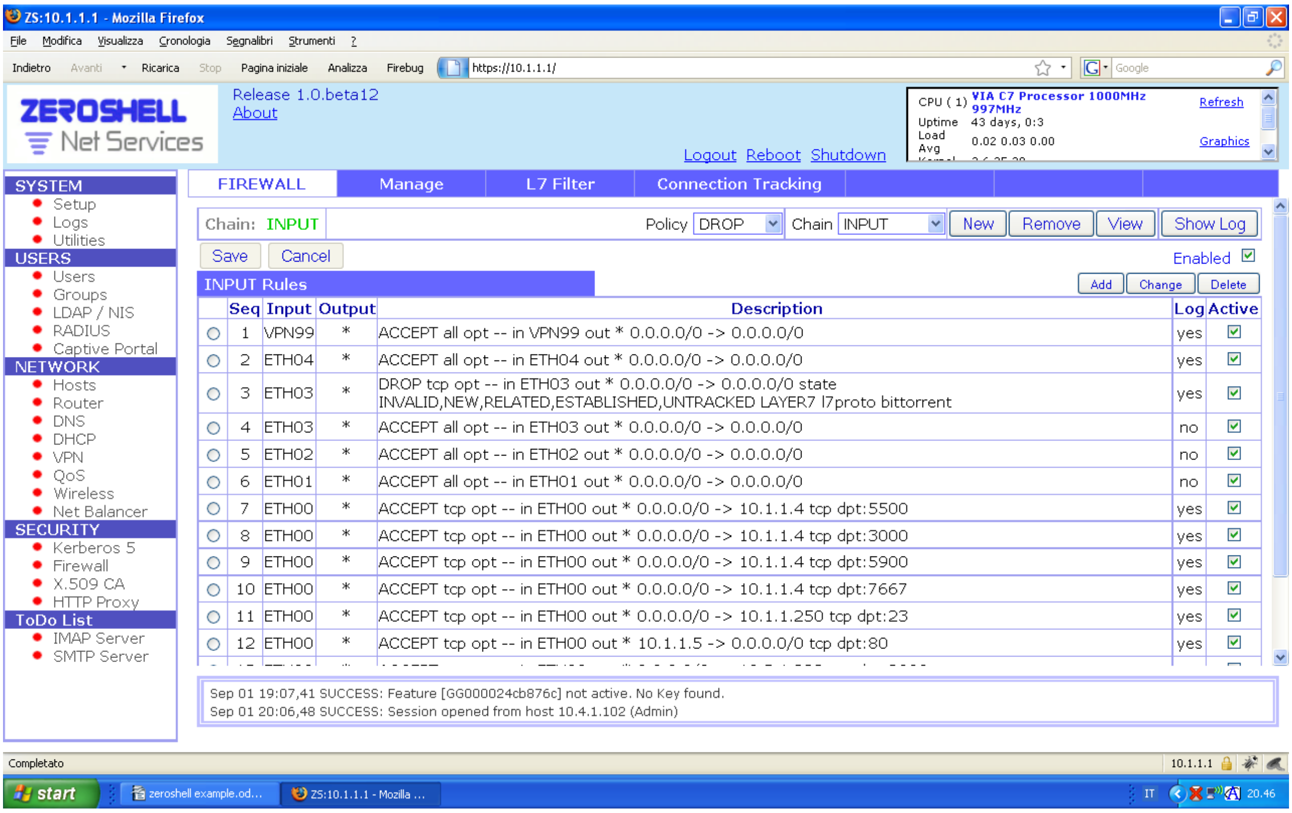
```
Sep 01 19:07,41 SUCCESS: Feature [GG000024cb876c] not active. No Key found.
Sep 01 20:06,48 SUCCESS: Session opened from host 10.4.1.102 (Admin)
```

FIREWALL

Imposto le policy di default del firewall

- input =drop
- forward=drop
- output=accept

poi abilito per input e forward in base alle varie porte ethernet


ZS:10.1.1.1 - Mozilla Firefox
File Modifica Visualizza Cronologia Segnalibri Strumenti ?
Indietro Avanti Ricarica Stop Pagina iniziale Analizza Firebug https://10.1.1.1/
ZEROSHELL Net Services
Release 1.0.beta12
About
CPU (1) VIA C7 Processor 1000MHz 997MHz
Uptime 43 days, 0:3
Load Avg 0.02 0.03 0.00
Refresh
Graphics
Logout Reboot Shutdown
SYSTEM Setup Logs Utilities
USERS Users Groups LDAP / NIS RADIUS Captive Portal
NETWORK Hosts Router DNS DHCP VPN QoS Wireless Net Balancer
SECURITY Kerberos 5 Firewall X.509 CA HTTP Proxy
ToDo List IMAP Server SMTP Server
FIREWALL Manage L7 Filter Connection Tracking
New Remove View Show Log
Save Cancel
Add Change Delete
Completato
10.1.1.1
start zeroshell example.od... ZS:10.1.1.1 - Mozilla ...
IT 20.46

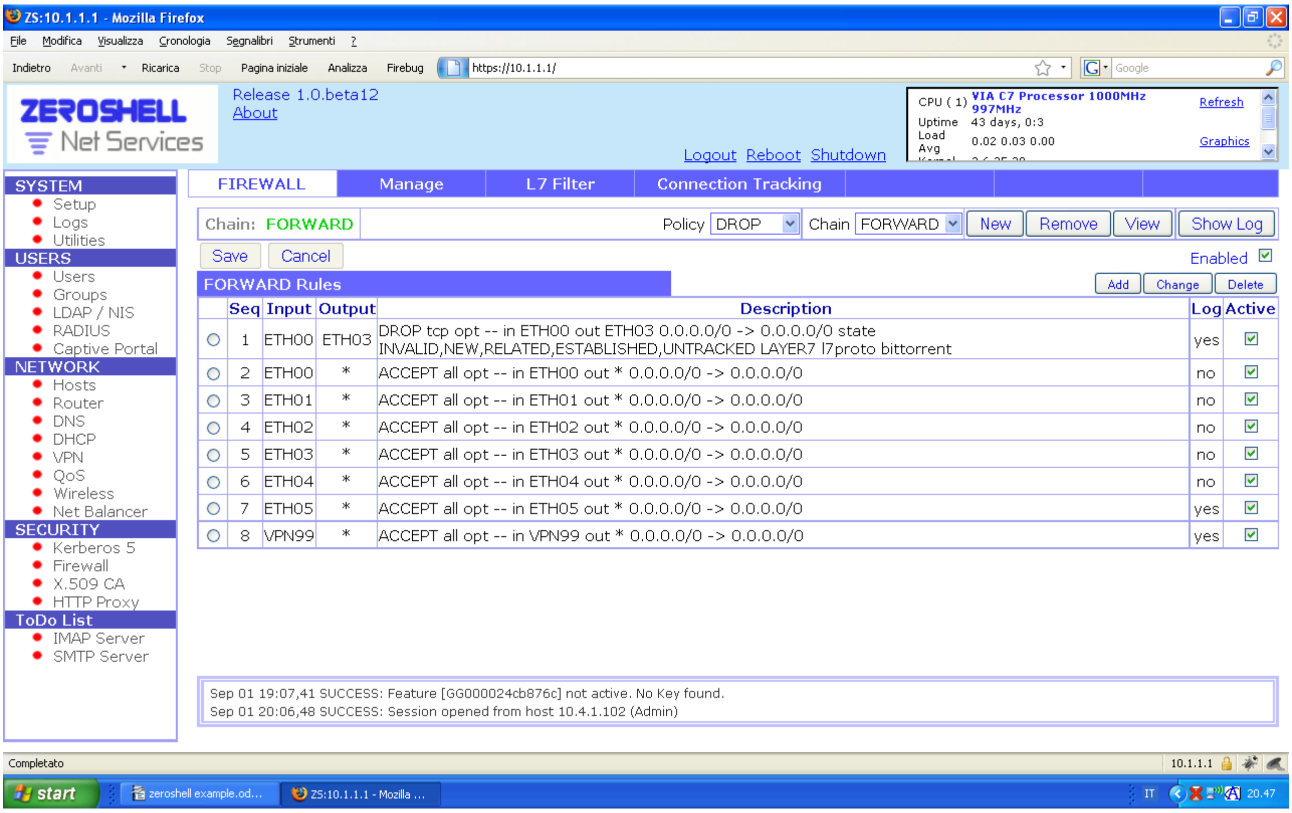
Chain: INPUT Policy DROP Chain INPUT

Enabled ☑

INPUT Rules

	Seq	Input	Output	Description	Log	Active
○	1	VPN99	*	ACCEPT all opt -- in VPN99 out * 0.0.0.0/0 -> 0.0.0.0/0	yes	☑
○	2	ETH04	*	ACCEPT all opt -- in ETH04 out * 0.0.0.0/0 -> 0.0.0.0/0	yes	☑
○	3	ETH03	*	DROP tcp opt -- in ETH03 out * 0.0.0.0/0 -> 0.0.0.0/0 state INVALID,NEW,RELATED,ESTABLISHED,UNTRACKED LAYER7 l7proto bittorrent	yes	☑
○	4	ETH03	*	ACCEPT all opt -- in ETH03 out * 0.0.0.0/0 -> 0.0.0.0/0	no	☑
○	5	ETH02	*	ACCEPT all opt -- in ETH02 out * 0.0.0.0/0 -> 0.0.0.0/0	no	☑
○	6	ETH01	*	ACCEPT all opt -- in ETH01 out * 0.0.0.0/0 -> 0.0.0.0/0	no	☑
○	7	ETH00	*	ACCEPT tcp opt -- in ETH00 out * 0.0.0.0/0 -> 10.1.1.4 tcp dpt:5500	yes	☑
○	8	ETH00	*	ACCEPT tcp opt -- in ETH00 out * 0.0.0.0/0 -> 10.1.1.4 tcp dpt:3000	yes	☑
○	9	ETH00	*	ACCEPT tcp opt -- in ETH00 out * 0.0.0.0/0 -> 10.1.1.4 tcp dpt:5900	yes	☑
○	10	ETH00	*	ACCEPT tcp opt -- in ETH00 out * 0.0.0.0/0 -> 10.1.1.4 tcp dpt:7667	yes	☑
○	11	ETH00	*	ACCEPT tcp opt -- in ETH00 out * 0.0.0.0/0 -> 10.1.1.250 tcp dpt:23	yes	☑
○	12	ETH00	*	ACCEPT tcp opt -- in ETH00 out * 10.1.1.5 -> 0.0.0.0/0 tcp dpt:80	yes	☑

```
Sep 01 19:07,41 SUCCESS: Feature [GG000024cb876c] not active. No Key found.
Sep 01 20:06,48 SUCCESS: Session opened from host 10.4.1.102 (Admin)
```


ZS:10.1.1.1 - Mozilla Firefox
File Modifica Visualizza Cronologia Segnalibri Strumenti ?
Indietro Avanti Ricarica Stop Pagina iniziale Analizza Firebug https://10.1.1.1/
ZEROSHELL Net Services
Release 1.0.beta12
About
CPU (1) VIA C7 Processor 1000MHz 997MHz
Uptime 43 days, 0:3
Load Avg 0.02 0.03 0.00
Refresh
Graphics
Logout Reboot Shutdown
SYSTEM Setup Logs Utilities
USERS Users Groups LDAP / NIS RADIUS Captive Portal
NETWORK Hosts Router DNS DHCP VPN QoS Wireless Net Balancer
SECURITY Kerberos 5 Firewall X.509 CA HTTP Proxy
ToDo List IMAP Server SMTP Server
FIREWALL Manage L7 Filter Connection Tracking
New Remove View Show Log
Save Cancel
Add Change Delete
Completato
10.1.1.1
start zeroshell example.od... ZS:10.1.1.1 - Mozilla ...
IT 20.47

Chain: FORWARD Policy DROP Chain FORWARD

Enabled ☑

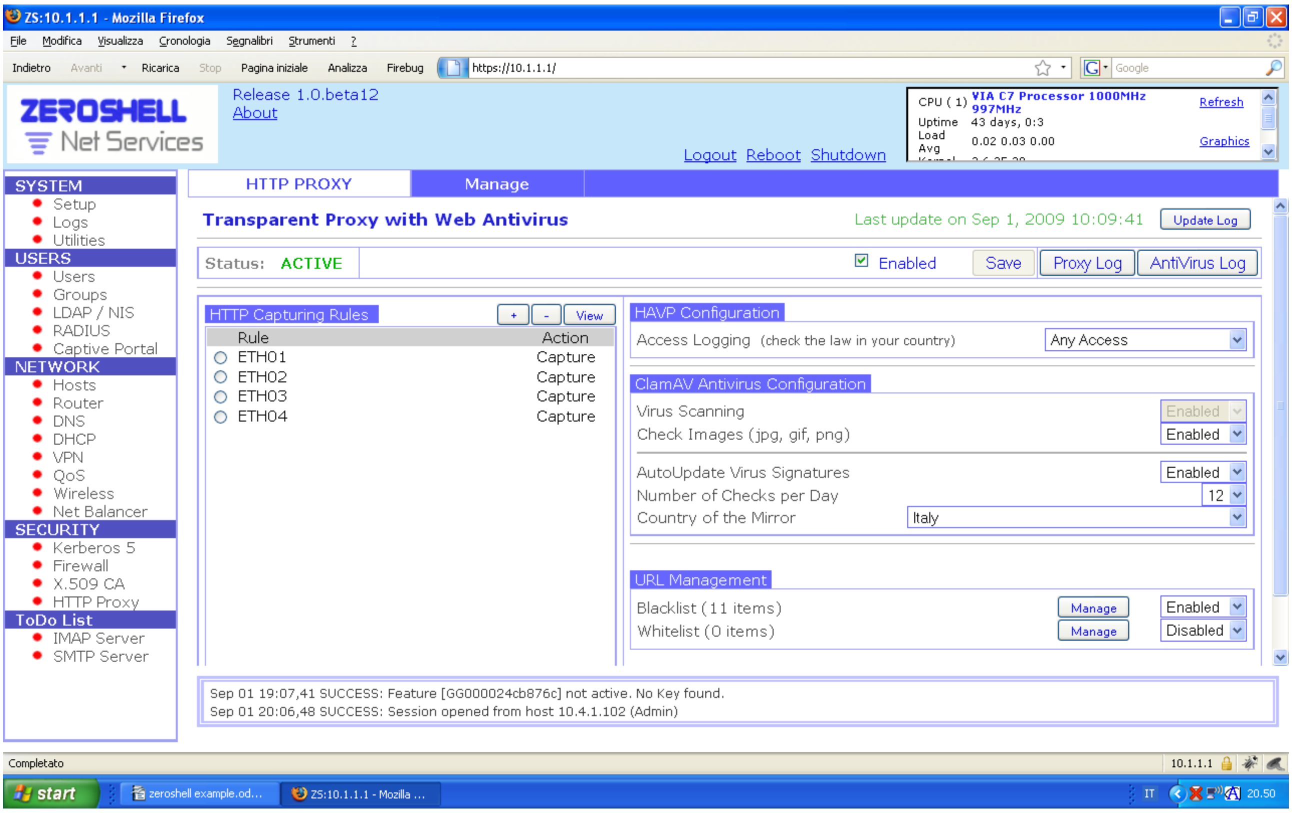
FORWARD Rules

	Seq	Input	Output	Description	Log	Active
○	1	ETH00	ETH03	DROP tcp opt -- in ETH00 out ETH03 0.0.0.0/0 -> 0.0.0.0/0 state INVALID,NEW,RELATED,ESTABLISHED,UNTRACKED LAYER7 l7proto bittorrent	yes	☑
○	2	ETH00	*	ACCEPT all opt -- in ETH00 out * 0.0.0.0/0 -> 0.0.0.0/0	no	☑
○	3	ETH01	*	ACCEPT all opt -- in ETH01 out * 0.0.0.0/0 -> 0.0.0.0/0	no	☑
○	4	ETH02	*	ACCEPT all opt -- in ETH02 out * 0.0.0.0/0 -> 0.0.0.0/0	no	☑
○	5	ETH03	*	ACCEPT all opt -- in ETH03 out * 0.0.0.0/0 -> 0.0.0.0/0	no	☑
○	6	ETH04	*	ACCEPT all opt -- in ETH04 out * 0.0.0.0/0 -> 0.0.0.0/0	no	☑
○	7	ETH05	*	ACCEPT all opt -- in ETH05 out * 0.0.0.0/0 -> 0.0.0.0/0	yes	☑
○	8	VPN99	*	ACCEPT all opt -- in VPN99 out * 0.0.0.0/0 -> 0.0.0.0/0	yes	☑

```
Sep 01 19:07,41 SUCCESS: Feature [GG000024cb876c] not active. No Key found.
Sep 01 20:06,48 SUCCESS: Session opened from host 10.4.1.102 (Admin)
```

PROXY

Imposto il proxy in modo da filtrare tutte le richieste provenienti dai vari client o server



Release 1.0.beta12

CPU (1) VIA C7 Processor 1000MHz 997MHz
Uptime 43 days, 0:3
Load Avg 0.02 0.03 0.00

Transparent Proxy with Web Antivirus

Last update on Sep 1, 2009 10:09:41

Status: ACTIVE

☑ Enabled

HTTP Capturing Rules

	Rule	Action
○	ETH01	Capture
○	ETH02	Capture
○	ETH03	Capture
○	ETH04	Capture

HAVP Configuration

Access Logging (check the law in your country): Any Access

ClamAV Antivirus Configuration

Virus Scanning: Enabled
Check Images (jpg, gif, png): Enabled
AutoUpdate Virus Signatures: Enabled
Number of Checks per Day: 12
Country of the Mirror: Italy

URL Management

Blacklist (11 items) Manage Enabled
Whitelist (0 items) Manage Disabled

```
Sep 01 19:07,41 SUCCESS: Feature [GG000024cb876c] not active. No Key found.
Sep 01 20:06,48 SUCCESS: Session opened from host 10.4.1.102 (Admin)
```