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)

P**roteggere 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

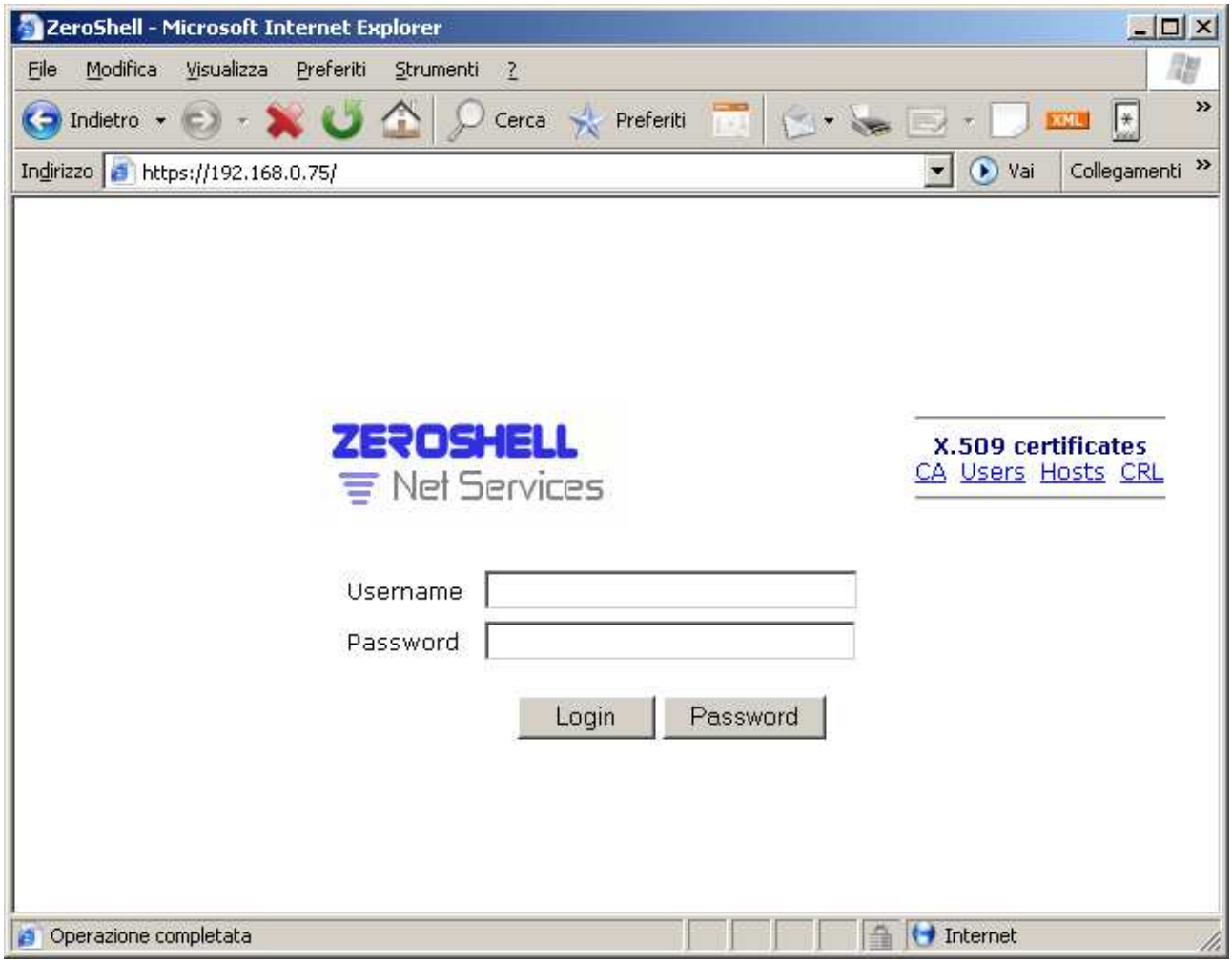
Vorrei comunque sottolineare che Zeroshell integra molte altre funzioni avanzate per reti ben più complesse; e che quindi con la presenza di Zeroshell la nostra rete diventa estremamente scalabile.

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:



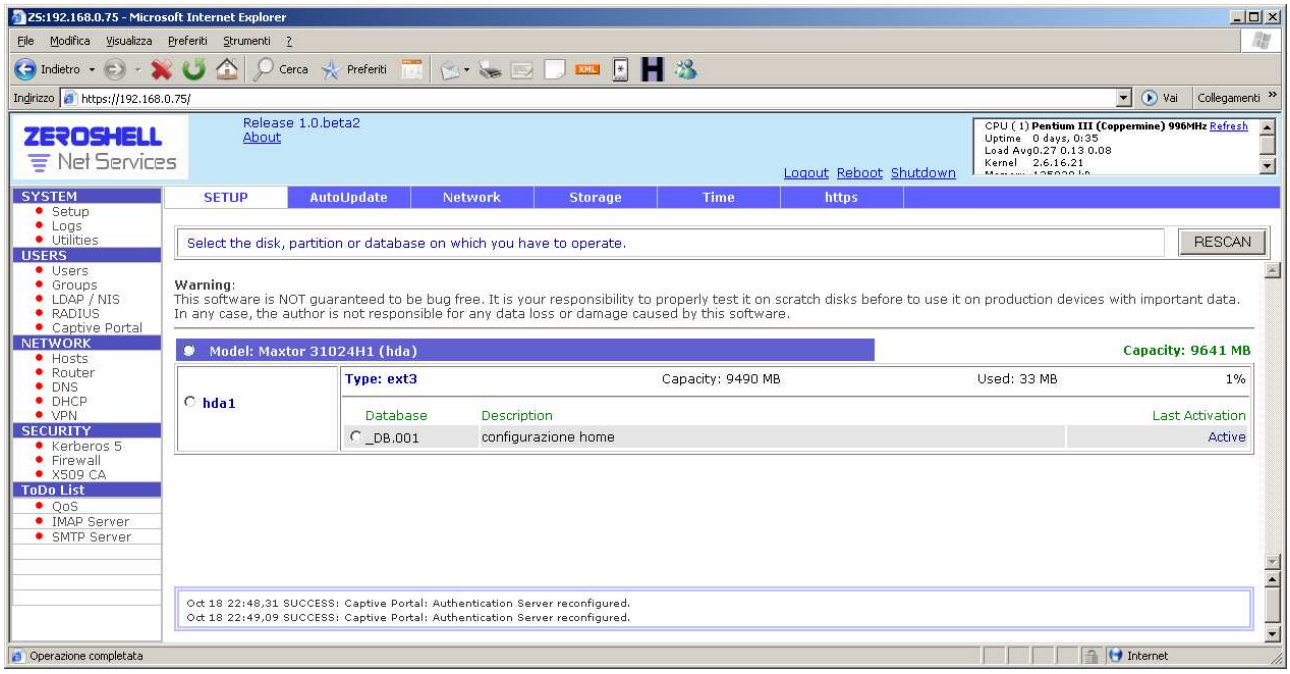
Entrare come:

User: admin
Password: zeroshell

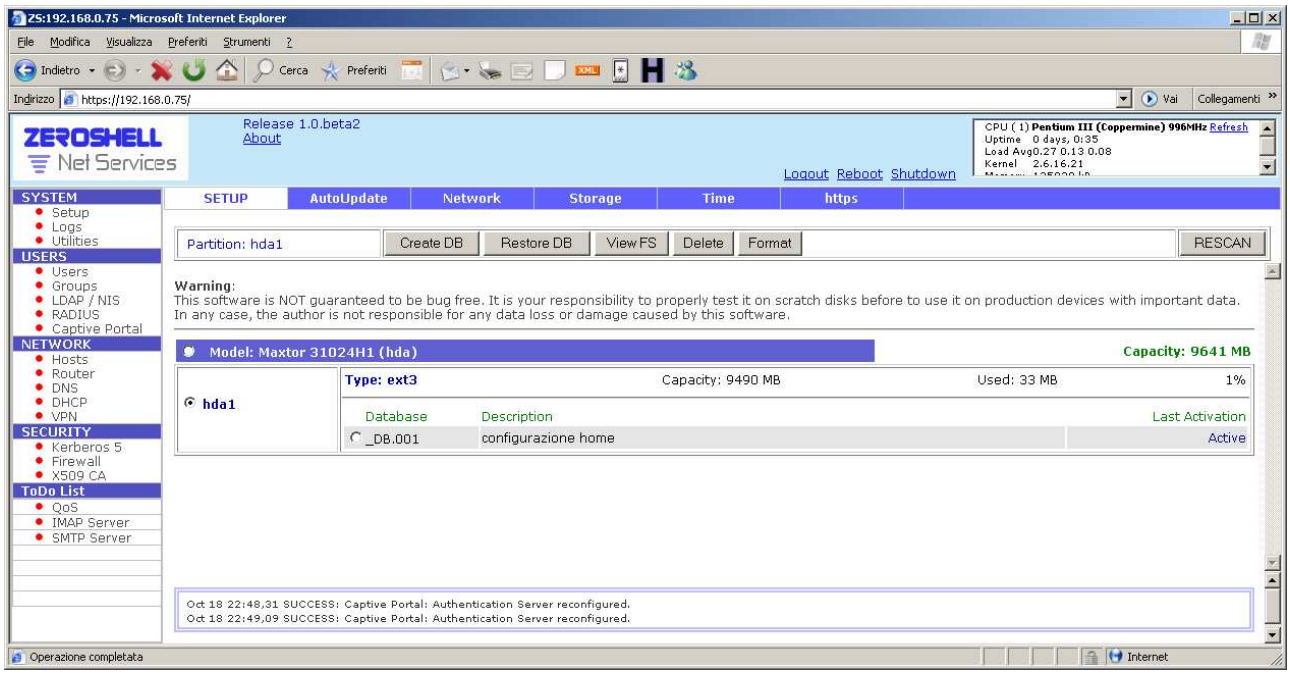
A questo punto dall'interfaccia web possiamo accedere ad ogni menu di configurazione del sistema.

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):**



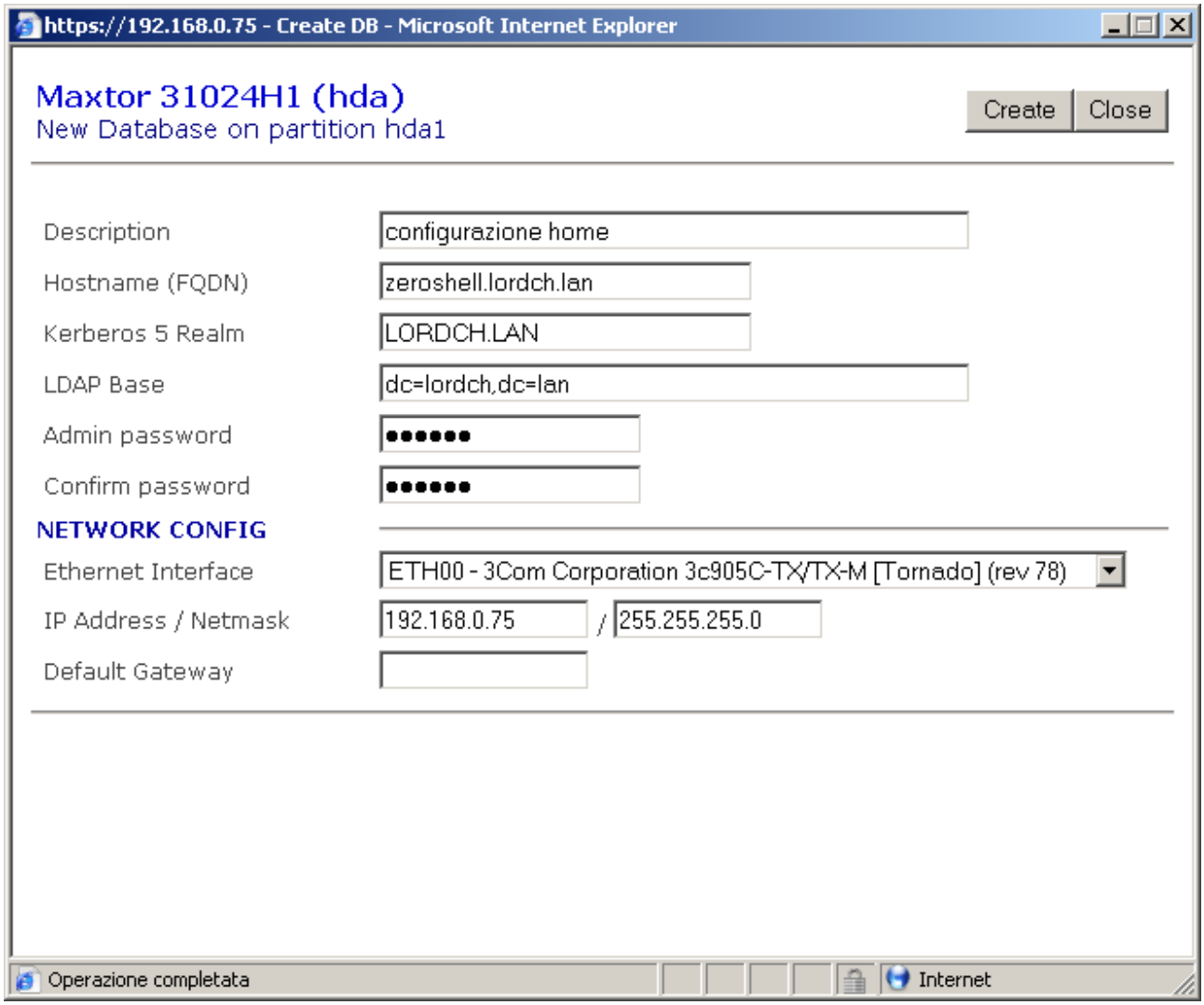
Subito ci viene mostrato il disco presente nel sistema. A questo punto selezionando le partizioni in esso presenti (se esistenti) decido di cancellarle una alla volta premendo sul tasto **DELETE**:



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).

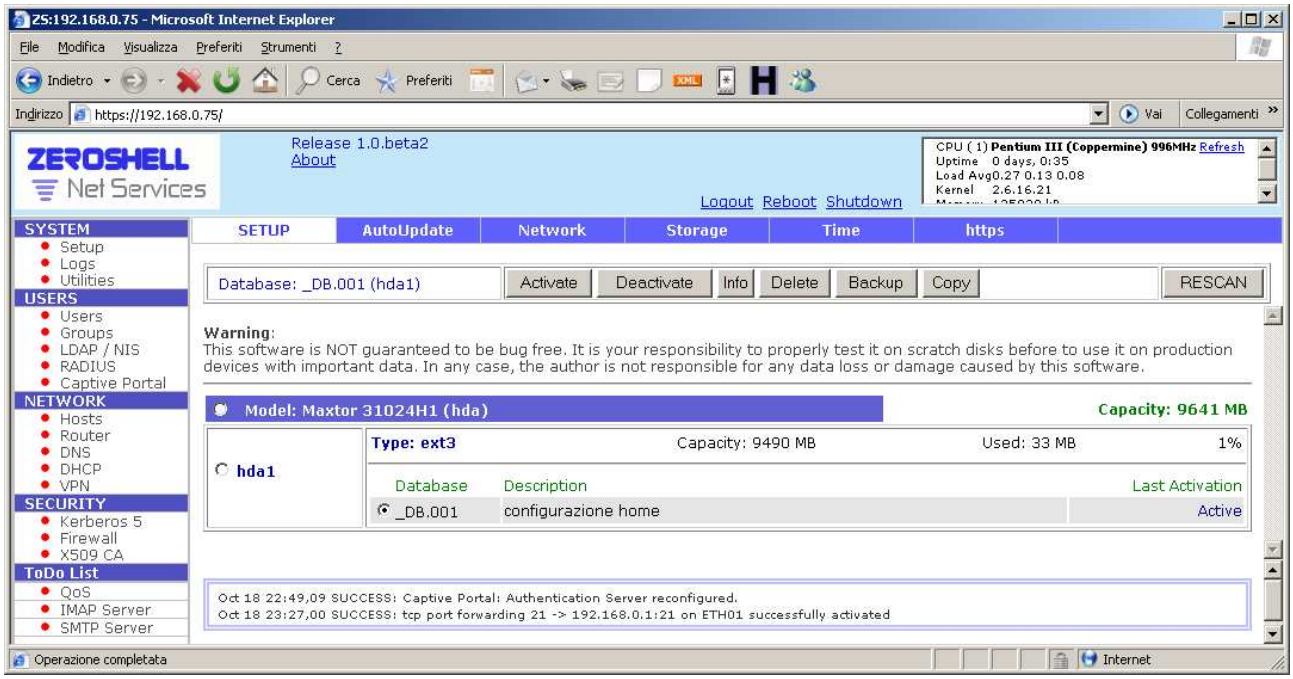
Memorizzare le nostre impostazioni:

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:



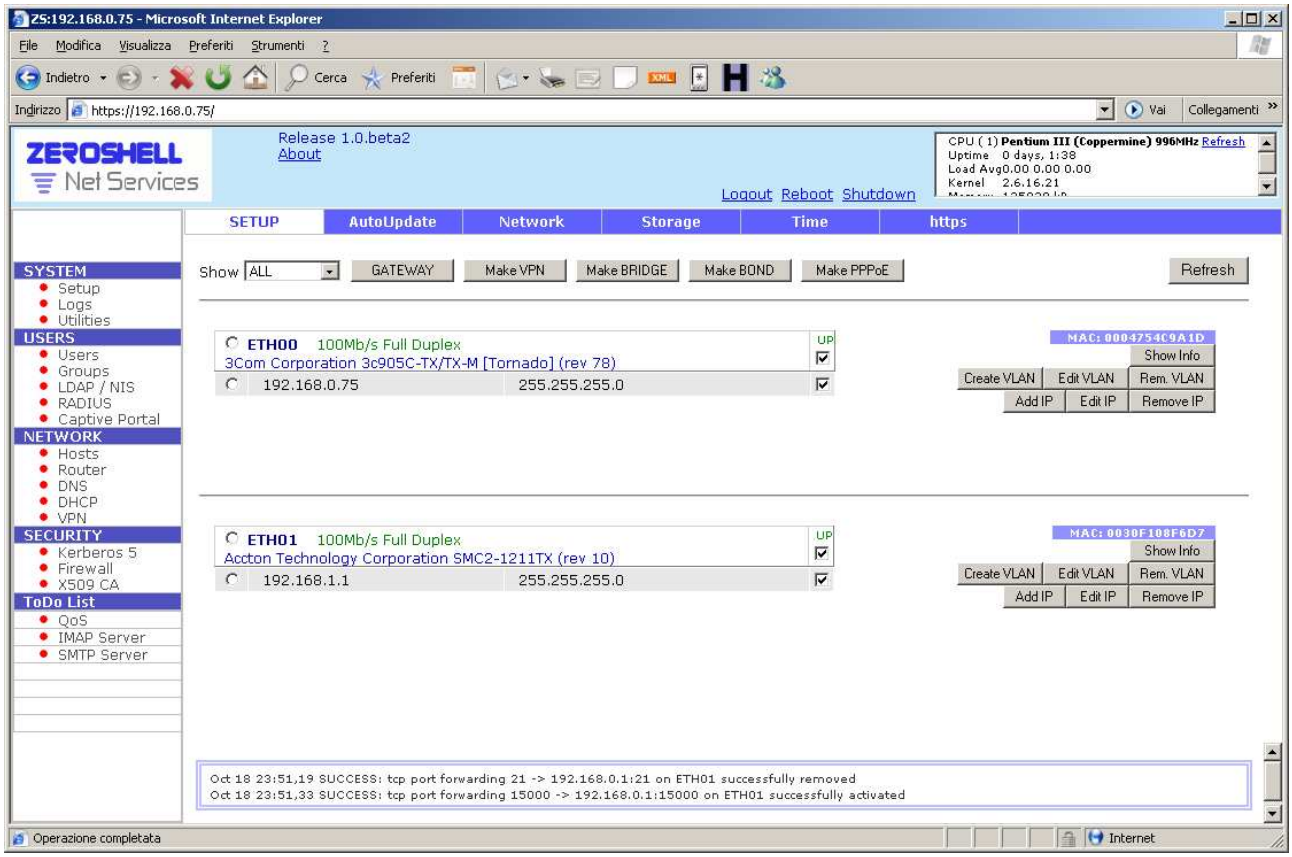
Ci viene chiesta una breve descrizione della configurazione; il nome completo del nostro sistema; il dominio eventuale Kerberos e LDAP; di settare una nuova password dell'utente "admin"; l'indirizzo ip dell'interfaccia generalmente primaria che viene usata per configurare il sistema; l'eventuale default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

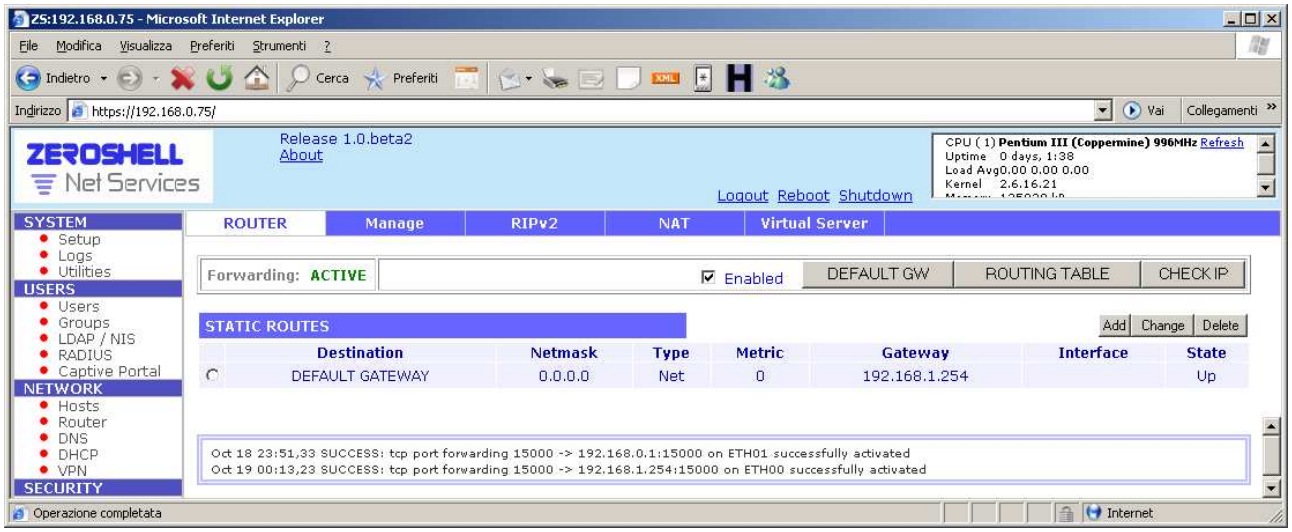

ZS:192.168.0.75 - Microsoft Internet Explorer
File Modifica Visualizza Preferiti Strumenti ?
Indietro Cerca Preferiti
Indirizzo https://192.168.0.75/
Vai Collegamenti
ZEROSHELL
Net Services
Release 1.0.beta2
About
Logout Reboot Shutdown
CPU (1) Pentium III (Coppermine) 996MHz Refresh
Uptime 0 days, 0:35
Load Avg0.27 0.13 0.08
Kernel 2.6.16.21
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)
Activate
Deactivate
Info
Delete
Backup
Copy
RESCAN
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:

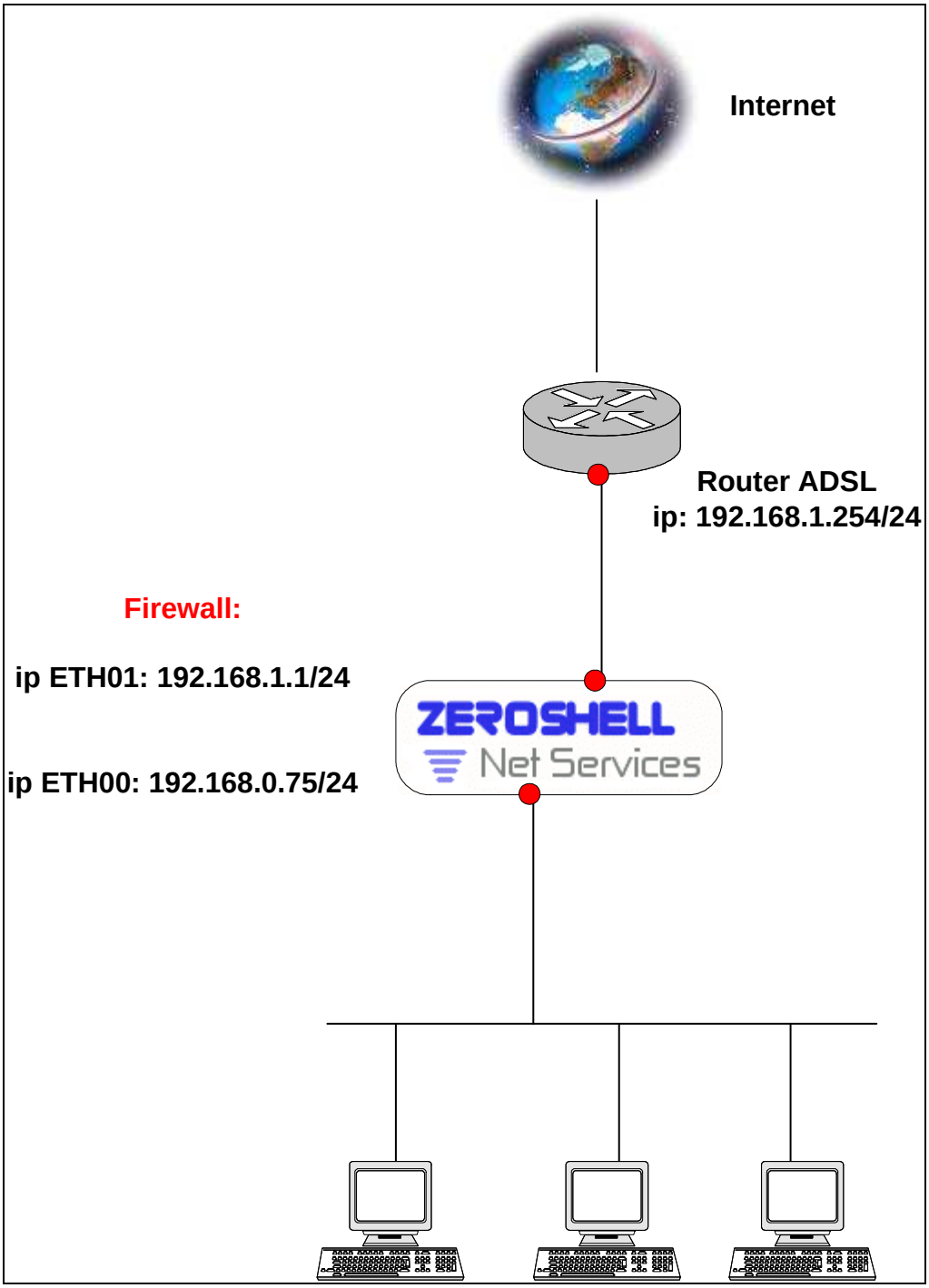
Una volta preparato il disco e creato il file di configurazione possiamo passare alla configurazione delle schede di rete dal menu **SETUP** alla voce **NETWORK**:



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 la 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:



la mia rete diventa quindi:

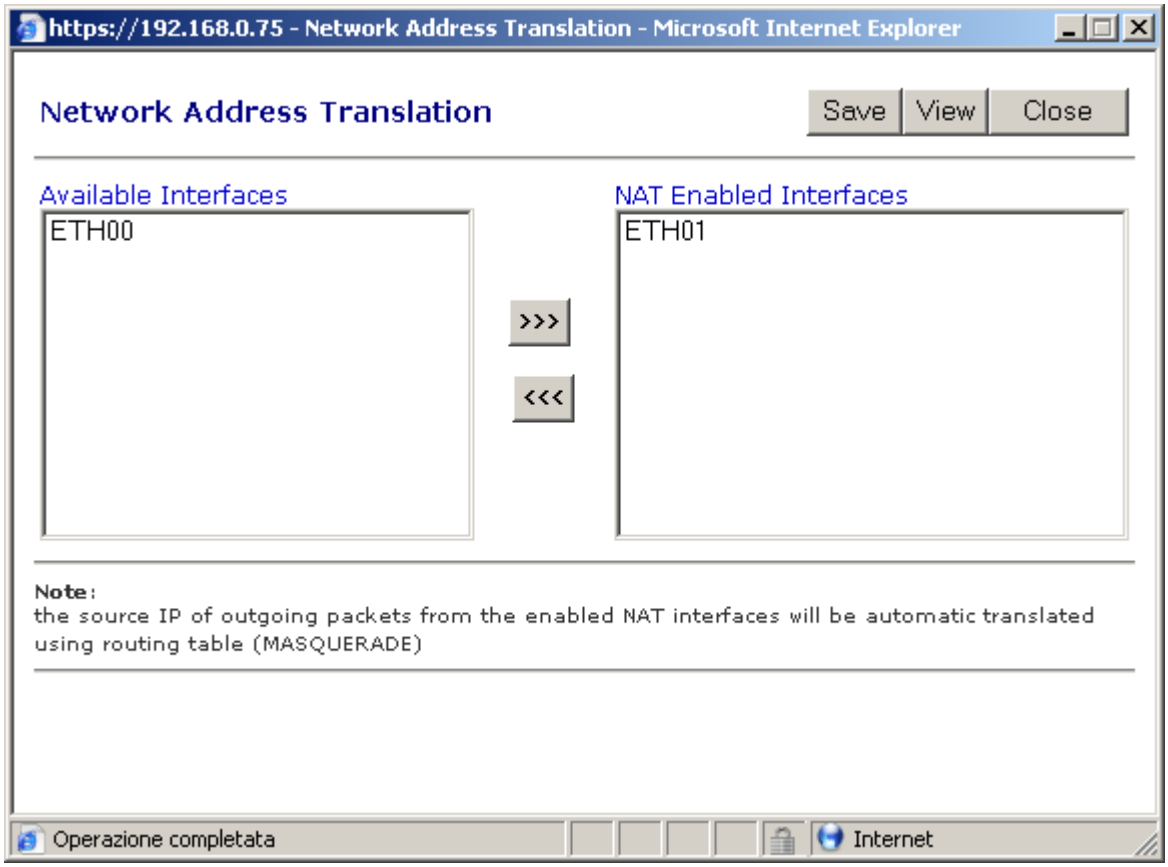


E’ facile intuire che una situazione del genere ci consente di sfruttare molte potenzialità del nostro sistema Zeroshell; per esempio possiamo scrivere delle politiche di protezione della nostra rete interna (192.168.0.0/24); oppure possiamo usare la funzione di Captive Portal per imporre utenza e password 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:

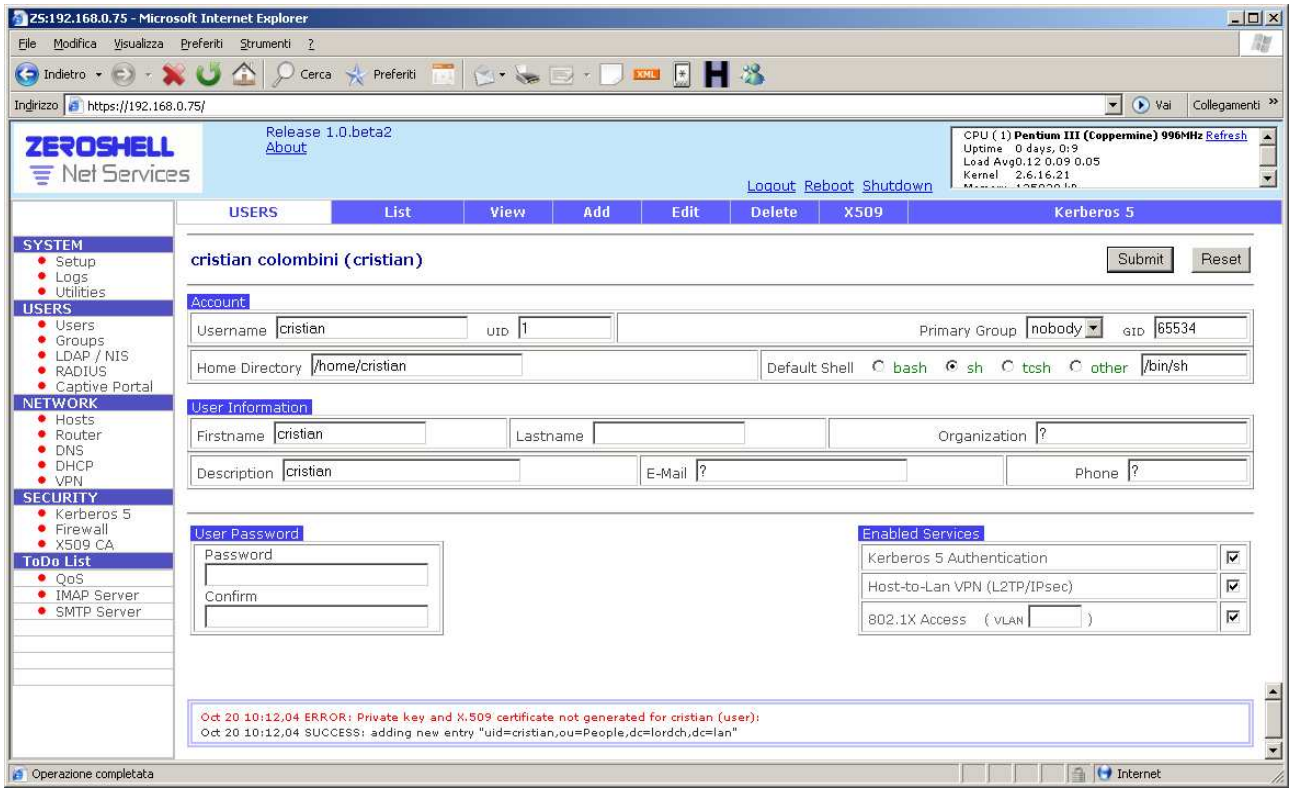


La rete dietro l'interfaccia ETH00 venga mascherata da ETH01. A questo punto i pc della rete riescono a navigare.

Attivare il Captive Portal:

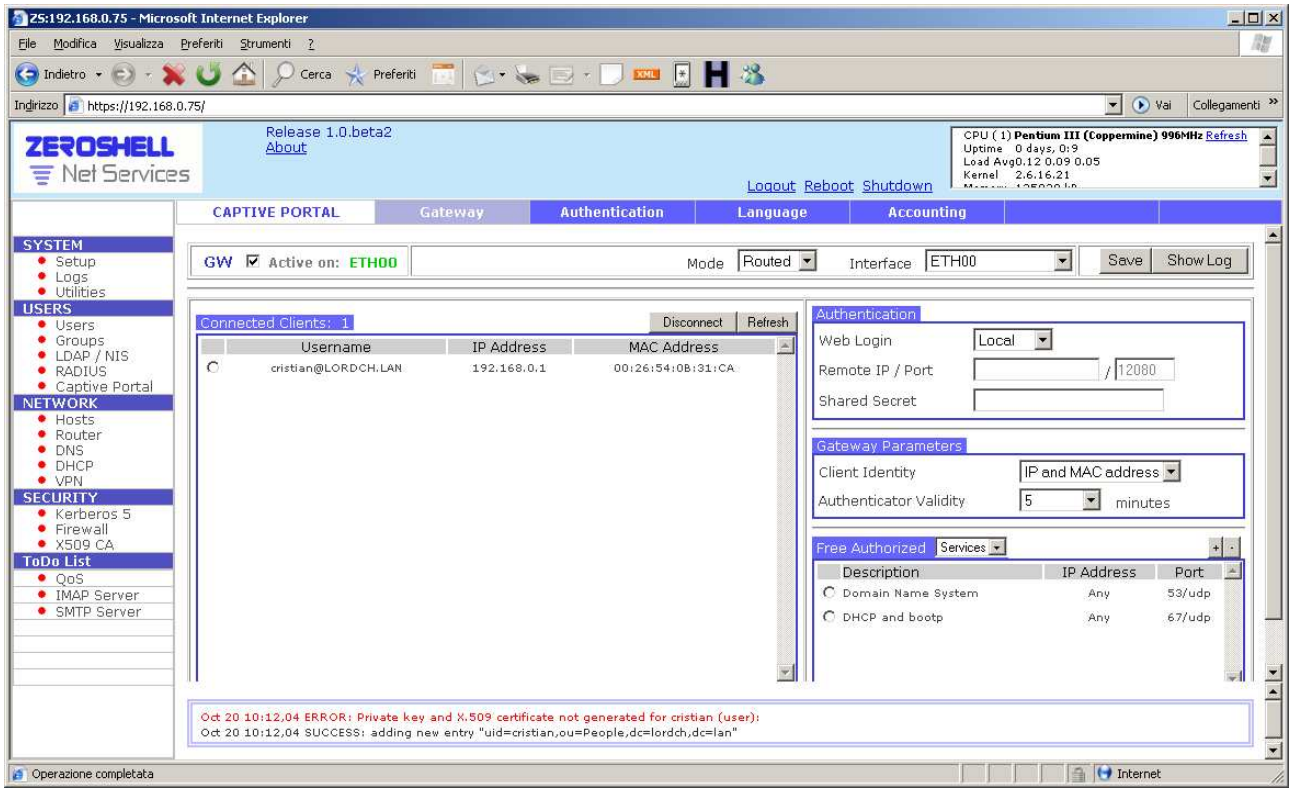
Si tratta di una utilissima funzione che richiede l'autenticazione con utente e password prima di consentire il passaggio di richieste verso l'esterno (per esempio prima di consultare internet, scaricare posta, ecc).

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:

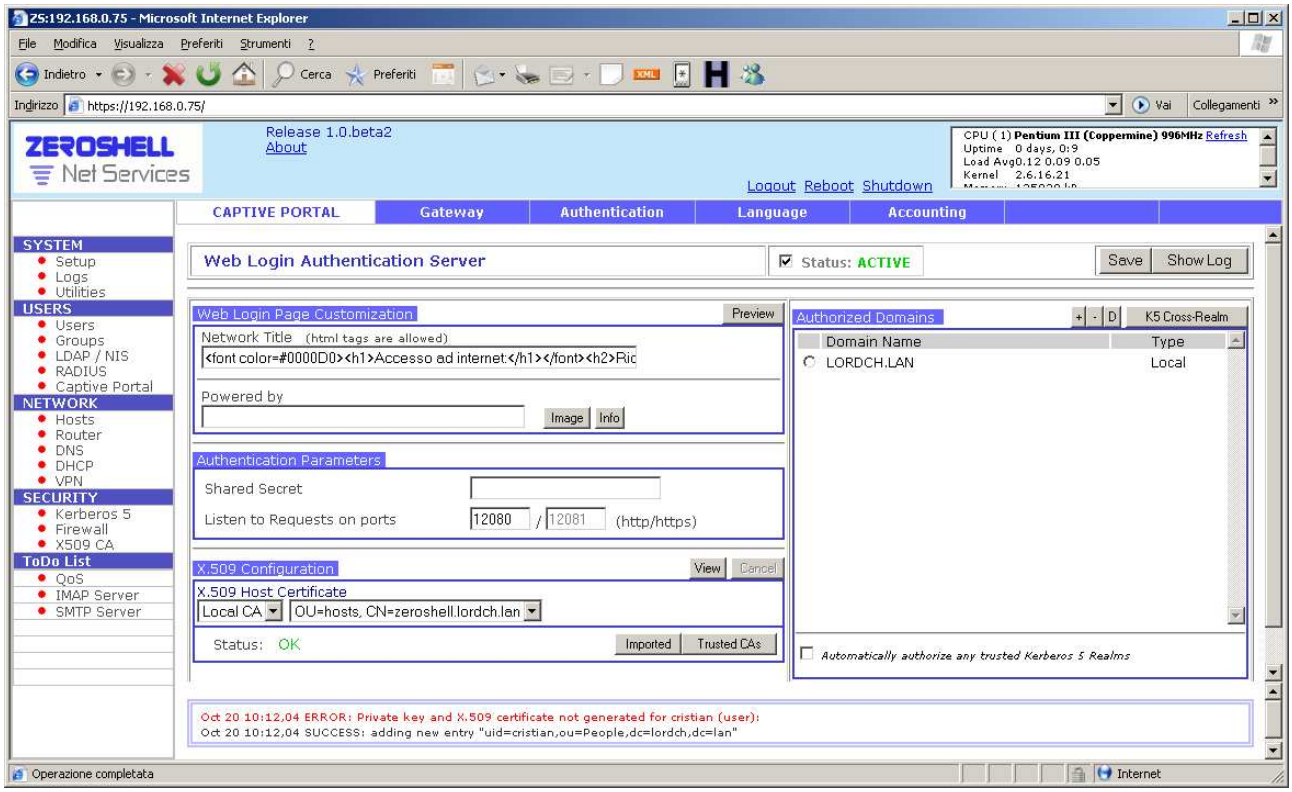


Ricordiamoci che lo user sarà la voce **USERNAME.**

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:

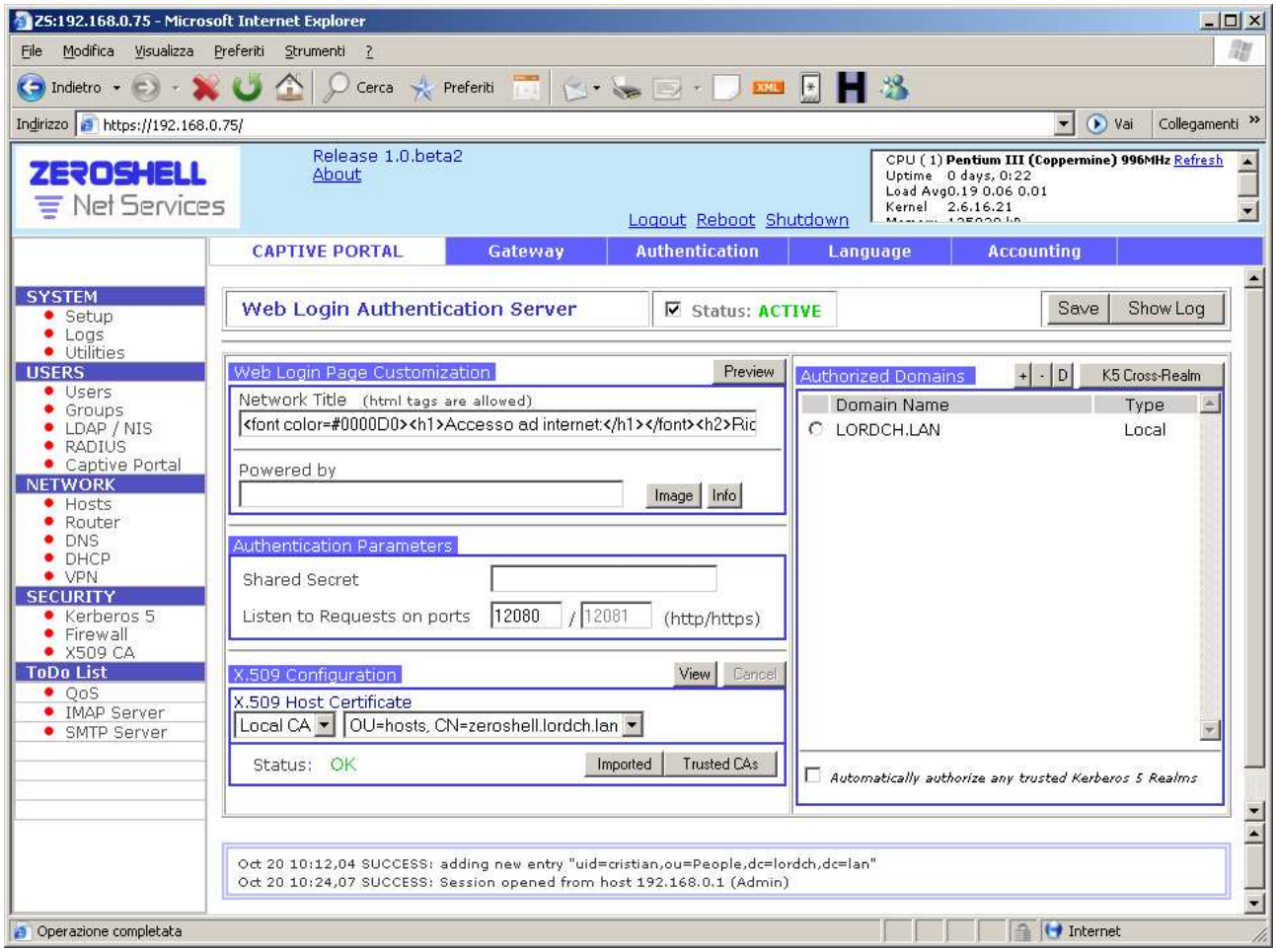


A questo punto se chiudiamo il browser e lo riapriamo, nel momento in cui cerchiamo di connetterci ad internet o alla stessa pagina di configurazione di Zeroshell, ci viene chiesto di autenticarci. Qui sotto ho personalizzato la pagina:

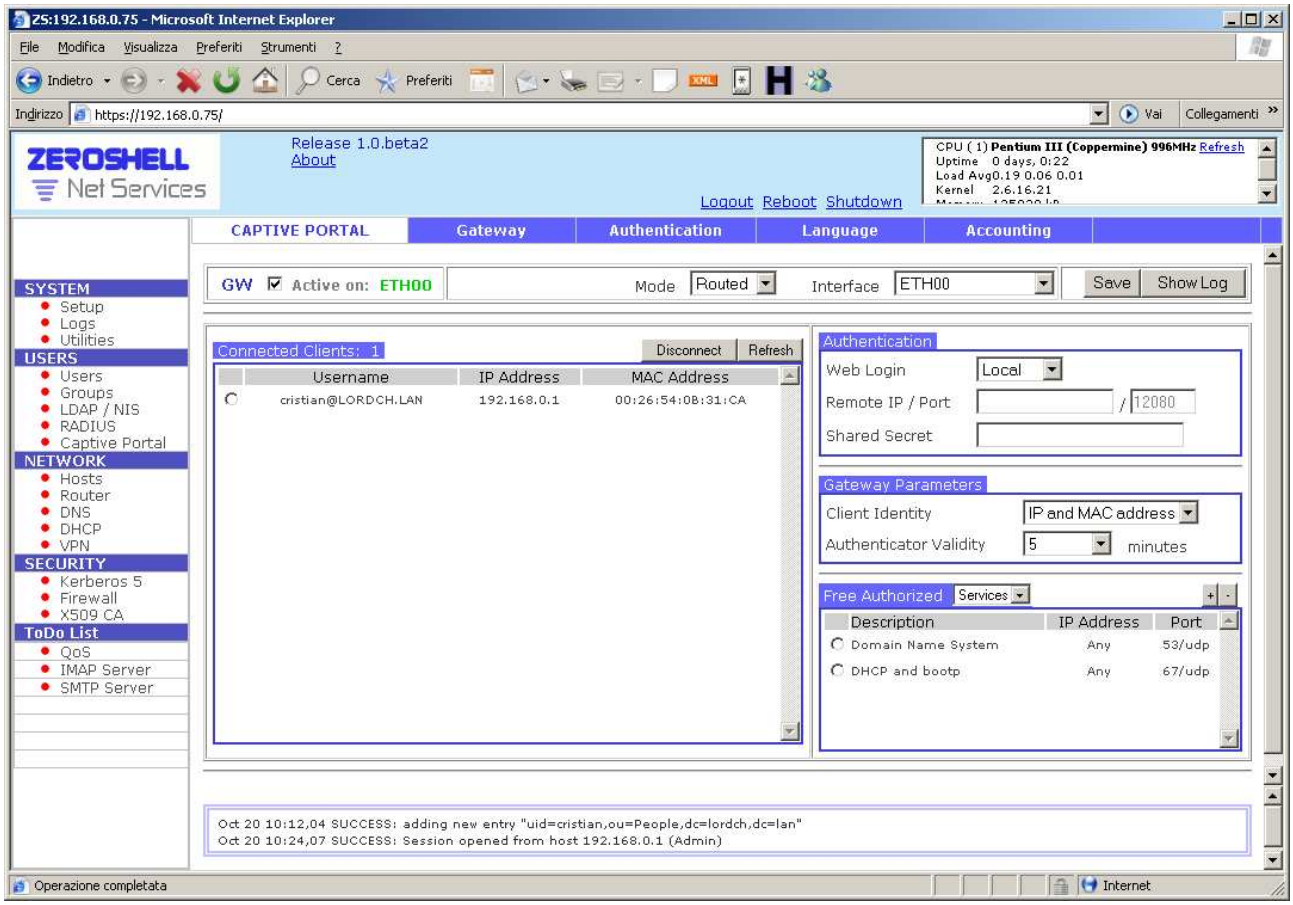
Dopo aver inserito le credenziali si apre un popup:

che mostra chiaro messaggio di non chiudere questa finestra finché si vuole continuare ad usare internet.

Si può personalizzare la pagina di richiesta autenticazione dalla voce **AUTHENTICATION** utilizzando semplice codice HTML:

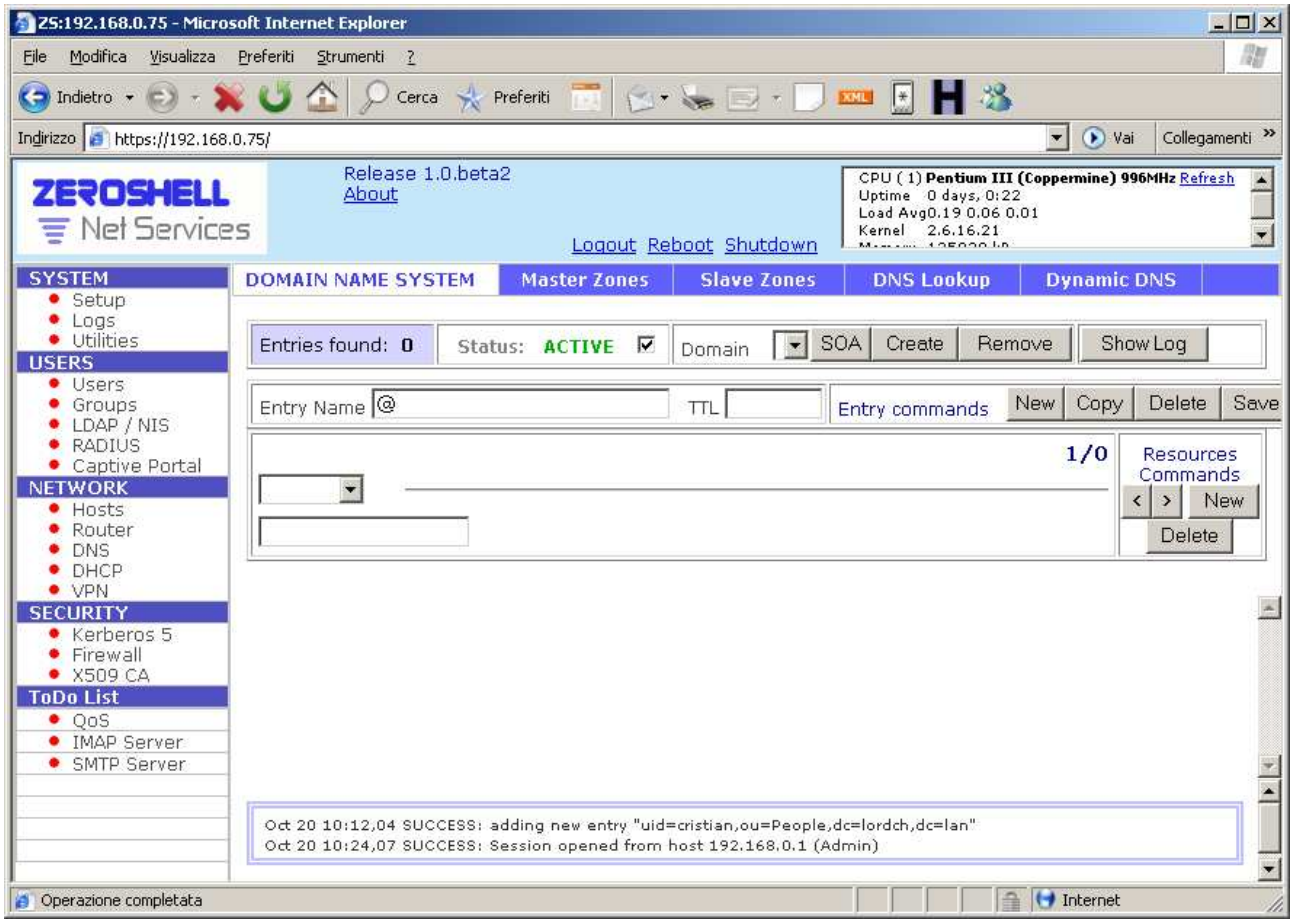


Interessante verificare alla voce **GATEWAY** le utenze autenticate e come tramite selezione delle stesse si possano disconnettere tramite bottone **DISCONNECT**:

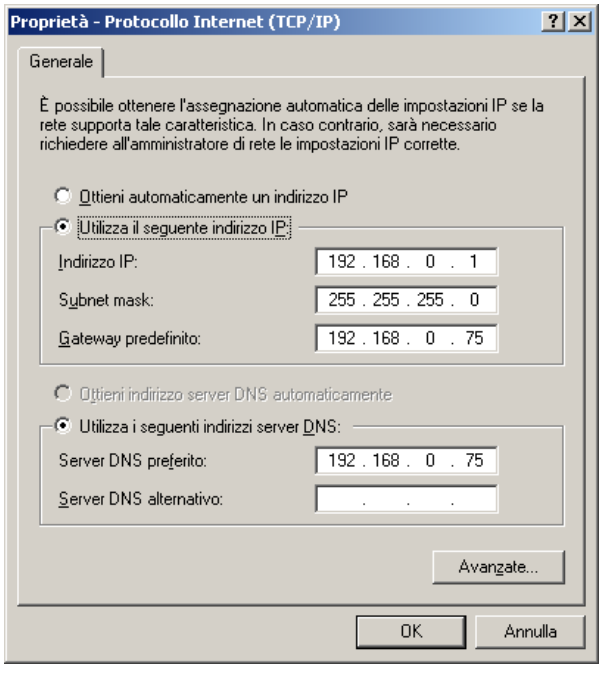

ZS:192.168.0.75 - Microsoft Internet Explorer
File Modifica Visualizza Preferiti Strumenti ?
Indietro Cerca Preferiti
Indirizzo https://192.168.0.75/
Vai Collegamenti
ZEROSHELL
Net Services
Release 1.0.beta2
About
Logout Reboot Shutdown
CPU (1) Pentium III (Coppermine) 996MHz Refresh
Uptime 0 days, 0:22
Load Avg0.19 0.06 0.01
Kernel 2.6.16.21
CAPTIVE PORTAL
Gateway
Authentication
Language
Accounting
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
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
00:26:54:0B: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
Domain Name System
Any
53/udp
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
Internet

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 **ACTIVATE**:

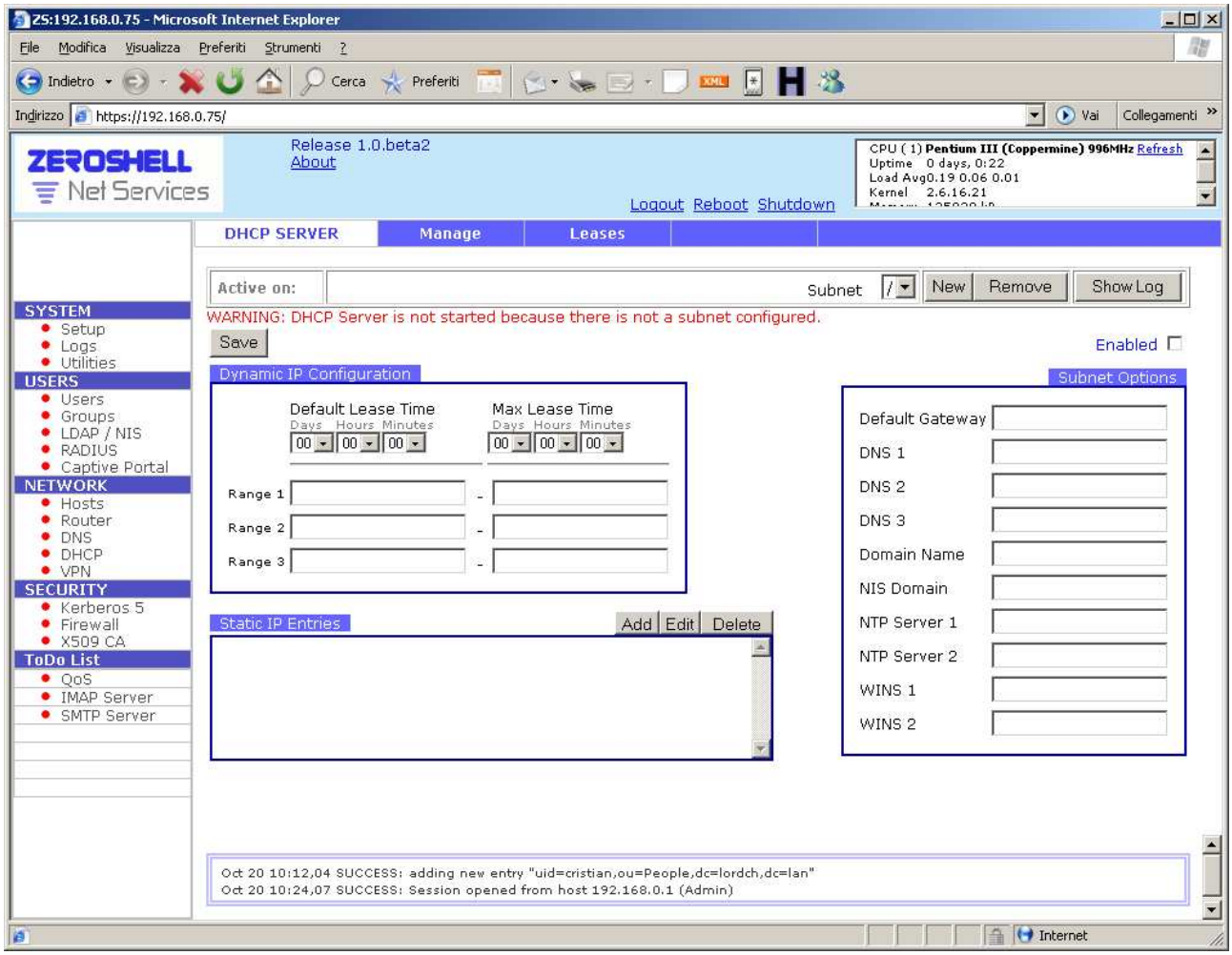


ed il gioco è fatto…possiamo ora configurare i nostri client come segue (dove 192.168.0.75 è il nostro Zeroshell..):

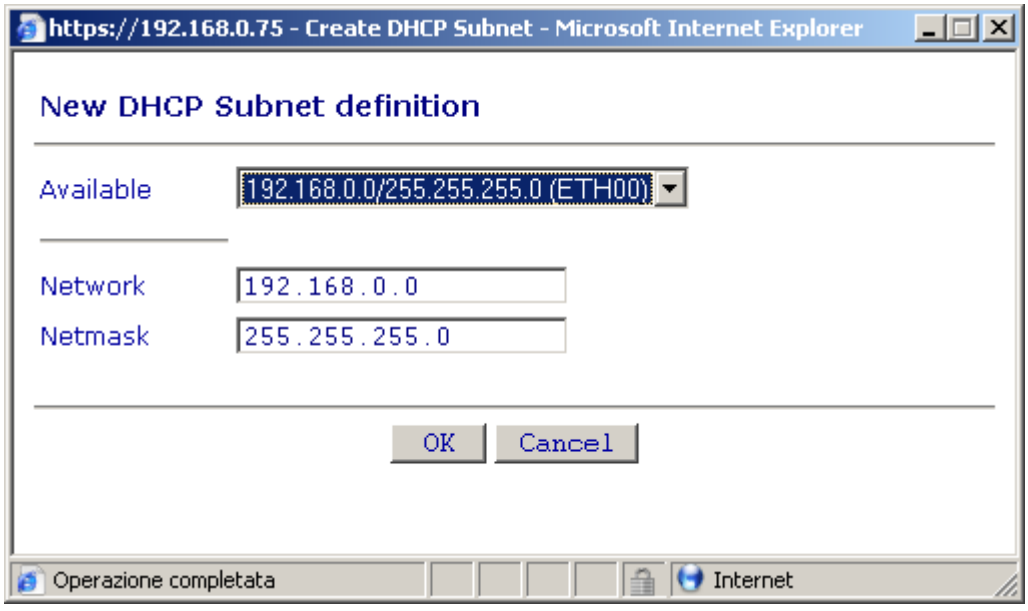


Attivare il servizio DHCP:

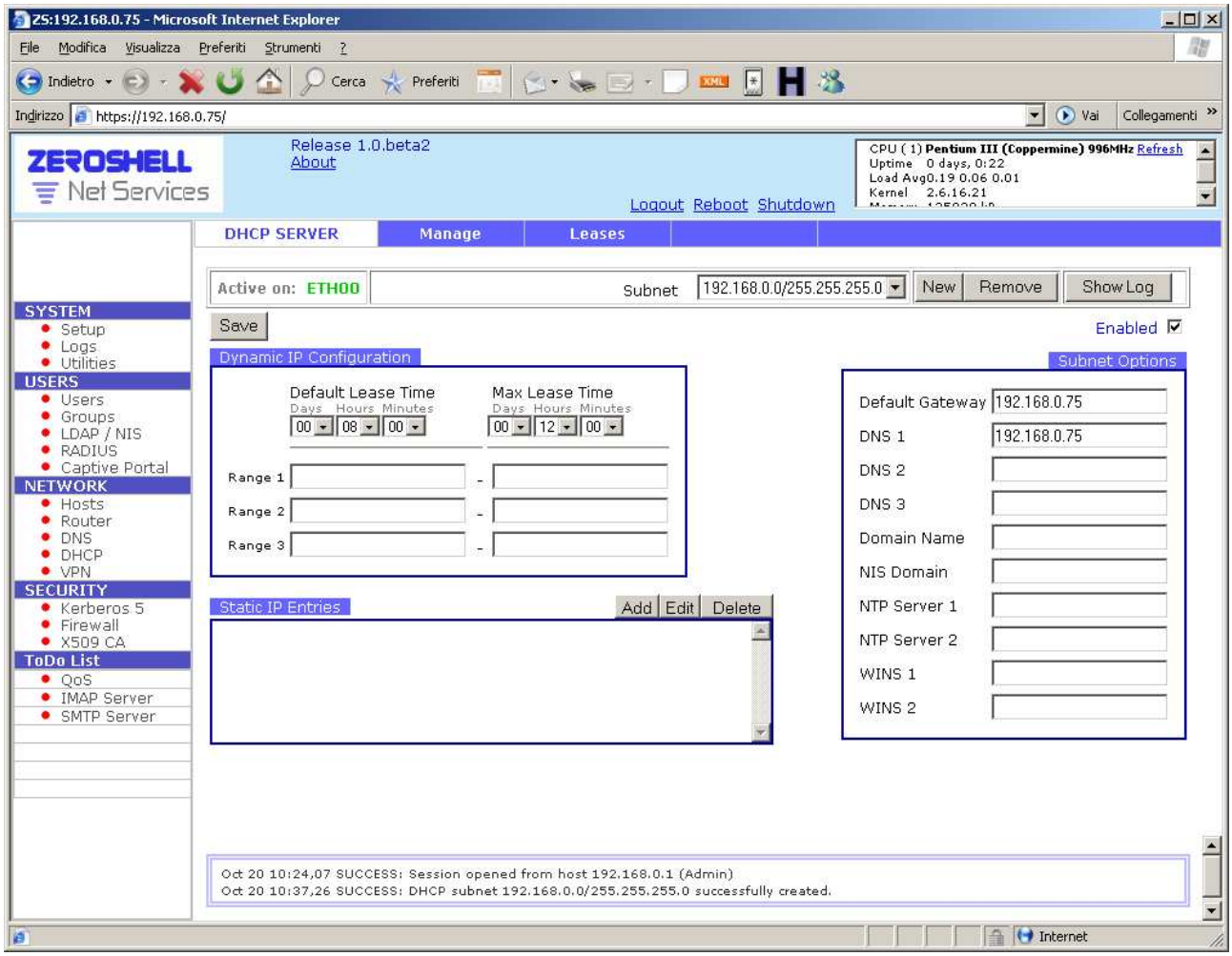
Perché avere ip statici sulla rete quando esiste la possibilità di avere uno strumento come Zeroshell? Basta continuare a cambiare ip, a controllare gateway e dns! Menu **DHCP**:



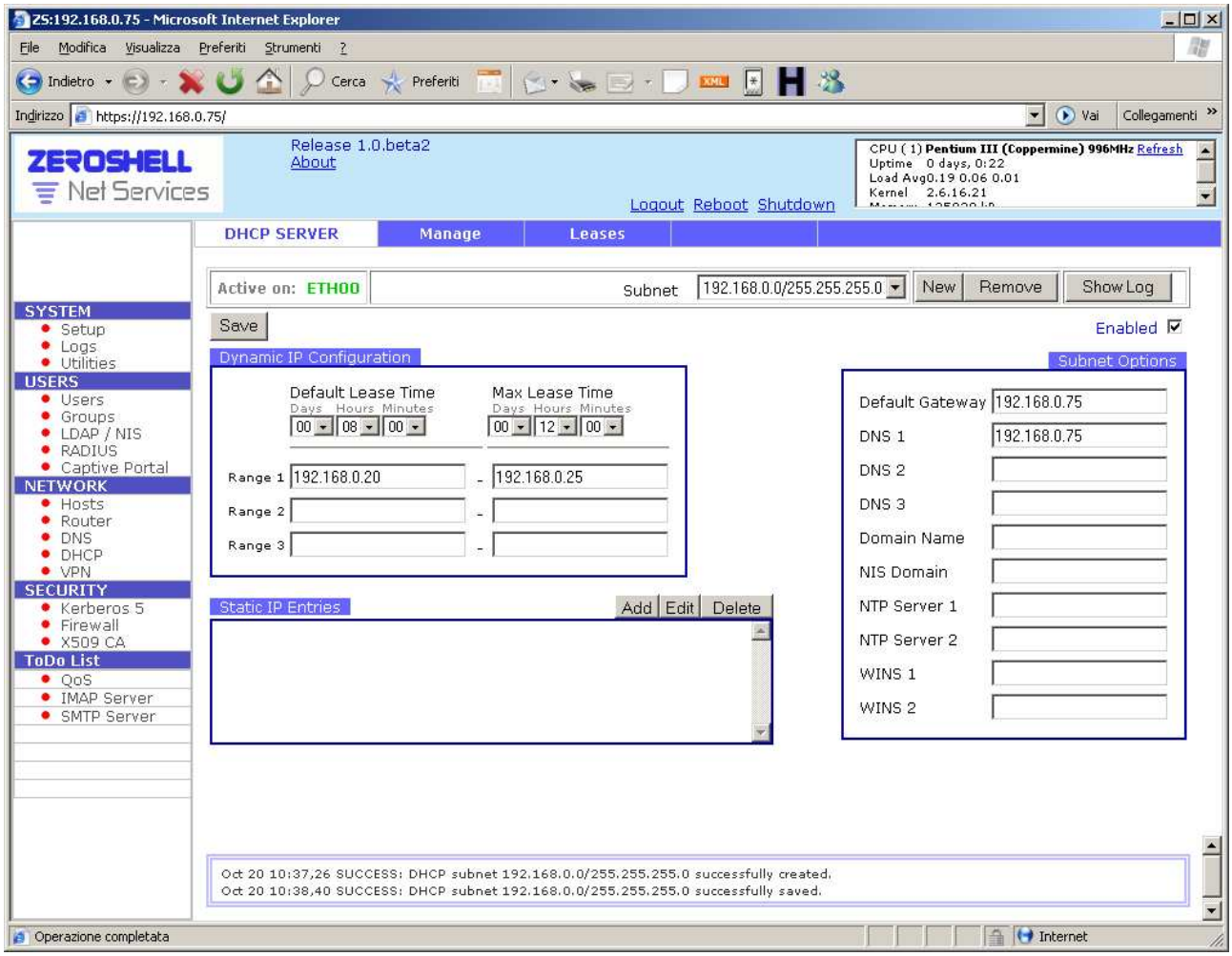
selezionare il bottone **NEW** e scegliere la rete sulla quale si vuole distribuire l'indirizzamento in modo automatico:



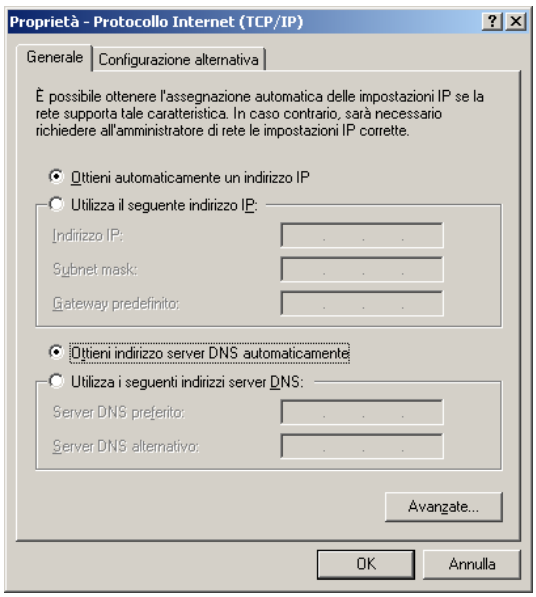
ecco:



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

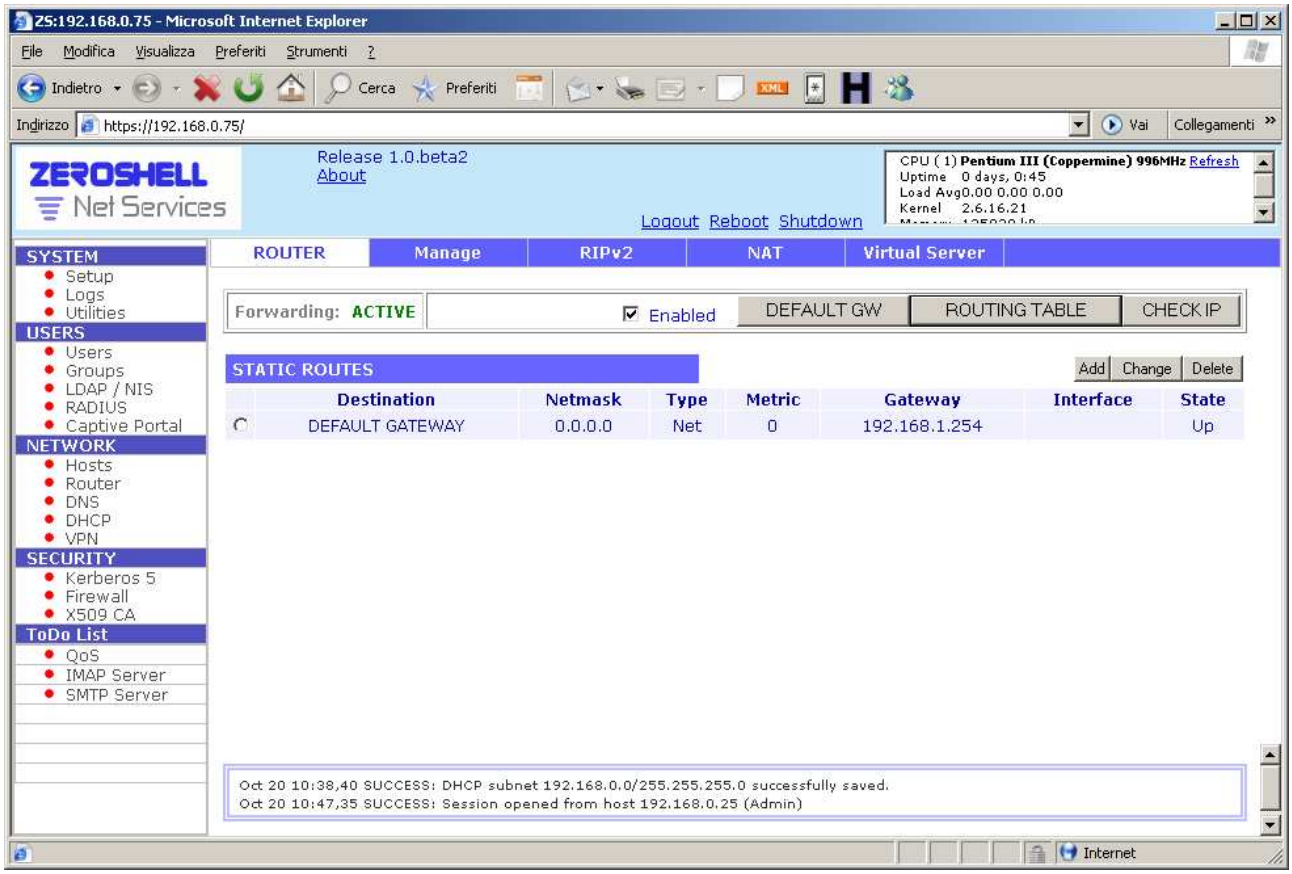
Scheda Ethernet Connessione alla rete locale (LAN):

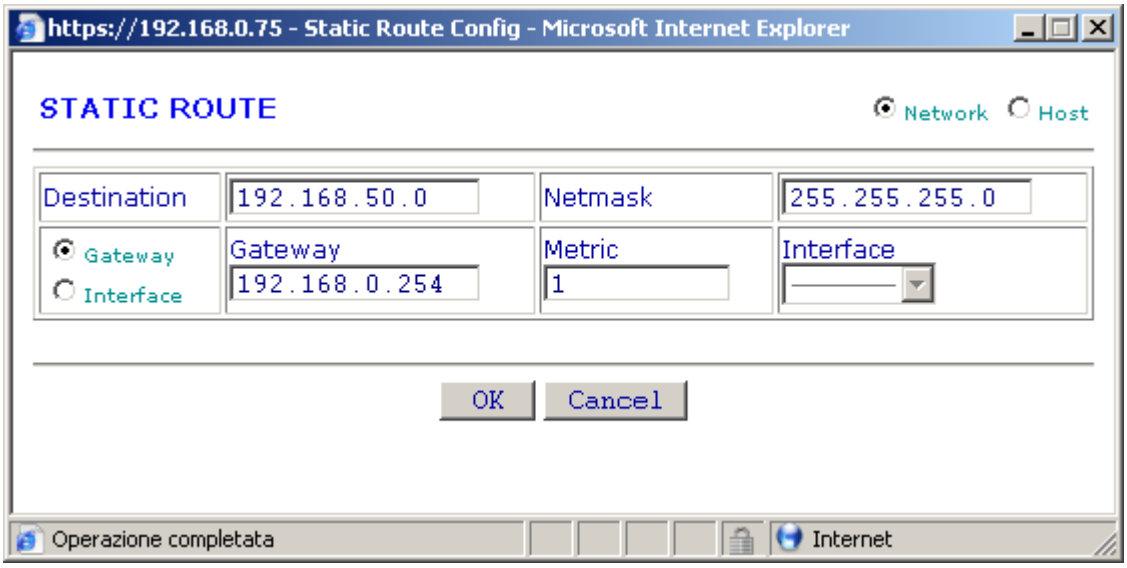
Suffisso DNS specifico per connessione:
Descrizione . . . . . : 3Com 3C920B-EMB Integrated Fast Ethernet Controller
Indirizzo fisico. . . . . : 00-26-54-0B-31-CA
DHCP abilitato. . . . . : Sì
Configurazione automatica abilitata : Sì
Indirizzo IP. . . . . : 192.168.0.25
Subnet mask . . . . . : 255.255.255.0
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

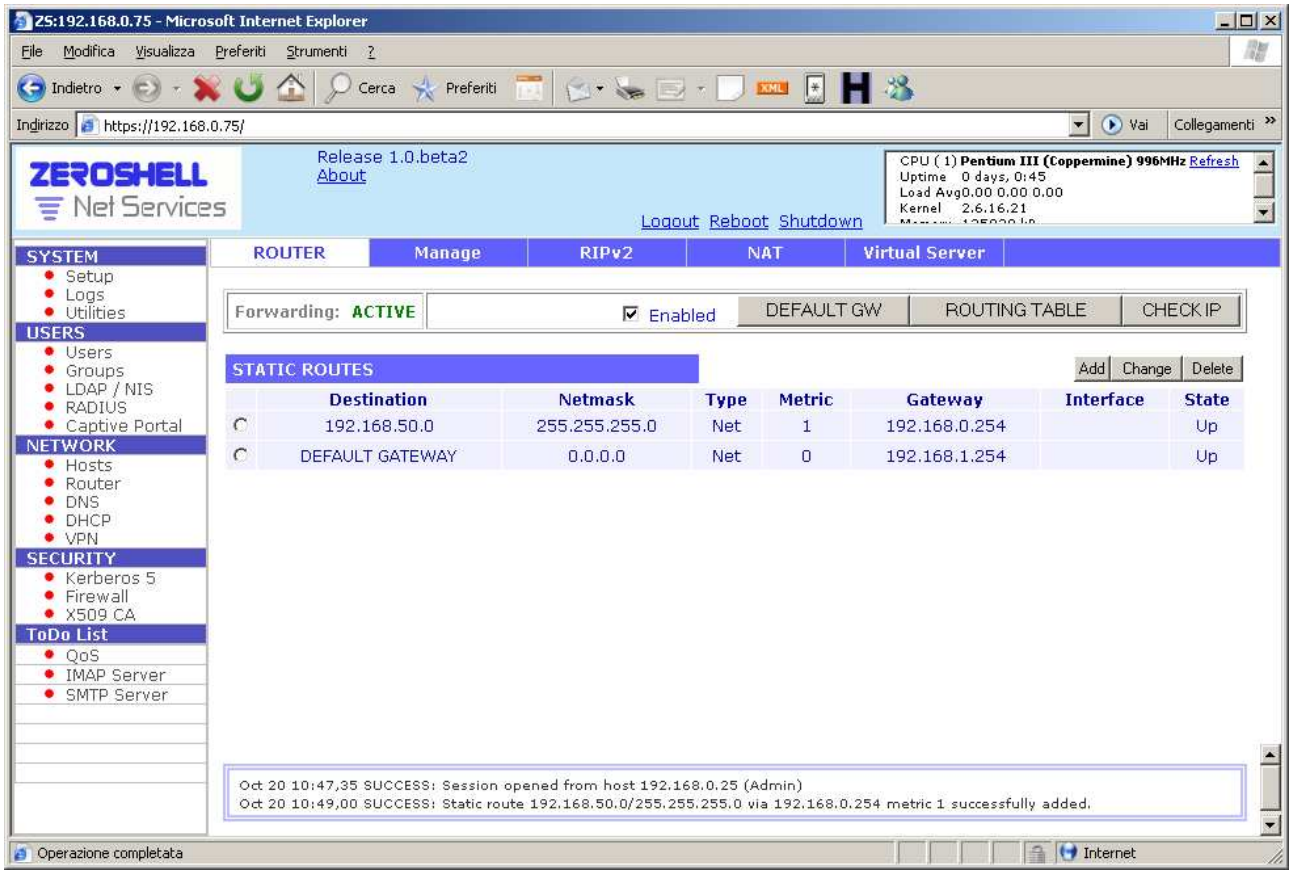
Routes statiche verso reti remote:

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:





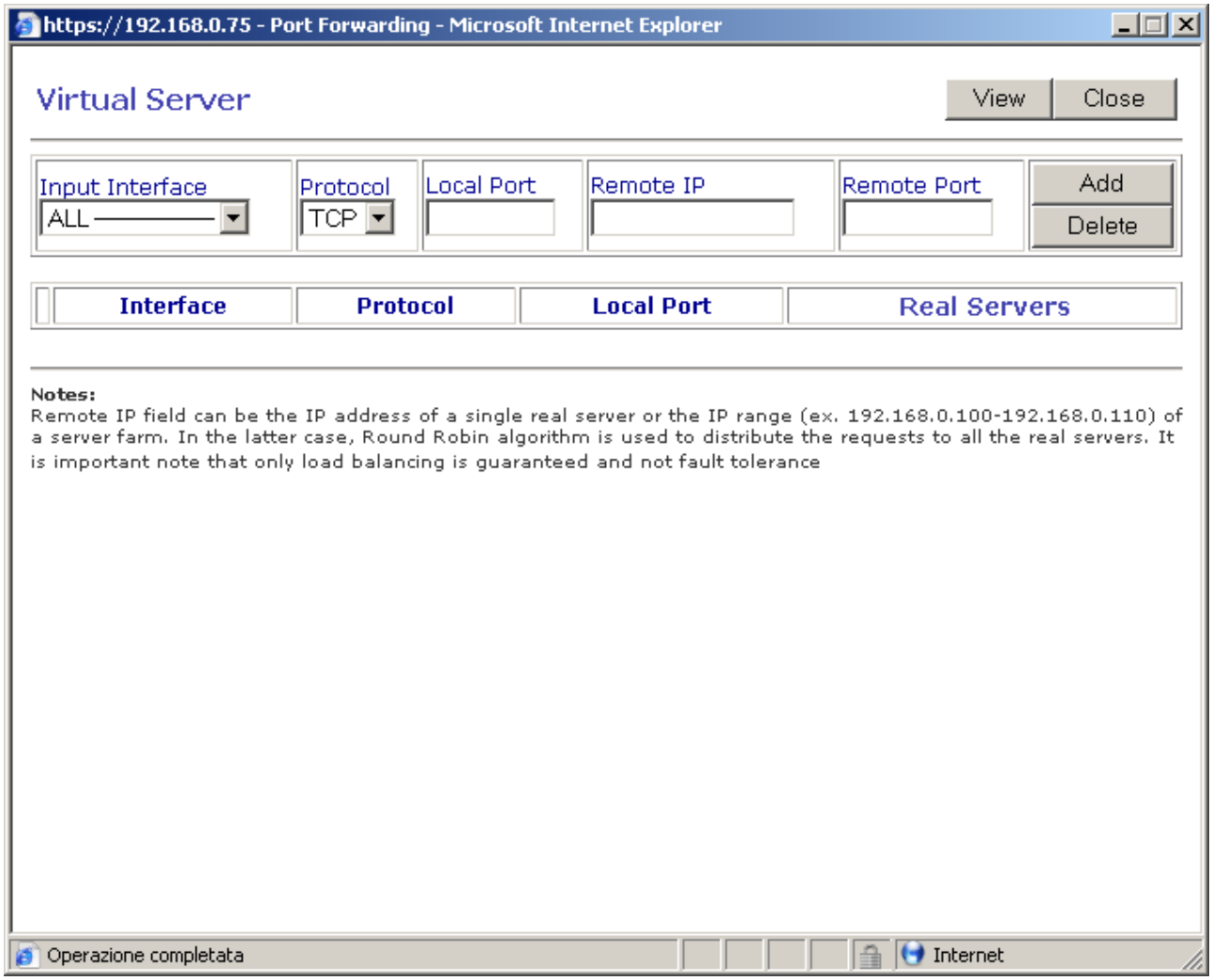
La voce metric indica come sempre il “costo” (la precedenza nel reindirizzamento) per raggiungere la rete remota. E’ possibile specificare la stessa rete remota quindi attraverso 2 router diversi che usano linee a diverso costo (o diversa velocità).



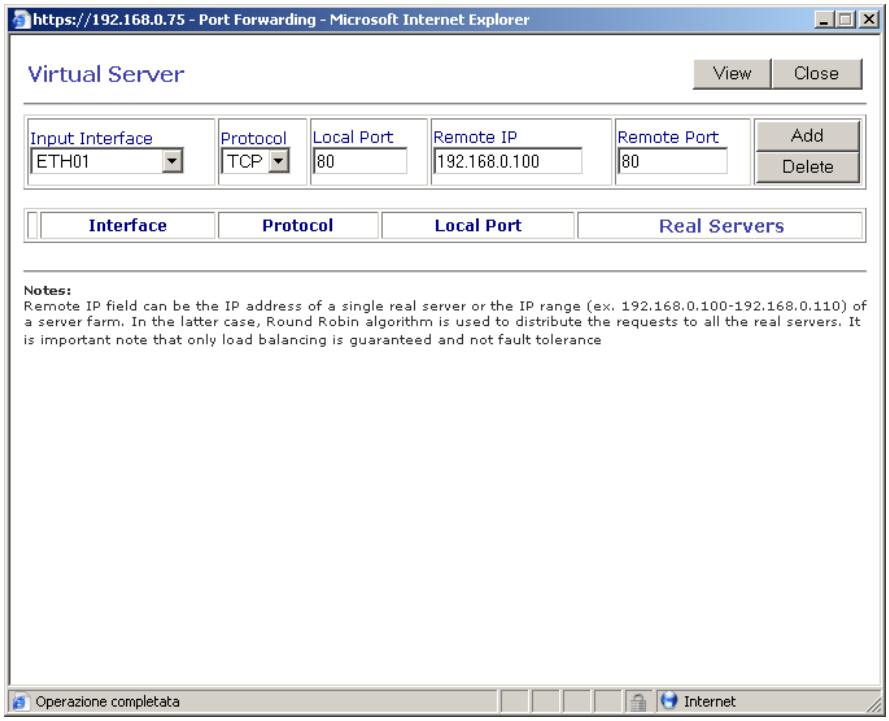
Zeroshell consente di attivare sulle proprie schede anche il protocollo RIP v2. Questo protocollo se attivato su tutti I router interni consente lo scambio di informazioni fra gli stessi in modo dinamico. Sostanzialmente i vari routers con ripv2 attivato si comunicheranno in modo periodico le reti che 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.

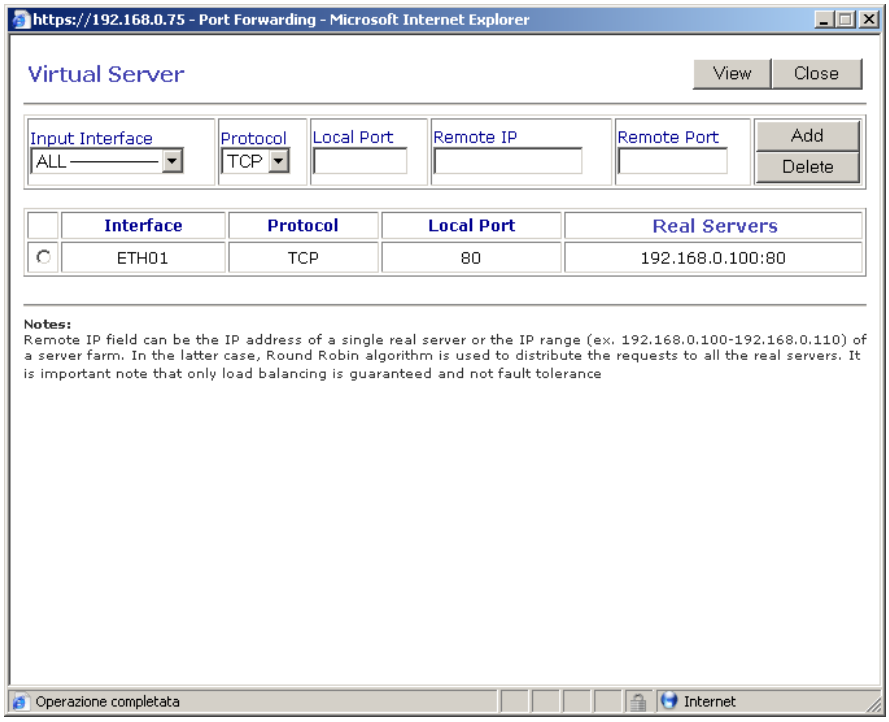
Servizi attraverso Virtual Server:

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** :

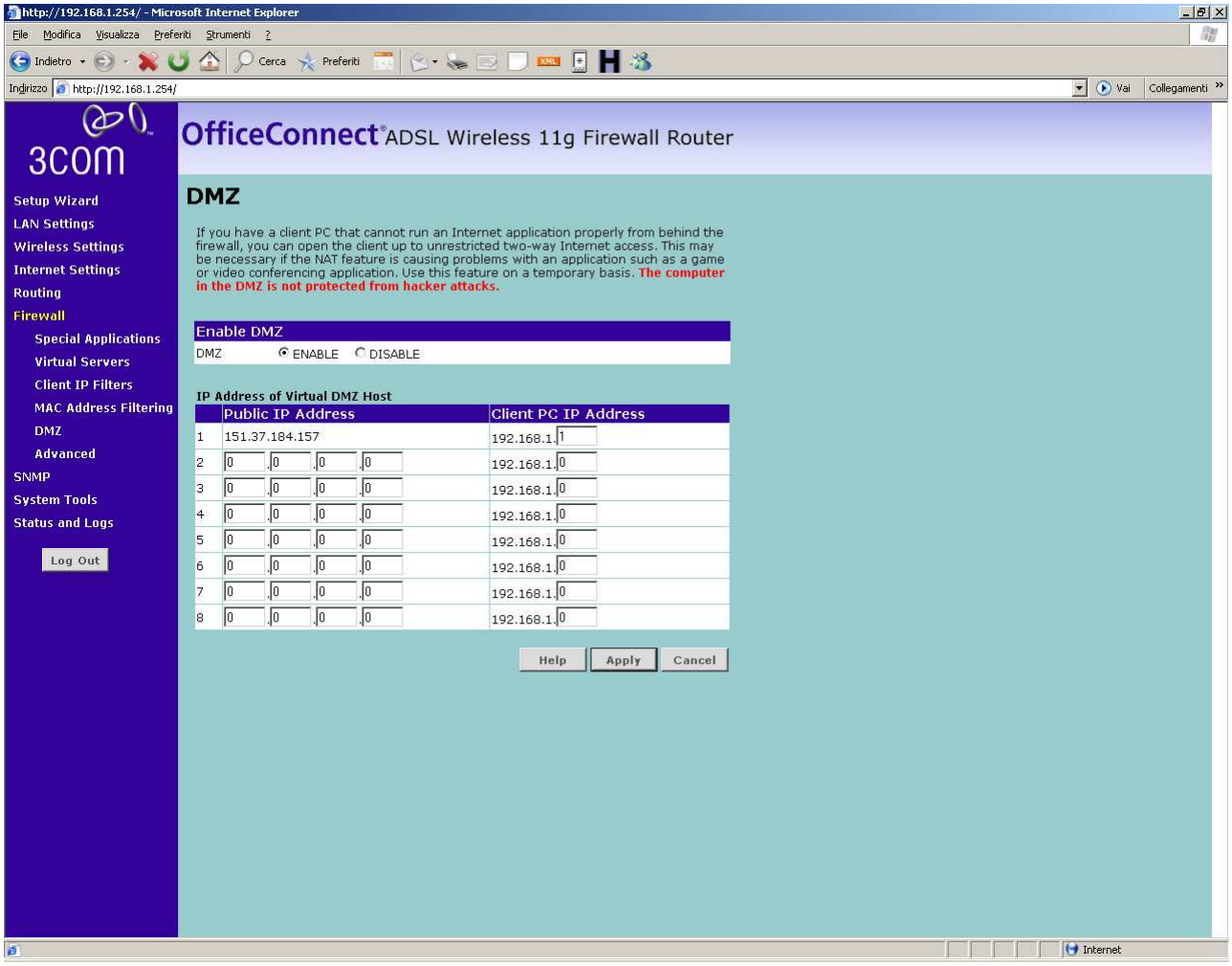


Si può definire quale interfaccia deve accettare la richiesta, su quale protocollo, su quale porta del protocollo. Poi quale sia il server interno e su quale porta questo ascolti. Per esempio, se ho un server web interno (192.168.0.100) che pubblica il sito web sulla porta 80 del protocollo TCP e decido 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:





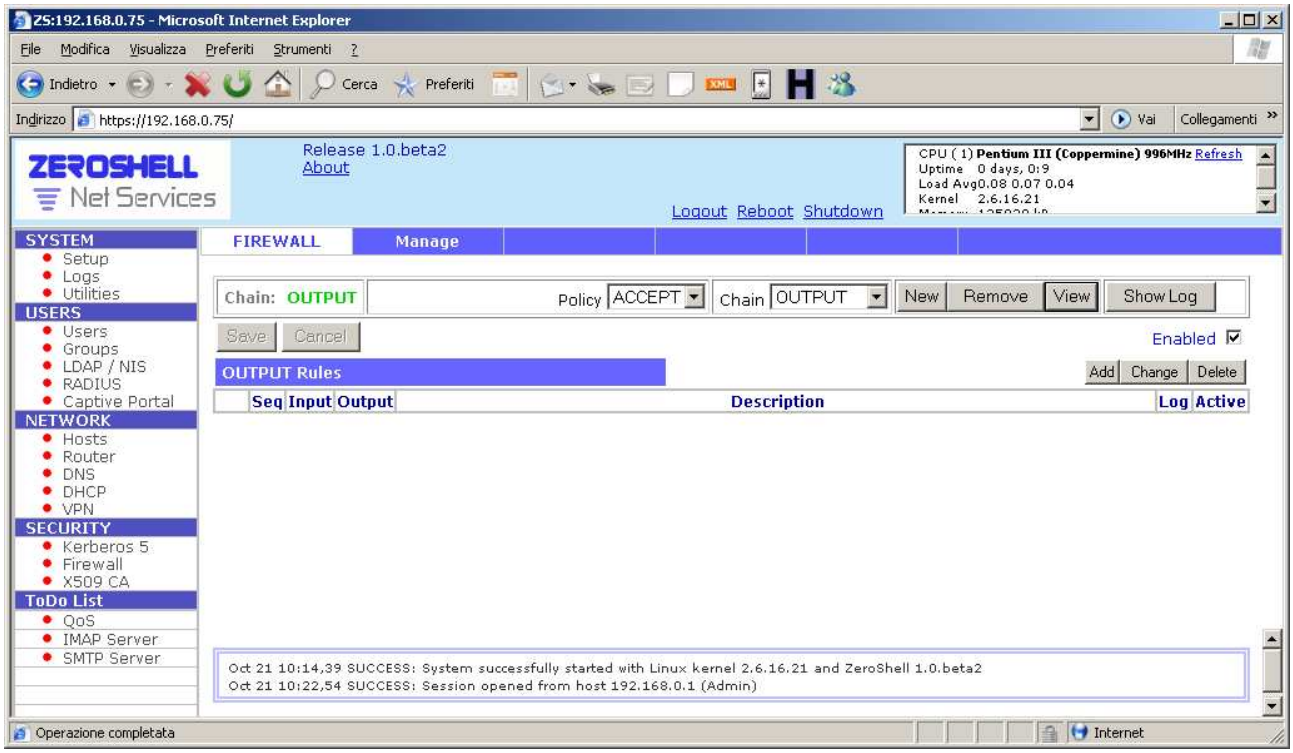
Ovviamente il router della linea adsl dovrà essere configurato per fare entrare ogni sorta di richiesta (o almeno porta 80 tcp) sull'interfaccia di Zeroshell. Con un router 3com :



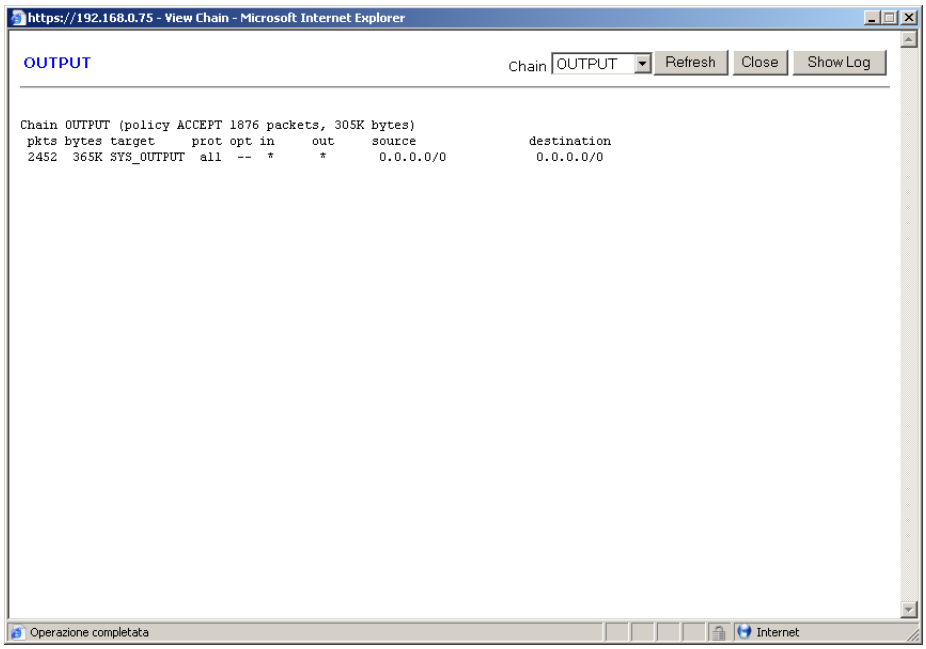
Dove 192.168.1.1 è la ETH01 esterna di Zeroshell.

Sicurezza: verificare le regole del firewall

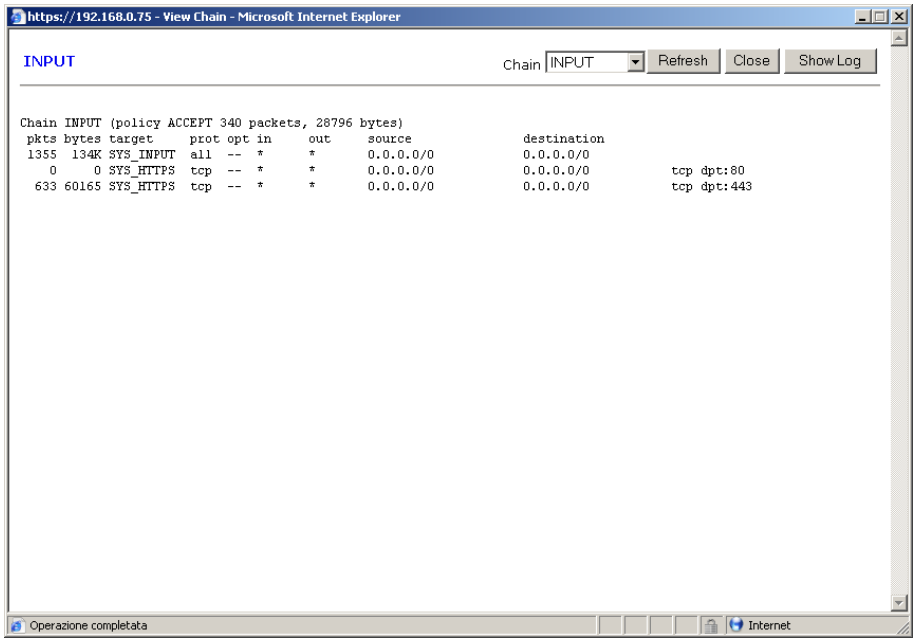
Tramite il menu **FIREWALL** è possibile verificare le regole impostate di default sul firewall.
Scegliendo la **CHAIN OUTPUT** e cliccando su **VIEW**:



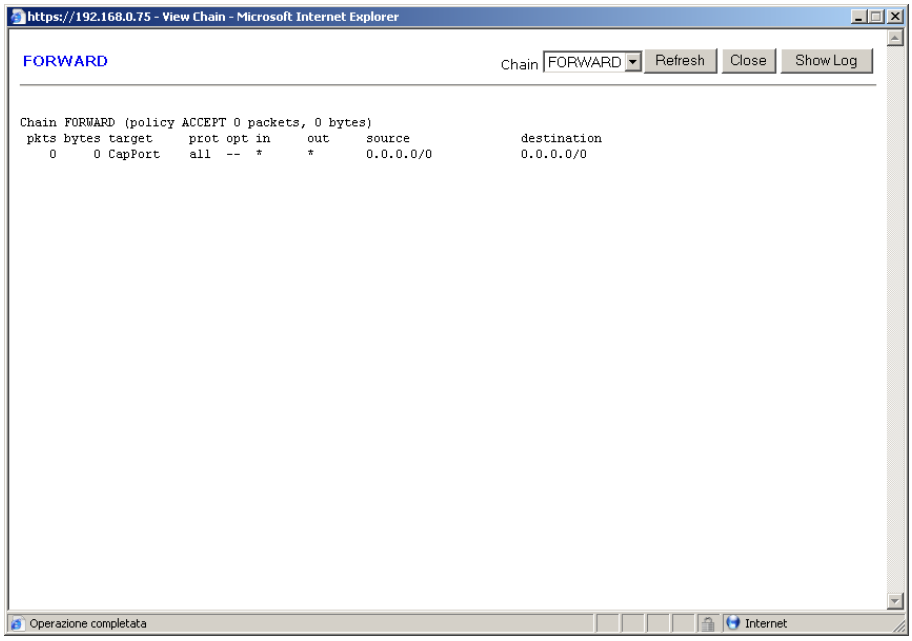
Ecco le regole attive di default in uscita:



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.