

Guida pratica all'utilizzo di Zeroshell



Il sistema operativo multifunzionale
creato da Fulvio.Ricciardi@zeroshell.net
www.zeroshell.net

Proteggere una piccola rete con stile

(Autore: cristiancolombini@libero.it)

Proteggere una piccola rete con stile:

Questa breve guida pratica ci consentirà di attivare in meno di un'ora un firewall a protezione della nostra rete. Grazie al sistema Zeroshell sarà possibile creare una barriera contro attacchi e minacce provenienti dalle reti pubbliche. Il classico esempio è quello di una rete connessa ad internet tramite un router ADSL usato spesso a sproposito da tutti gli utenti della rete.

Ecco quindi le brevi guide di Zeroshell trattate :

Primo avvio ed accesso

Preparare il disco per memorizzare le nostre impostazioni

Memorizzare le nostre impostazioni

Configurazione schede di rete

Accesso ad internet

Attivare il Captive Portal

Attivare il servizio DNS

Attivare il servizio DHCP

Routes statiche verso reti remote

Servizi attraverso Virtual Server

Sicurezza: verificare le regole di default del firewall

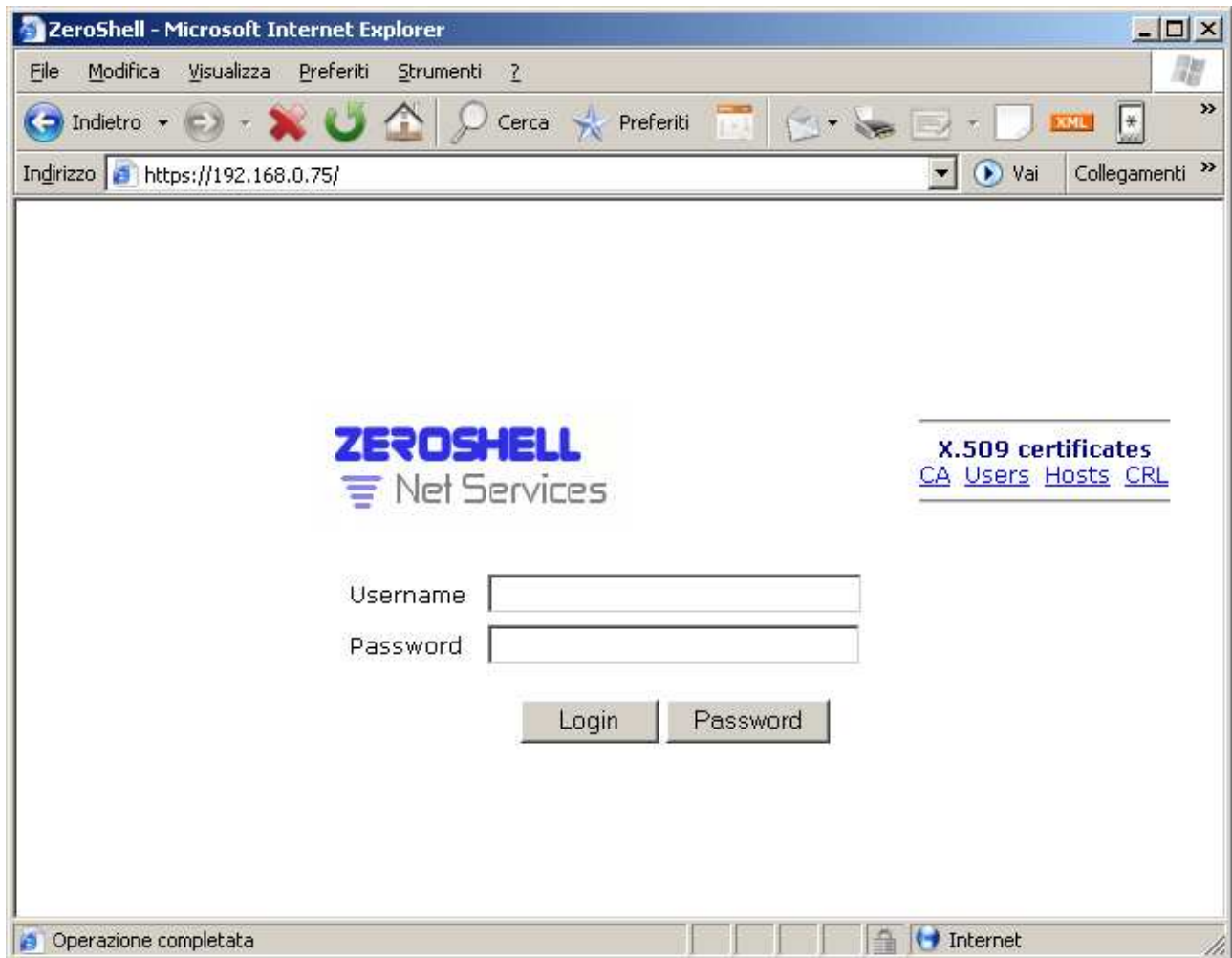
Vorrei comunque sottolineare che Zeroshell integra molte altre funzioni avanzate per reti ben più complesse; e che quindi con la presenza di Zeroshell la nostra rete diventa estremamente scalabile.

Primo avvio ed accesso:

Dopo aver lasciato partire il cd autoavviante su un pc dotato di almeno una scheda di rete, il sistema può essere raggiunto tramite connessione https puntando all'indirizzo ip 192.168.0.75

<https://192.168.0.75>

All'accesso verrà richiesto di accettare la connessione sicura, poi una utenza e password:



Entrare come:

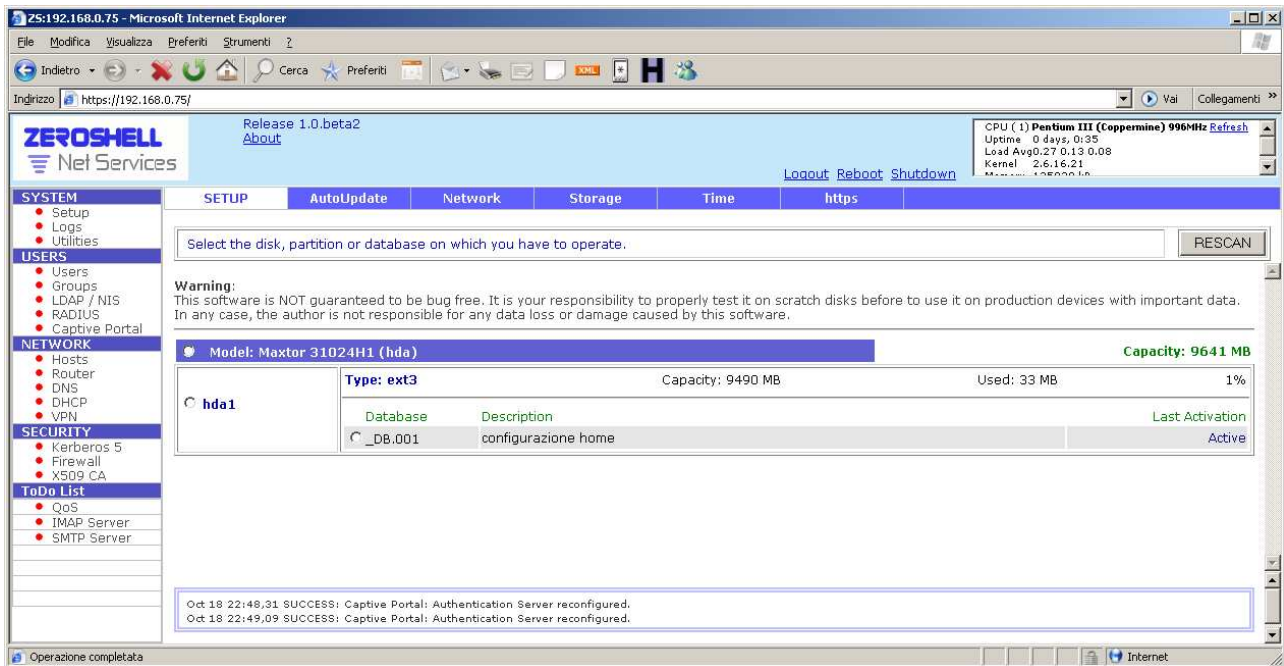
User: admin
Password: zershell

A questo punto dall'interfaccia web possiamo accedere ad ogni menu di configurazione del sistema.

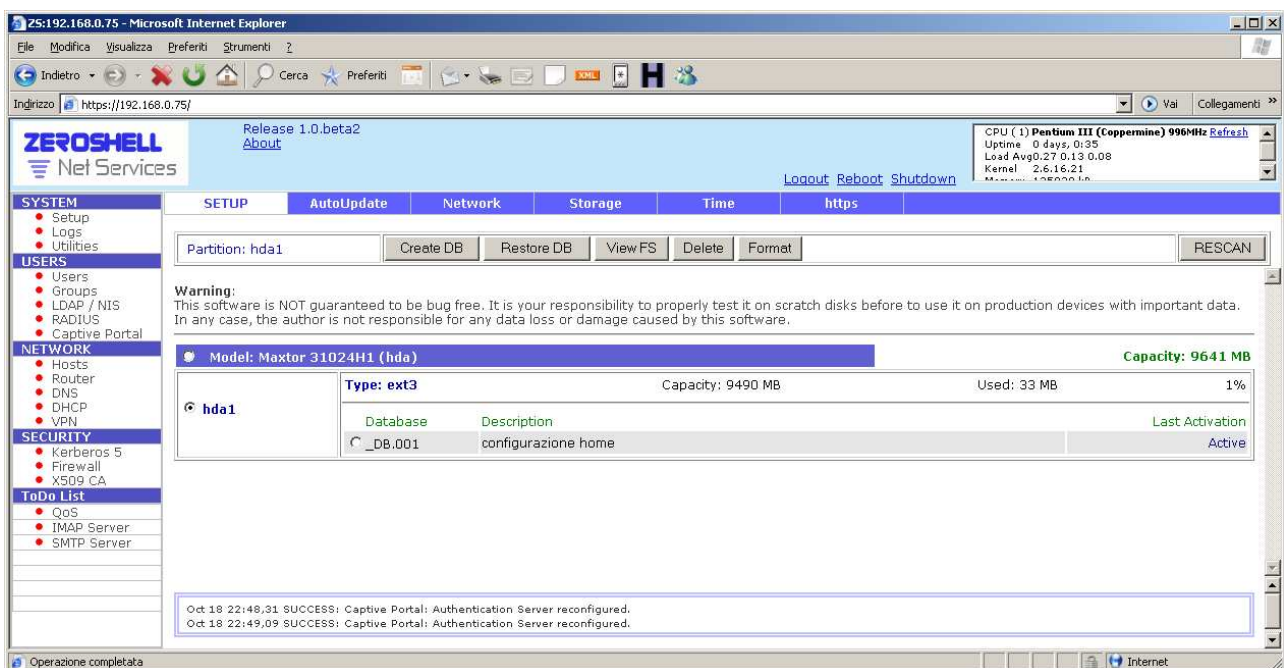
Preparare il disco per memorizzare le nostre impostazioni:

E' importante configurare il sistema in base alle nostre necessità senza perdere le modifiche. Per fare questo Zeroshell si appoggia su un file di configurazione archiviato in un disco fisso. In realtà basta avere anche un disco fisso con poco spazio (es: 1 gb è più che adatto!). Si può decidere se riutilizzare delle partizioni in esso presenti (per esempio partizioni di tipo ext3, reiserfs, ext2 o fat32). Io per comodità creo una partizione nuova ext3. Quindi scelgo di cancellare completamente la struttura di partizioni presenti sul mio disco (i dati in esse verranno cancellati) e di creare un'unica partizione ext3.

Accediamo al menu **SETUP** (nel frame di sinistra) nella voce **STORAGE** (nel frame in alto):



Subito ci viene mostrato il disco presente nel sistema. A questo punto selezionando le partizioni in esso presenti (se esistenti) decido di cancellarle una alla volta premendo sul tasto **DELETE**:



Ci viene chiesto di confermare l'eliminazione della partizione selezionata.

In questo modo arrivo ad avere un disco privo di partizioni. Ne creo una nuova occupando pure tutto lo spazio disponibile (solo per comodità).

Memorizzare le nostre impostazioni:

Una volta preparato lo spazio per l'archiviazione del nostro file di configurazione procediamo alla creazione di un primo file. Selezionando la partizione nuova da utilizzare cliccare sul bottone CREATE DB:

https://192.168.0.75 - Create DB - Microsoft Internet Explorer

Maxtor 31024H1 (hda)
New Database on partition hda1

Create Close

Description: configurazione home

Hostname (FQDN): zeroshell.lordch.lan

Kerberos 5 Realm: LORDCH.LAN

LDAP Base: dc=lordch,dc=lan

Admin password:

Confirm password:

NETWORK CONFIG

Ethernet Interface: ETH00 - 3Com Corporation 3c905C-TX/TX-M [Tornado] (rev 78)

IP Address / Netmask: 192.168.0.75 / 255.255.255.0

Default Gateway:

Operazione completata Internet

Ci viene chiesta una breve descrizione della configurazione; il nome completo del nostro sistema; il dominio eventuale Kerberos e LDAP; di settare una nuova password dell'utente "admin"; l'indirizzo ip dell'interfaccia generalmente primaria che viene usata per configurare il sistema; l'eventuale default gateway per l'accesso ad altre reti (esempio internet).

Questa configurazione diventerà quella che il sistema attiva al prossimo avvio. Quindi conterrà tutte le nostre personalizzazioni. Possiamo in ogni momento decidere di creare altre configurazioni e di renderle attive in base alle nostre necessità (tramite il bottone **ACTIVATE**). Possiamo farne delle copie di backup su un altro sistema tramite il bottone **BACKUP**.

25:192.168.0.75 - Microsoft Internet Explorer

File Modifica Visualizza Preferiti Strumenti ?

Indietro Cerca Preferiti

Indirizzo https://192.168.0.75/ Vai Collegamenti >>

ZEROSHELL
Net Services

Release 1.0.beta2
[About](#)

CPU (1) **Pentium III (Coppermine) 996MHz** [Refresh](#)
Uptime 0 days, 0:35
Load Avg 0.27 0.13 0.08
Kernel 2.6.16.21
Memory 128000 KB

[Logout](#) [Reboot](#) [Shutdown](#)

SYSTEM

- Setup
- Logs
- Utilities

USERS

- Users
- Groups
- LDAP / NIS
- RADIUS
- Captive Portal

NETWORK

- Hosts
- Router
- DNS
- DHCP
- VPN

SECURITY

- Kerberos 5
- Firewall
- X509 CA

ToDo List

- QoS
- IMAP Server
- SMTP Server

SETUP

AutoUpdate

Network

Storage

Time

https

Database: **_DB.001 (hda1)**

Warning:
This software is NOT guaranteed to be bug free. It is your responsibility to properly test it on scratch disks before to use it on production devices with important data. In any case, the author is not responsible for any data loss or damage caused by this software.

Model: Maxtor 31024H1 (hda) **Capacity: 9641 MB**

hda1

Type: ext3

Capacity: 9490 MB

Used: 33 MB

1%

Database	Description	Last Activation
_DB.001	configurazione home	Active

Oct 18 22:49,09 SUCCESS: Captive Portal: Authentication Server reconfigured.
Oct 18 23:27,00 SUCCESS: tcp port forwarding 21 -> 192.168.0.1:21 on ETH01 successfully activated

Operazione completata

Internet

Configurazione schede di rete:

Una volta preparato il disco e creato il file di configurazione possiamo passare alla configurazione delle schede di rete dal menu **SETUP** alla voce **NETWORK**:

Release 1.0.beta2
About

Logout Reboot Shutdown

CPU (1) Pentium III (Coppermine) 996MHz Refresh
Uptime: 0 days, 1:38
Load Avg: 0.00 0.00 0.00
Kernel: 2.6.16.21

SETUP AutoUpdate Network Storage Time https

Show ALL GATEWAY Make VPN Make BRIDGE Make BOND Make PPPoE Refresh

SYSTEM
• Setup
• Logs
• Utilities

USERS
• Users
• Groups
• LDAP / NIS
• RADIUS
• Captive Portal

NETWORK
• Hosts
• Router
• DNS
• DHCP
• VPN

SECURITY
• Kerberos 5
• Firewall
• X509 CA

ToDo List
• QoS
• IMAP Server
• SMTP Server

ETH00 100Mb/s Full Duplex
3Com Corporation 3c905C-TX/TX-M [Tornado] (rev 78) UP
192.168.0.75 255.255.255.0

MAC: 0004754C9A1D
Show Info
Create VLAN Edit VLAN Rem. VLAN
Add IP Edit IP Remove IP

ETH01 100Mb/s Full Duplex
Acton Technology Corporation SMC2-1211TX (rev 10) UP
192.168.1.1 255.255.255.0

MAC: 0030F108F6D7
Show Info
Create VLAN Edit VLAN Rem. VLAN
Add IP Edit IP Remove IP

Oct 18 23:51:19 SUCCESS: tcp port forwarding 21 -> 192.168.0.1:21 on ETH01 successfully removed
Oct 18 23:51:33 SUCCESS: tcp port forwarding 15000 -> 192.168.0.1:15000 on ETH01 successfully activated

Operazione completata

Generalmente in fase di creazione di un firewall in modalità routed si identifica con ETH00 la scheda di rete sicura (interna) e con ETH01 quella che andrà a comunicare con la rete insicura (esterna). E' opportuno assegnare a queste degli indirizzi ip statici tramite i relativi bottoni **Add IP**.

Una volta stabilito per esempio che nella rete interna il nostro firewall risponderà all'ip 192.168.0.75 e che sulla rete esterna (seconda scheda di rete) risponderà al 192.168.1.1 possiamo pensare di impostare un gateway che ci collegherà ad internet: dal bottone **Gateway**. Ho impostato che il mio gateway è 192.168.1.254; posso verificare nel menu **ROUTER** che effettivamente la mia route di default sia stata scritta:

Release 1.0.beta2
About

Logout Reboot Shutdown

CPU (1) Pentium III (Coppermine) 996MHz Refresh
Uptime: 0 days, 1:38
Load Avg: 0.00 0.00 0.00
Kernel: 2.6.16.21

ROUTER Manage IPv2 NAT Virtual Server

Forwarding: ACTIVE Enabled DEFAULT GW ROUTING TABLE CHECK IP

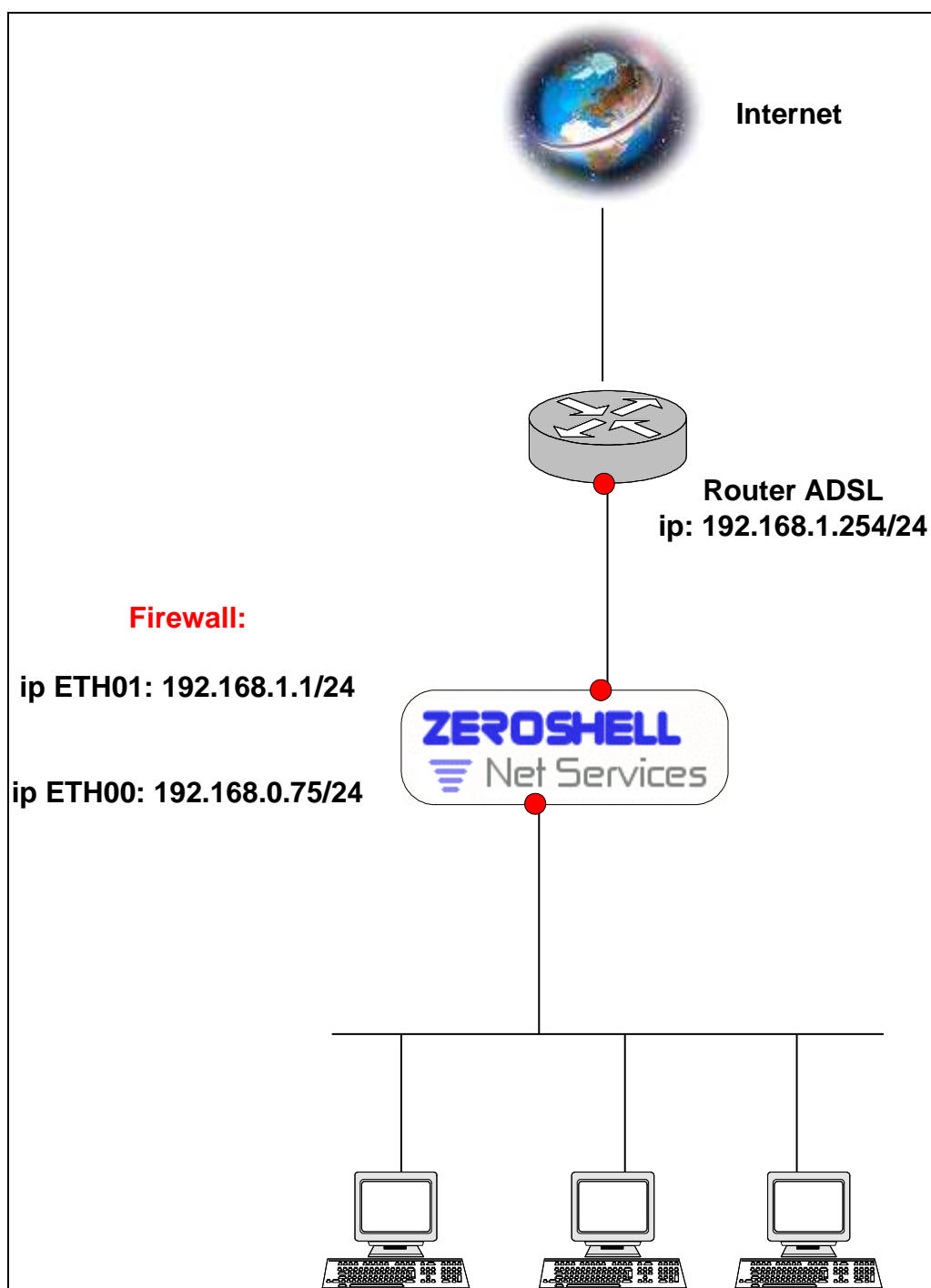
STATIC ROUTES
Add Change Delete

	Destination	Netmask	Type	Metric	Gateway	Interface	State
•	DEFAULT GATEWAY	0.0.0.0	Net	0	192.168.1.254		Up

Oct 18 23:51:33 SUCCESS: tcp port forwarding 15000 -> 192.168.0.1:15000 on ETH01 successfully activated
Oct 19 00:13:23 SUCCESS: tcp port forwarding 15000 -> 192.168.1.254:15000 on ETH00 successfully activated

Operazione completata

la mia rete diventa quindi:

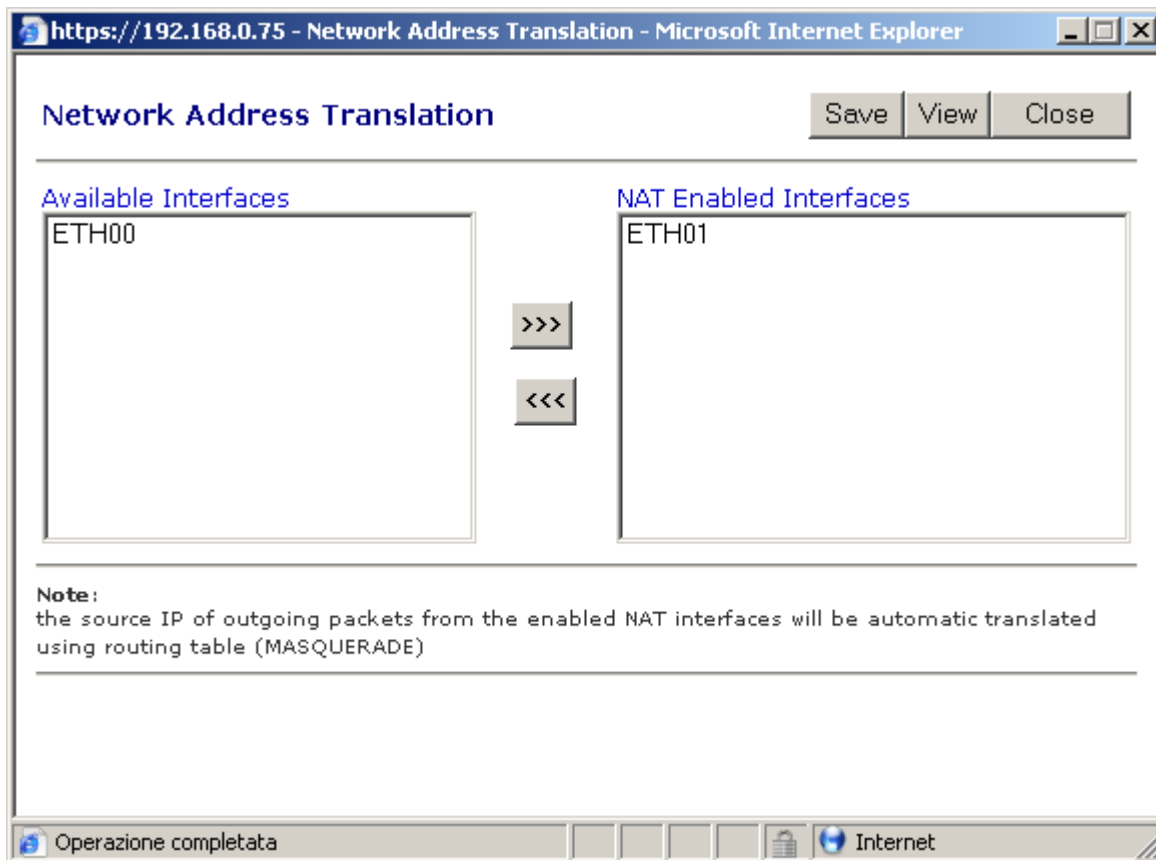


E' facile intuire che una situazione del genere ci consente di sfruttare molte potenzialità del nostro sistema Zeroshell; per esempio possiamo scrivere delle politiche di protezione della nostra rete interna (192.168.0.0/24); oppure possiamo usare la funzione di Captive Portal per imporre utenza e password al momento della navigazione dei nostri client; possiamo anche pensare di creare dei server virtuali per dare alcuni servizi all'esterno, ecc.

Accesso ad internet:

Per concedere agli hosts interni alla rete di accedere ad internet a questo punto ci basta abilitare il NAT.

Nel menu **ROUTER** alla voce **NAT** settiamo che:



La rete dietro l'interfaccia ETH00 venga mascherata da ETH01. A questo punto i pc della rete riescono a navigare.

Attivare il Captive Portal:

Si tratta di una utilissima funzione che richiede l'autenticazione con utente e password prima di consentire il passaggio di richieste verso l'esterno (per esempio prima di consultare internet, scaricare posta, ecc).

Prima di attivare il Captive Portal dobbiamo creare le utenze tramite il menu **USERS** alla voce **ADD** ; qui sarà possibile riempire i vari campi come sotto:

The screenshot shows the Zeroshell Net Services web interface in a Microsoft Internet Explorer browser window. The address bar shows 'https://192.168.0.75/'. The interface has a sidebar menu on the left with categories: SYSTEM (Setup, Logs, Utilities), USERS (Users, Groups, LDAP / NIS, RADIUS, Captive Portal), NETWORK (Hosts, Router, DNS, DHCP, VPN), and SECURITY (Kerberos 5, Firewall, X509 CA). The 'USERS' section is active, and the 'ADD' button is selected. The main content area shows the user creation form for 'cristian colombini (cristian)'. The form includes fields for Username ('cristian'), UID ('1'), Primary Group ('nobody'), GID ('65534'), Home Directory ('/home/cristian'), Default Shell ('bash'), User Information (Firstname, Lastname, Organization, Description, E-Mail, Phone), User Password (Password, Confirm), and Enabled Services (Kerberos 5 Authentication, Host-to-Lan VPN (L2TP/IPsec), 802.1X Access (VLAN)). A status bar at the bottom indicates 'Operazione completata'.

Release 1.0.beta2
About

Logout Reboot Shutdown

CPU (1) Pentium III (Coppermine) 996MHz Refresh
Uptime 0 days, 0:9
Load Avg0.12 0.09 0.05
Kernel 2.6.16.21
Memory 125000K

USERS List View Add Edit Delete X509 Kerberos 5

cristian colombini (cristian) Submit Reset

Account

Username cristian UID 1 Primary Group nobody GID 65534

Home Directory /home/cristian Default Shell bash sh tcsh other /bin/sh

User Information

Firstname cristian Lastname Organization ?

Description cristian E-Mail ? Phone ?

User Password

Password

Confirm

Enabled Services

Kerberos 5 Authentication ☒

Host-to-Lan VPN (L2TP/IPsec) ☒

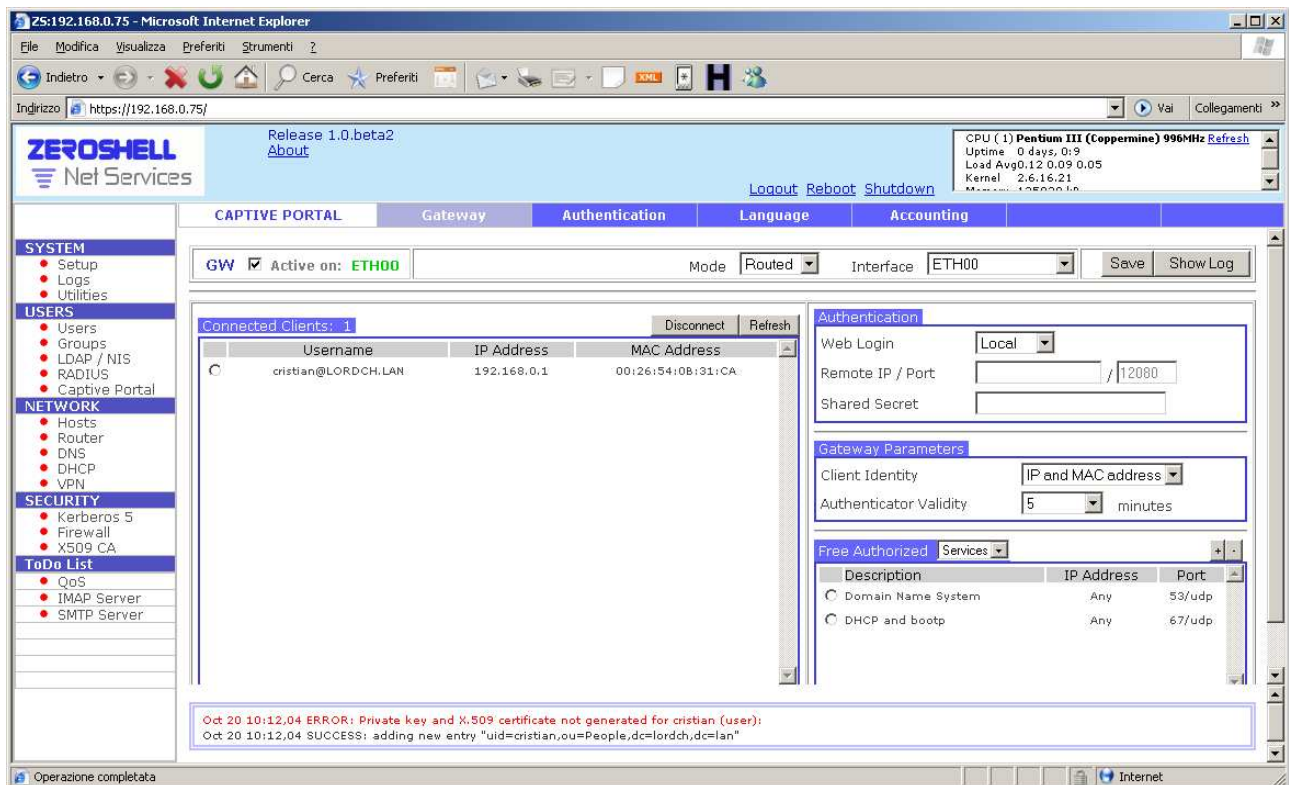
802.1X Access (VLAN) ☒

Oct 20 10:12:04 ERROR: Private key and X.509 certificate not generated for cristian (user):
Oct 20 10:12:04 SUCCESS: adding new entry "uid=cristian,ou=People,dc=lordch,dc=lan"

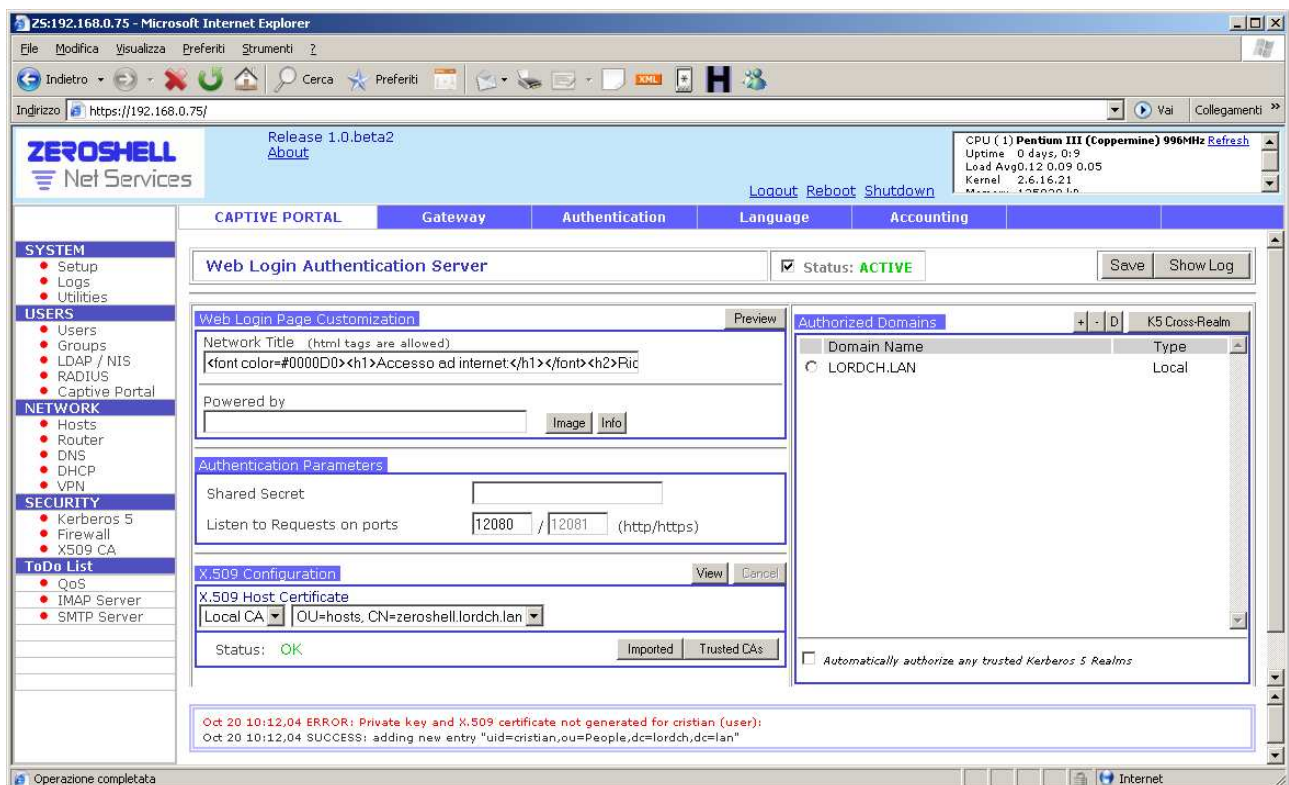
Operazione completata

Ricordiamoci che lo user sarà la voce **USERNAME**.

Una volta creato almeno un utente passiamo al menu **CAPTIVE PORTAL** ; flag su **GW** scegliamo **ROUTED MODE** e la scheda di rete sulla quale vogliamo che venga richiesta l'autenticazione (la scheda interna che rappresenta il default gateway della nostra rete).



Fatto ciò spostiamoci nella voce **AUTHENTICATION** ed attiviamola:



A questo punto se chiudiamo il browser e lo riapriamo, nel momento in cui cerchiamo di connetterci ad internet o alla stessa pagina di configurazione di Zeroshell, ci viene chiesto di autenticarci. Qui sotto ho personalizzato la pagina:

25:192.168.0.75 - Microsoft Internet Explorer

Indirizzo: https://192.168.0.75/

ZEROSHELL Net Services

Release 1.0.beta2
[About](#)

CPU (1) **Pentium III (Coppermine) 996MHz** [Refresh](#)
 Uptime 0 days, 0:22
 Load Avg 0.19 0.06 0.01
 Kernel 2.6.16.21
 Memory 10500 kb

[Logout](#) [Reboot](#) [Shutdown](#)

CAPTIVE PORTAL Gateway Authentication Language Accounting

Web Login Authentication Server ☒ Status: **ACTIVE** [Save](#) [Show Log](#)

Web Login Page Customization [Preview](#)

Network Title (html tags are allowed):

Powered by: [Image](#) [Info](#)

Authentication Parameters

Shared Secret:

Listen to Requests on ports: / (http/https)

X.509 Configuration [View](#) [Cancel](#)

X.509 Host Certificate

Status: **OK** [Imported](#) [Trusted CAs](#)

Authorized Domains [+](#) [-](#) [D](#) K5 Cross-Realm

Domain Name	Type
<input type="radio"/> LORDCH.LAN	Local

☐ Automatically authorize any trusted Kerberos 5 Realms

Oct 20 10:12,04 SUCCESS: adding new entry "uid=cristian,ou=People,dc=lordch,dc=lan"
 Oct 20 10:24,07 SUCCESS: Session opened from host 192.168.0.1 (Admin)

Operazione completata

Interessante verificare alla voce **GATEWAY** le utenze autenticate e come tramite selezione delle stesse si possano disconnettere tramite bottone **DISCONNECT**:

25:192.168.0.75 - Microsoft Internet Explorer

File Modifica Visualizza Preferiti Strumenti ?

Indietro Cerca Preferiti

Indirizzo https://192.168.0.75/

ZEROSHELL
Net Services

Release 1.0.beta2
[About](#)

[Logout](#) [Reboot](#) [Shutdown](#)

CPU (1) **Pentium III (Coppermine) 996MHz** [Refresh](#)
Uptime 0 days, 0:22
Load Avg 0.19 0.06 0.01
Kernel 2.6.16.21
Memory 128000 Kb

CAPTIVE PORTAL Gateway Authentication Language Accounting

GW ☒ Active on: **ETH00** Mode **Routed** Interface **ETH00** **Save** **Show Log**

Connected Clients: 1 **Disconnect** **Refresh**

	Username	IP Address	MAC Address
	cristian@LORDCH.LAN	192.168.0.1	00:26:54:08:31:CA

Authentication

Web Login **Local**

Remote IP / Port / **12080**

Shared Secret

Gateway Parameters

Client Identity **IP and MAC address**

Authenticator Validity **5** minutes

Free Authorized Services

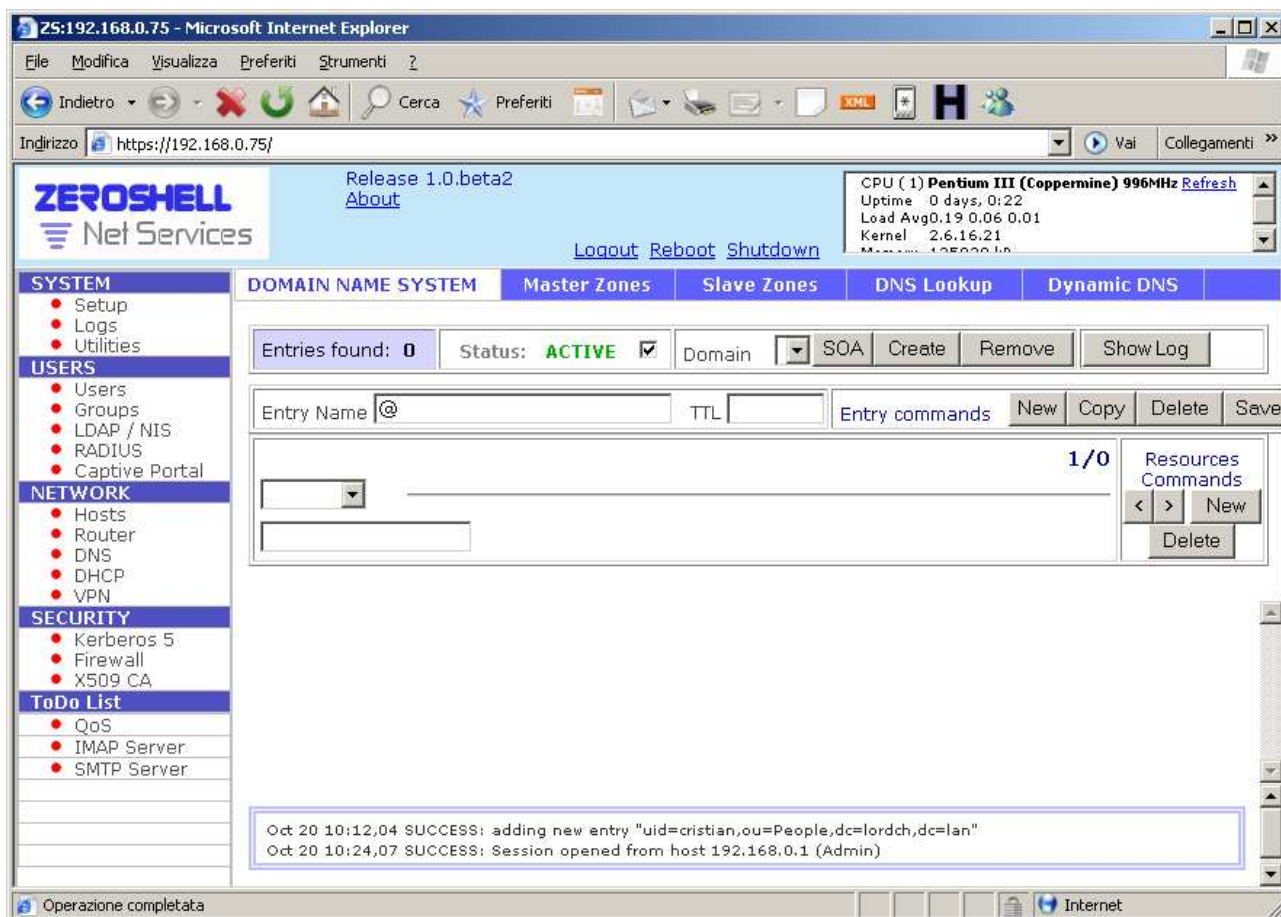
Description	IP Address	Port
<input type="radio"/> Domain Name System	Any	53/udp
<input type="radio"/> DHCP and bootp	Any	67/udp

Oct 20 10:12:04 SUCCESS: adding new entry "uid=cristian,ou=People,dc=lordch,dc=lan"
Oct 20 10:24:07 SUCCESS: Session opened from host 192.168.0.1 (Admin)

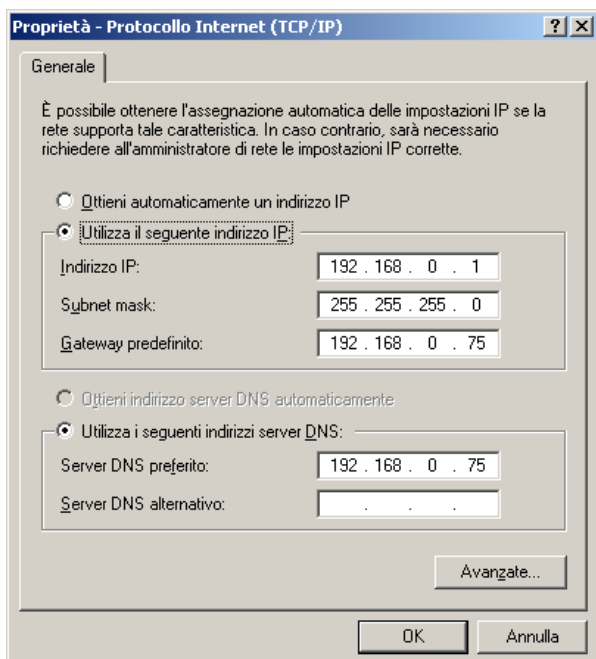
Operazione completata

Attivare il servizio DNS:

Si sa che con linee adsl per poter navigare da una rete domestica o priva di DNS interno bisogna impostare i dns esterni segnalateci dal provider. Molto scomodo anche perché a volte questi servizi non sono perfettamente funzionanti... Cosa c'è di meglio se non settare Zeroshell per avere anche questo servizio? Basta proprio un click al menu **DNS** ..sul flag **ATTIVATE**:

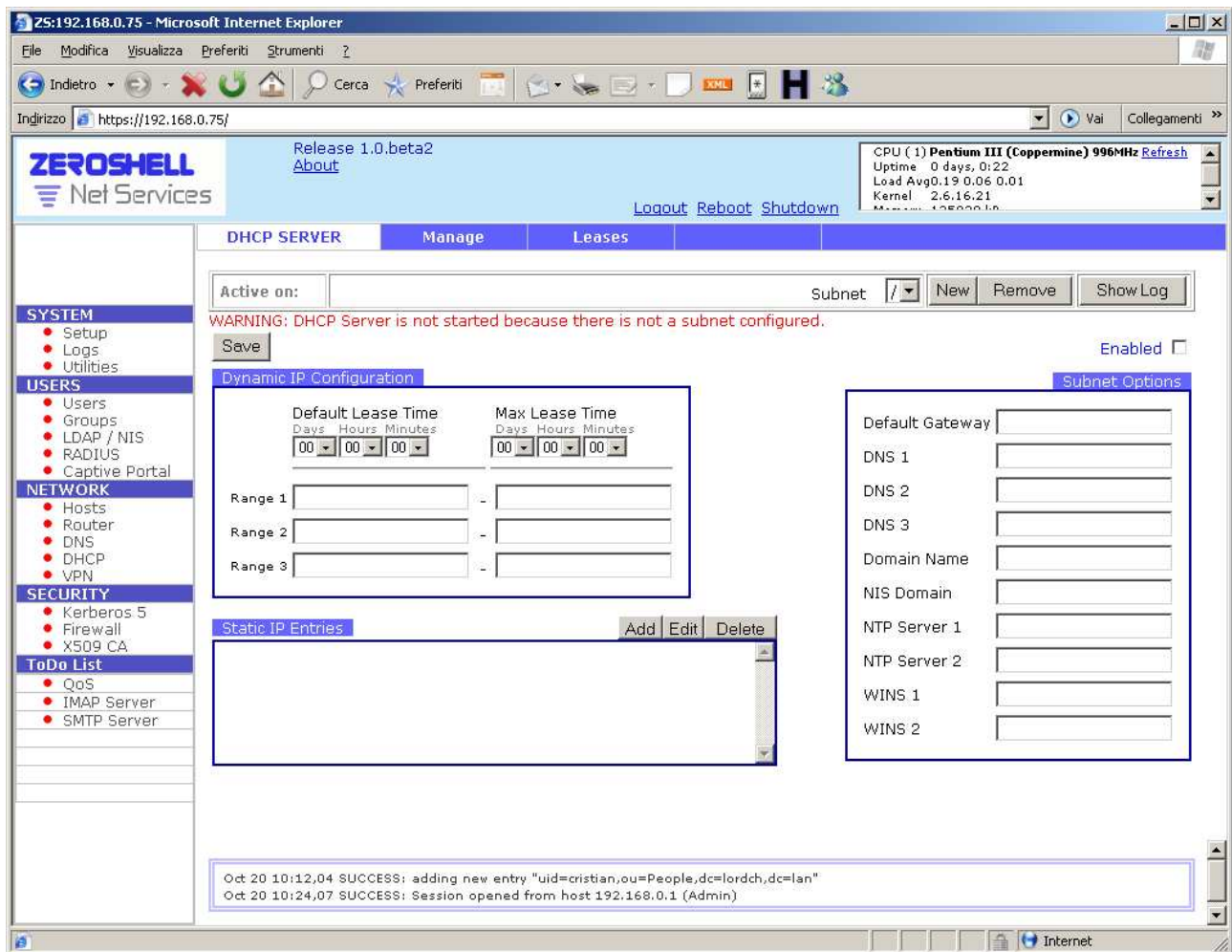


ed il gioco è fatto...possiamo ora configurare i nostri client come segue (dove 192.168.0.75 è il nostro Zeroshell..):

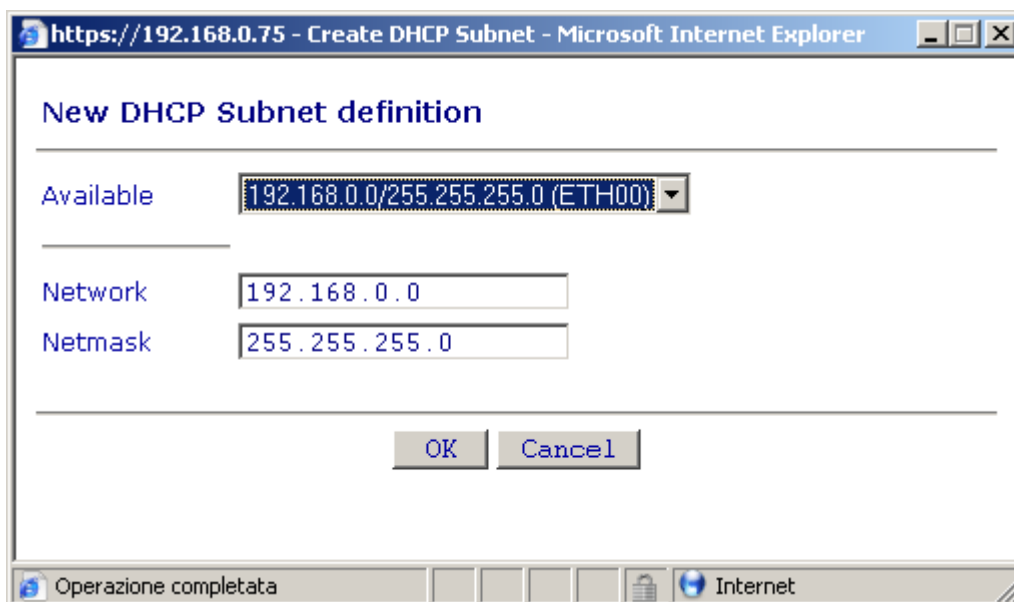


Attivare il servizio DHCP:

Perché avere ip statici sulla rete quando esiste la possibilità di avere uno strumento come Zeroshell? Basta continuare a cambiare ip, a controllare gateway e dns! Menu **DHCP**:



selezionare il bottone **NEW** e scegliere la rete sulla quale si vuole distribuire l'indirizzamento in modo automatico:



ecco:

25:192.168.0.75 - Microsoft Internet Explorer

File Modifica Visualizza Preferiti Strumenti ?

Indietro Cerca Preferiti

Indirizzo https://192.168.0.75/ Vai Collegamenti >>

ZEROSHELL
Net Services

Release 1.0.beta2
[About](#)

[Logout](#) [Reboot](#) [Shutdown](#)

CPU (1) **Pentium III (Coppermine) 996MHz** [Refresh](#)
Uptime 0 days, 0:22
Load Avg 0.19 0.06 0.01
Kernel 2.6.16.21
Memory 4096000 kb

DHCP SERVER Manage Leases

Active on: **ETH00** Subnet 192.168.0.0/255.255.255.0 New Remove Show Log

Save Enabled ☒

Dynamic IP Configuration

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

Range 1 -
Range 2 -
Range 3 -

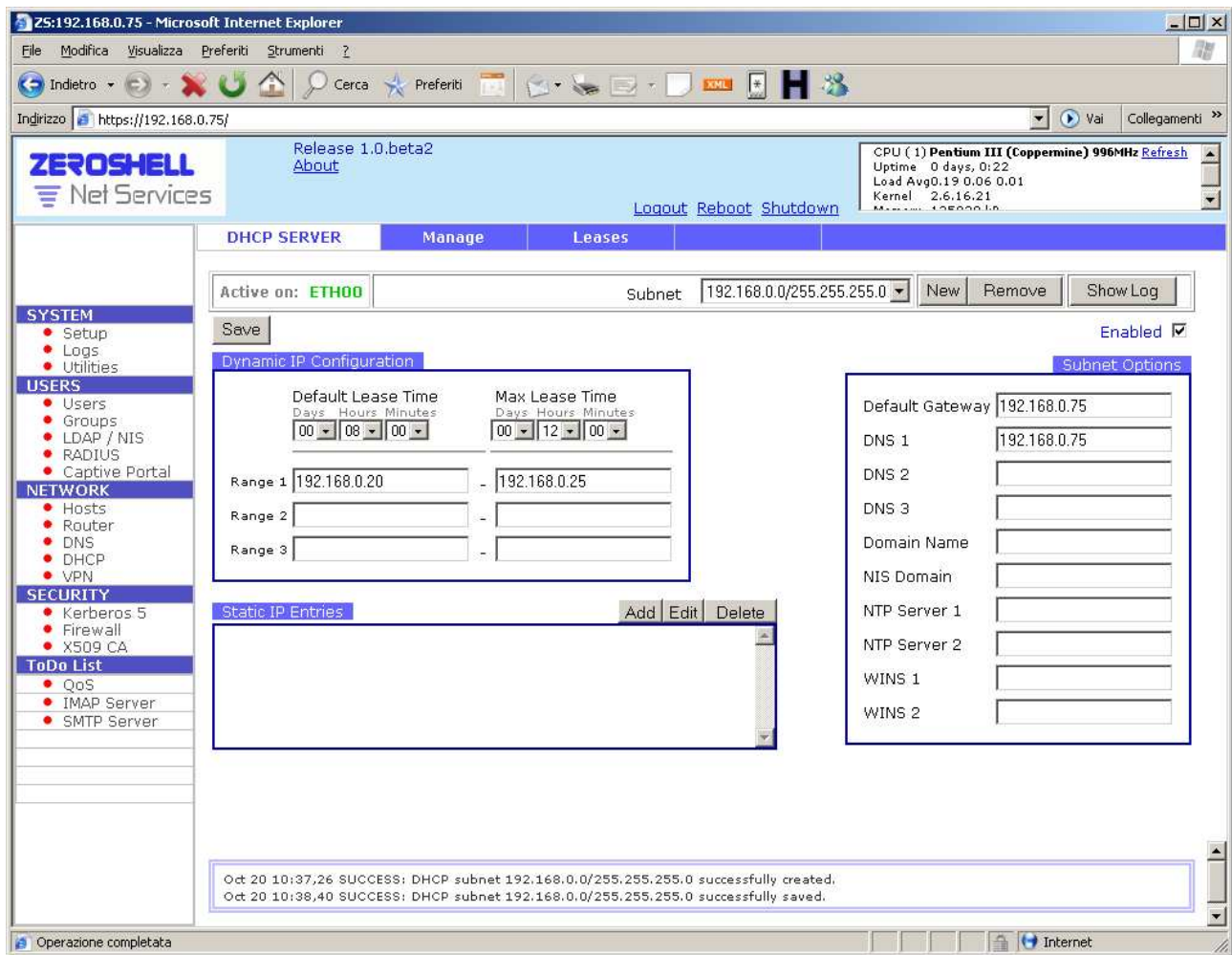
Static IP Entries Add Edit Delete

Default Gateway 192.168.0.75
DNS 1 192.168.0.75
DNS 2
DNS 3
Domain Name
NIS Domain
NTP Server 1
NTP Server 2
WINS 1
WINS 2

Oct 20 10:24:07 SUCCESS: Session opened from host 192.168.0.1 (Admin)
Oct 20 10:37:26 SUCCESS: DHCP subnet 192.168.0.0/255.255.255.0 successfully created.

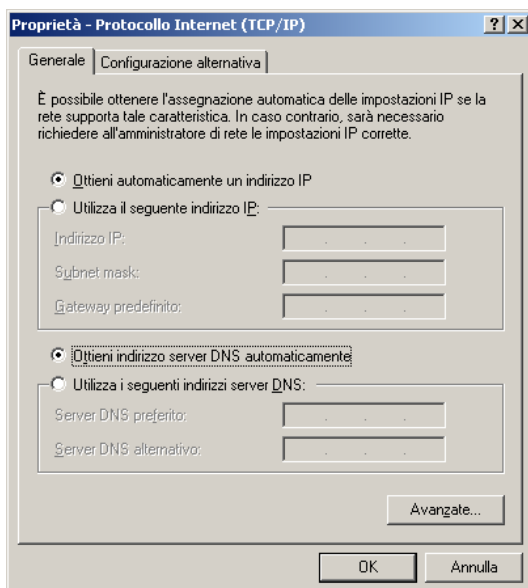
Internet

A questo punto definire il range di indirizzamenti che si vuole utilizzare:



e salvare.

Notare che in automatico Zeroshell si impone come default gateway e DNS server ma che può essere modificato!
Ora configuriamo il nostro pc per prendere ip in modo dinamico:



Dopo pochi attimi ecco che il nostro pc riesce ad ottenere l'indirizzo dal dhcp server:

C:\Documents and Settings\Administrator>ipconfig /all

Configurazione IP di Windows

Nome host : PIZZA
Suffisso DNS primario :
Tipo nodo : Sconosciuto
Routing IP abilitato. : No
Proxy WINS abilitato : No

Scheda Ethernet Connessione alla rete locale (LAN):

Suffisso DNS specifico per connessione:
Descrizione : 3Com 3C920B-EMB Integrated Fast

Ethernet Controller

Indirizzo fisico. : 00-26-54-0B-31-CA

DHCP abilitato. : Sì

Configurazione automatica abilitata : Sì

Indirizzo IP. : 192.168.0.25

Subnet mask : 255.255.255.0

Gateway predefinito : 192.168.0.75

Server DHCP : 192.168.0.75

Server DNS : 192.168.0.75

Lease ottenuto. : venerdì 20 ottobre 2006 10.41.59

Scadenza lease : venerdì 20 ottobre 2006 18.41.59

Routes statiche verso reti remote:

Capita di avere sedi remote connesse tramite un secondo router connesso in rete locale.

Se per esempio raggiungiamo la sede remota 192.168.50.0/24 tramite il router 192.168.0.254 ecco che possiamo ruotare le richieste che arrivano a Zeroshell (poiché default router) sul router giusto. Dal menu **ROUTER** tramite bottone **ADD** possiamo specificare la rete remota:

The screenshot shows the Zeroshell Net Services web interface in a Microsoft Internet Explorer browser window. The address bar shows <https://192.168.0.75/>. The interface has a sidebar menu on the left with categories: SYSTEM (Setup, Logs, Utilities), USERS (Users, Groups, LDAP / NIS, RADIUS, Captive Portal), NETWORK (Hosts, Router, DNS, DHCP, VPN), SECURITY (Kerberos 5, Firewall, X509 CA), and ToDo List (QoS, IMAP Server, SMTP Server). The main content area is titled 'ROUTER' and includes tabs for Manage, RIPv2, NAT, and Virtual Server. Under the 'ROUTER' tab, there's a 'Forwarding' section with 'ACTIVE' status and an 'Enabled' checkbox. Below this is a 'STATIC ROUTES' table with columns: Destination, Netmask, Type, Metric, Gateway, Interface, and State. The table contains one entry: 'DEFAULT GATEWAY' with Netmask '0.0.0.0', Type 'Net', Metric '0', Gateway '192.168.1.254', and State 'Up'. At the bottom, a log shows two successful messages: 'DHCP subnet 192.168.0.0/255.255.255.0 successfully saved.' and 'Session opened from host 192.168.0.25 (Admin)'.

The screenshot shows the 'Static Route Config' dialog box. It has a title bar with the URL <https://192.168.0.75 - Static Route Config>. The dialog is titled 'STATIC ROUTE' and has two radio buttons: 'Network' (selected) and 'Host'. Below the radio buttons are four input fields: 'Destination' (192.168.50.0), 'Netmask' (255.255.255.0), 'Gateway' (192.168.0.254), and 'Metric' (1). There is also an 'Interface' dropdown menu. At the bottom are 'OK' and 'Cancel' buttons. The status bar at the bottom of the browser window shows 'Operazione completata'.

La voce metric indica come sempre il “costo” (la precedenza nel reindirizzamento) per raggiungere la rete remota. E’ possibile specificare la stessa rete remota quindi attraverso 2 router diversi che usano linee a diverso costo (o diversa velocità).

25:192.168.0.75 - Microsoft Internet Explorer

File Modifica Visualizza Preferiti Strumenti ?

Indietro Cerca Preferiti

Indirizzo <https://192.168.0.75/> Vai Collegamenti >>

Release 1.0.beta2
[About](#)

[Logout](#) [Reboot](#) [Shutdown](#)

CPU (1) **Pentium III (Coppermine) 996MHz** [Refresh](#)
 Uptime 0 days, 0:45
 Load Avg 0.00 0.00 0.00
 Kernel 2.6.16.21
 Memory 125000 kb

SYSTEM

- Setup
- Logs
- Utilities

USERS

- Users
- Groups
- LDAP / NIS
- RADIUS
- Captive Portal

NETWORK

- Hosts
- Router
- DNS
- DHCP
- VPN

SECURITY

- Kerberos 5
- Firewall
- X509 CA

ToDo List

- QoS
- IMAP Server
- SMTP Server

ROUTER Manage RIPv2 NAT Virtual Server

Forwarding: **ACTIVE** ☒ Enabled **DEFAULT GW** **ROUTING TABLE** **CHECK IP**

STATIC ROUTES [Add](#) [Change](#) [Delete](#)

	Destination	Netmask	Type	Metric	Gateway	Interface	State
○	192.168.50.0	255.255.255.0	Net	1	192.168.0.254		Up
○	DEFAULT GATEWAY	0.0.0.0	Net	0	192.168.1.254		Up

Oct 20 10:47,35 SUCCESS: Session opened from host 192.168.0.25 (Admin)
 Oct 20 10:49,00 SUCCESS: Static route 192.168.50.0/255.255.255.0 via 192.168.0.254 metric 1 successfully added.

Operazione completata

Zeroshell consente di attivare sulle proprie schede anche il protocollo RIP v2. Questo protocollo se attivato su tutti i router interni consente lo scambio di informazioni fra gli stessi in modo dinamico. Sostanzialmente i vari router con ripv2 attivato si comunicheranno in modo periodico le reti che essi possono ruotare, senza quindi la necessità di doverle specificare a mano su ogni dispositivo come abbiamo fatto poco fa per esempio. Esistono vantaggi e svantaggi nel fare ciò...meditare.

Servizi attraverso Virtual Server:

E' possibile distribuire dei servizi interni anche per la rete esterna. Per esempio si può decidere di pubblicare un sito web ospitato su un server interno.

Dal menu **ROUTER** scegliere la voce **VIRTUAL SERVER** :

Virtual Server

View Close

Input Interface ALL	Protocol TCP	Local Port	Remote IP	Remote Port	Add Delete
------------------------	-----------------	------------	-----------	-------------	---------------

Interface	Protocol	Local Port	Real Servers
-----------	----------	------------	--------------

Notes:
Remote IP field can be the IP address of a single real server or the IP range (ex. 192.168.0.100-192.168.0.110) of a server farm. In the latter case, Round Robin algorithm is used to distribute the requests to all the real servers. It is important note that only load balancing is guaranteed and not fault tolerance

Operazione completata Internet

Si può definire quale interfaccia deve accettare la richiesta, su quale protocollo, su quale porta del protocollo. Poi quale sia il server interno e su quale porta questo ascolti. Per esempio, se ho un server web interno (192.168.0.100) che pubblica il sito web sulla porta 80 del protocollo TCP e decido di concedere a chi è fuori dalla mia rete di visualizzare le mie pagine web (quindi entrando dalla scheda di rete esterna del mio Zeroshell) dovrò configurarlo così:

https://192.168.0.75 - Port Forwarding - Microsoft Internet Explorer

Virtual Server

View Close

Input Interface ETH01	Protocol TCP	Local Port 80	Remote IP 192.168.0.100	Remote Port 80	Add Delete
--------------------------	-----------------	------------------	----------------------------	-------------------	---------------

Interface	Protocol	Local Port	Real Servers
-----------	----------	------------	--------------

Notes:
Remote IP field can be the IP address of a single real server or the IP range (ex. 192.168.0.100-192.168.0.110) of a server farm. In the latter case, Round Robin algorithm is used to distribute the requests to all the real servers. It is important note that only load balancing is guaranteed and not fault tolerance

Operazione completata Internet

https://192.168.0.75 - Port Forwarding - Microsoft Internet Explorer

Virtual Server

View Close

Input Interface ALL	Protocol TCP	Local Port	Remote IP	Remote Port	Add Delete
------------------------	-----------------	------------	-----------	-------------	---------------

Interface	Protocol	Local Port	Real Servers
ETH01	TCP	80	192.168.0.100:80

Notes:
Remote IP field can be the IP address of a single real server or the IP range (ex. 192.168.0.100-192.168.0.110) of a server farm. In the latter case, Round Robin algorithm is used to distribute the requests to all the real servers. It is important note that only load balancing is guaranteed and not fault tolerance

Operazione completata Internet

Ovviamente il router della linea adsl dovrà essere configurato per fare entrare ogni sorta di richiesta (o almeno porta 80 tcp) sull'interfaccia di Zeroshell. Con un router 3com :

http://192.168.1.254/ - Microsoft Internet Explorer

File Modifica Visualizza Preferiti Strumenti ?

Indietro Cerca Preferiti XML H

Indirizzo http://192.168.1.254/ Vai Collegamenti >>

3COM

Setup Wizard
LAN Settings
Wireless Settings
Internet Settings
Routing
Firewall
Special Applications
Virtual Servers
Client IP Filters
MAC Address Filtering
DMZ
Advanced
SNMP
System Tools
Status and Logs

Log Out

OfficeConnect® ADSL Wireless 11g Firewall Router

DMZ

If you have a client PC that cannot run an Internet application properly from behind the firewall, you can open the client up to unrestricted two-way Internet access. This may be necessary if the NAT feature is causing problems with an application such as a game or video conferencing application. Use this feature on a temporary basis. **The computer in the DMZ is not protected from hacker attacks.**

Enable DMZ

DMZ ☒ ENABLE ☐ DISABLE

IP Address of Virtual DMZ Host

	Public IP Address	Client PC IP Address
1	151.37.184.157	192.168.1.1
2	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>	192.168.1.0
3	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>	192.168.1.0
4	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>	192.168.1.0
5	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>	192.168.1.0
6	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>	192.168.1.0
7	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>	192.168.1.0
8	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>	192.168.1.0

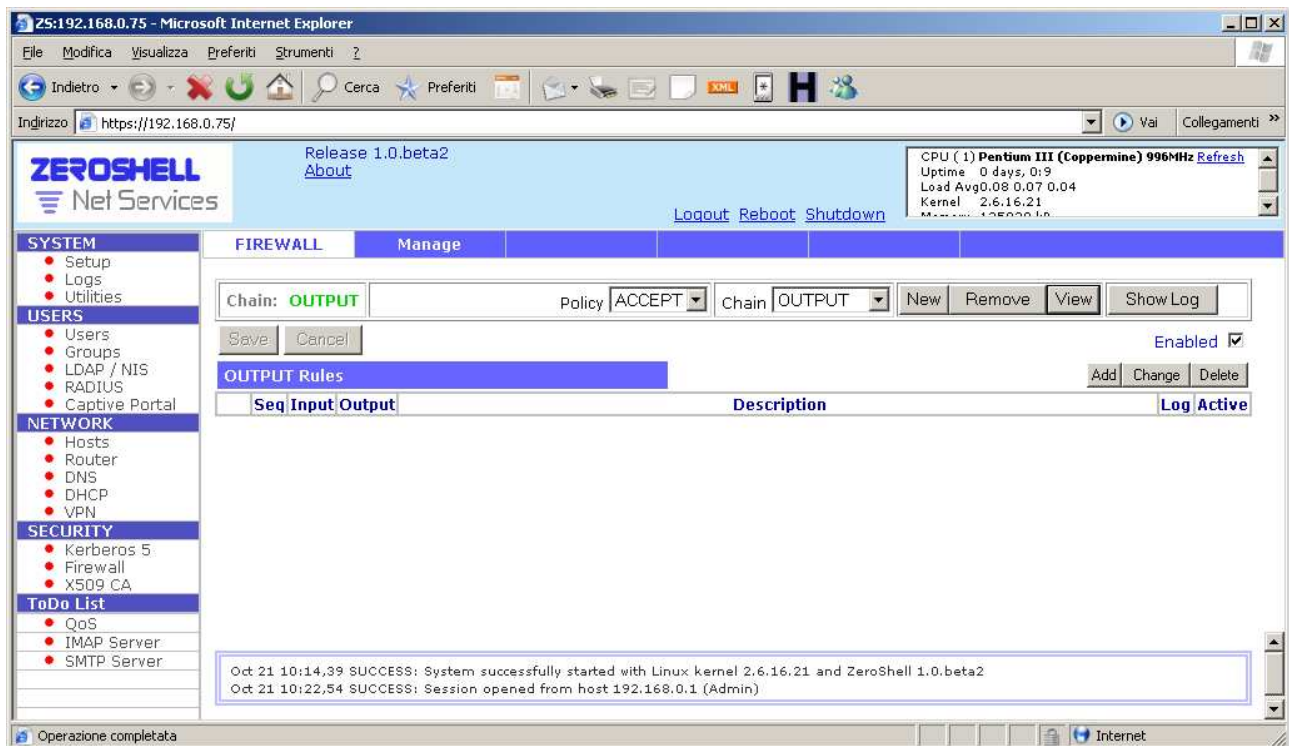
Help Apply Cancel

Internet

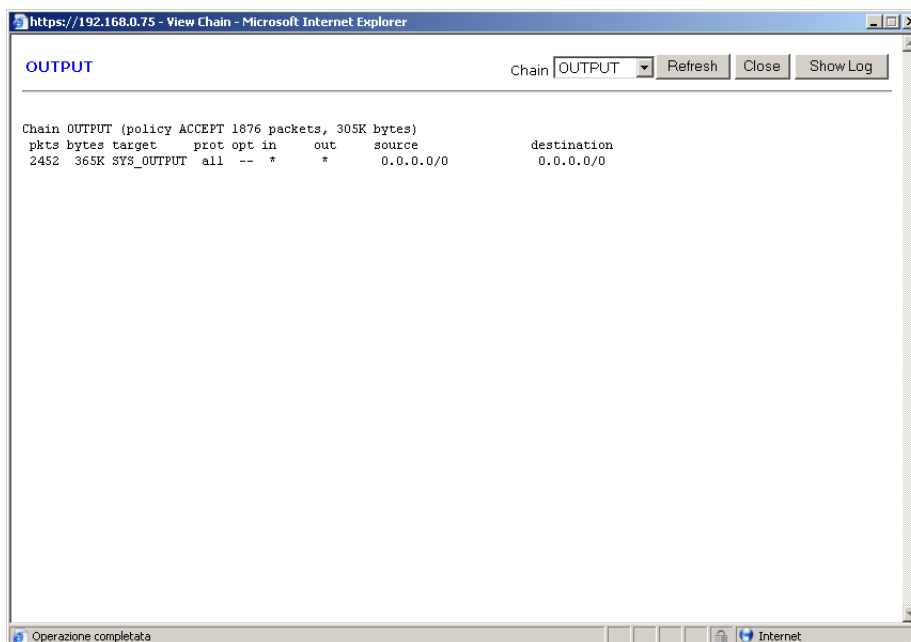
Dove 192.168.1.1 è la ETH01 esterna di Zeroshell.

Sicurezza: verificare le regole del firewall

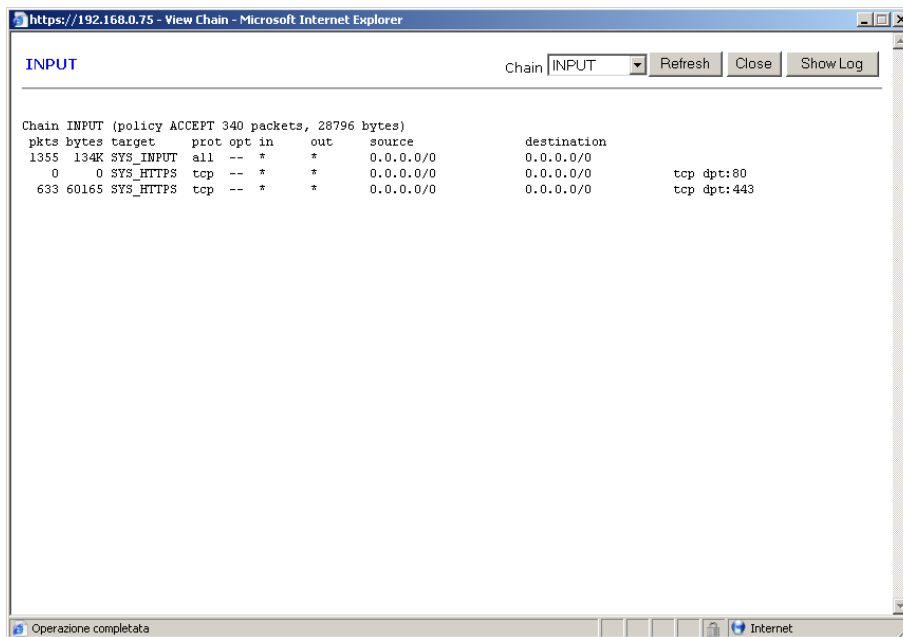
Tramite il menu **FIREWALL** è possibile verificare le regole impostate di default sul firewall. Scegliendo la **CHAIN OUTPUT** e cliccando su **VIEW**:



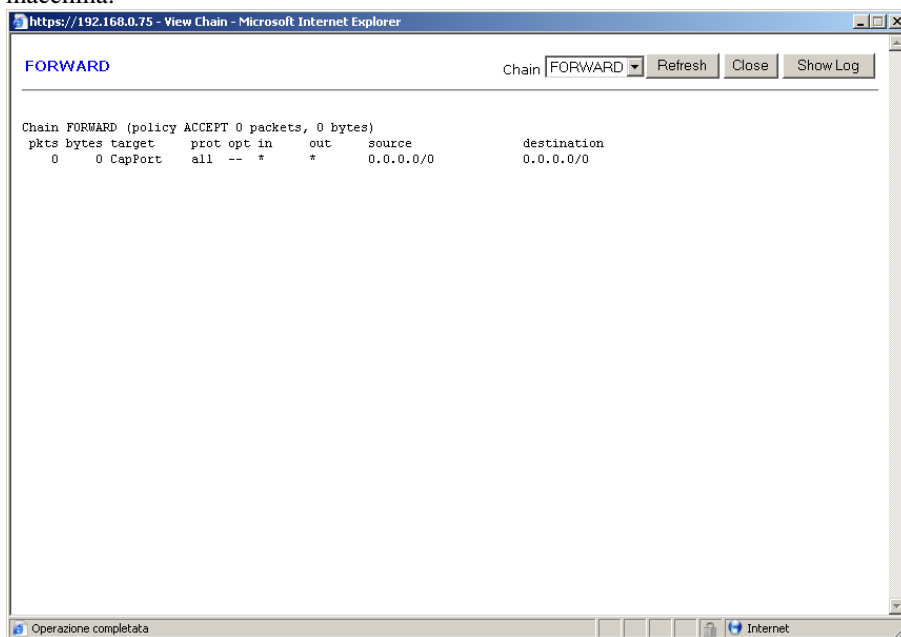
Ecco le regole attive di default in uscita:



Scegliendo la **CHAIN INPUT** e cliccando su **VIEW** , ecco le regole attive di default in entrata nella macchina:



Scegliendo la **CHAIN FORWARD** e cliccando su **VIEW** , ecco le regole attive di default di attraversamento della macchina:



Come si nota il firewall viene attraversato dall'interno (ETH00) all'esterno (ETH01) senza problemi; in senso opposto invece non essendo specificato nulla, non viene attraversato da nulla.