

Zeroshell HOWTO



The multifunctional OS created by
Fulvio.Ricciardi@zeroshell.net

www.zeroshell.net

How to secure my private network

(Author: cristiancolombini@libero.it)

How to secure my private Network:

This short guide will let us configure a network firewall for our network in less than one hour. Zeroshell will secure our private network from external attacks. Our private network is connected to internet through a xDSL router.
Here the steps to follow :

First start and login

Preparing a partition disk where to store our configurations

Storing our configuration

Network adapters configuration

Internet surfing

Captive Portal activation

DNS Service

DHCP Service

Static routes to remote networks

Virtual Servers

Security: check default policies

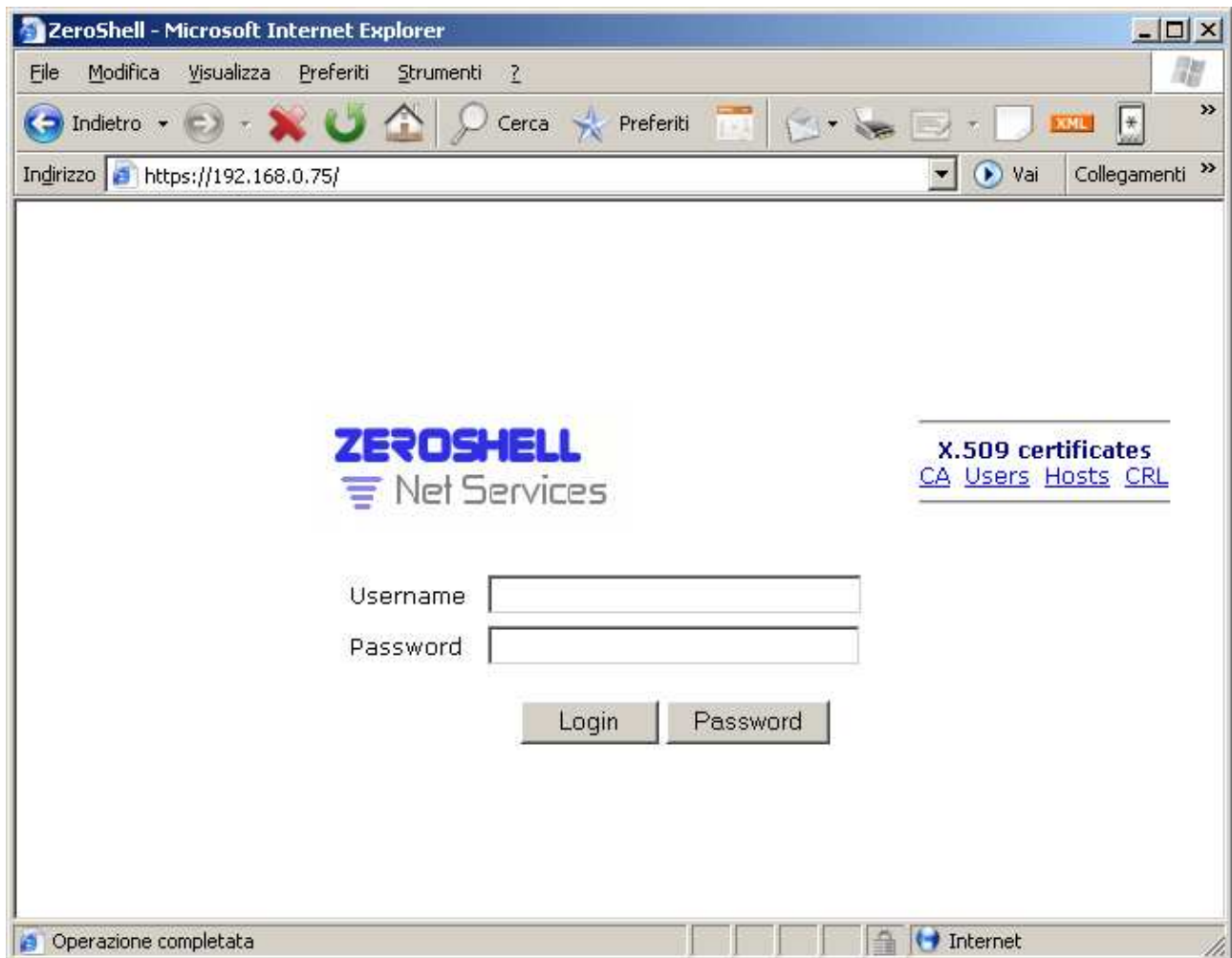
In Zeroshell we can find many other important features for more complex networks; this is a great scalable solution for our network.

First start and login:

After booting from CD, the system is reachable with a browser at the http secure:

<https://192.168.0.75>

Accepting the secure connection we are asked user and password to login:



Use these:

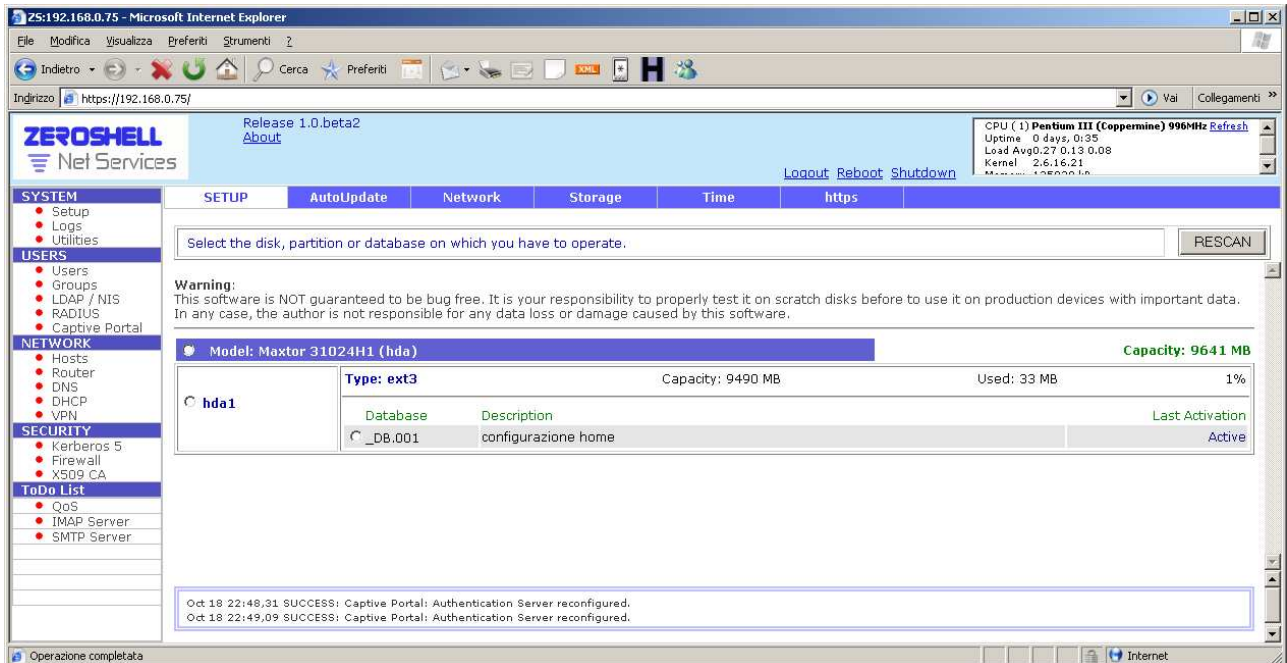
User: admin
Password: zershell

Now we can use web interface to setup our firewall.

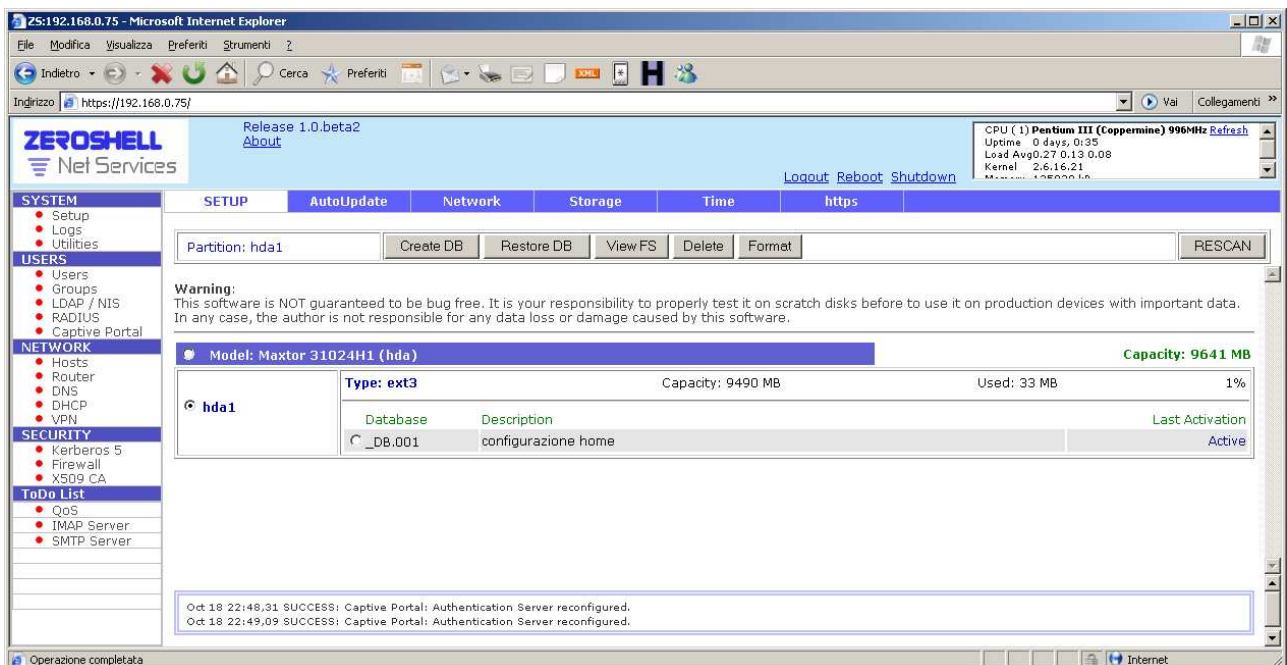
Preparing a partition disk where to store our configurations:

It's so important to save our changes that Zeroshell lets us save them in a configuration file. It can be stored in a partition on a hard disk. It's not necessary to format any existing partitions, we can save our configuration files in existing partition such as: ext3, reiserfs, ext2 o fat32. For my own preference I prefer to create a new partition ext3. So I choose to delete any existing partition on my disk (all data on this disk will be lost).

Using **SETUP** menu (in left frame) choose tag **STORAGE** (in upper frame):



We are shown existing disks. We select existing partitions and **DELETE** them:



We are asked confirmation for deletion. YES

Now we have a blank disk without partitions. I am ready to create just one partition.

Storing our configuration:

Once the disk is ready to be used, we can create our first configuration file. Chosing the right partition click on CREATE DB:

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

Insert a short description for the configuration file; fully qualified name of our system; Kerberos Realm and LDAP; choose a new password for user “admin”; Ip address for the interface used to configure the system; default gateway to access external networks (to access internet).

This configuration will be used everytime the system will start. We can choose to create several different configuration files to be activated (**ACTIVATE**) for default startup of the system. Using **BACKUP** button we can create a copy of the selected configuration file on the pc we are using to browse Zeroshell administrative homepage .

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 125000 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)** [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**

| Type: ext3 | Capacity: 9490 MB | Used: 33 MB | 1% |
|-----------------|---------------------|------------------------|----|
| hda1 | | | |
| 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

Network adapters configuration:

Once prepared disk and created the first configuration file we can configure the ip address of the network adapters, by clicking **SETUP** nad **NETWORK** tag:

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-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

Usually ETH00 is the internal network adapter (secure interface of the firewall) and ETH01 is the external that communicate with xDSL router. Using **Add IP** buttons we can set static ip addresses for these interfaces. I have choosen 192.168.0.75 for internal interface (ETH00) and 192.168.1.1 for the external one (ETH01); now I set default gateway using button **DEFAULT GW**. My gateway is 192.168.1.254; I can now verify the statics routes in **ROUTER** menu:

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 RIPv2 NAT Virtual Server

Forwarding: ACTIVE Enabled DEFAULT GW ROUTING TABLE CHECK IP

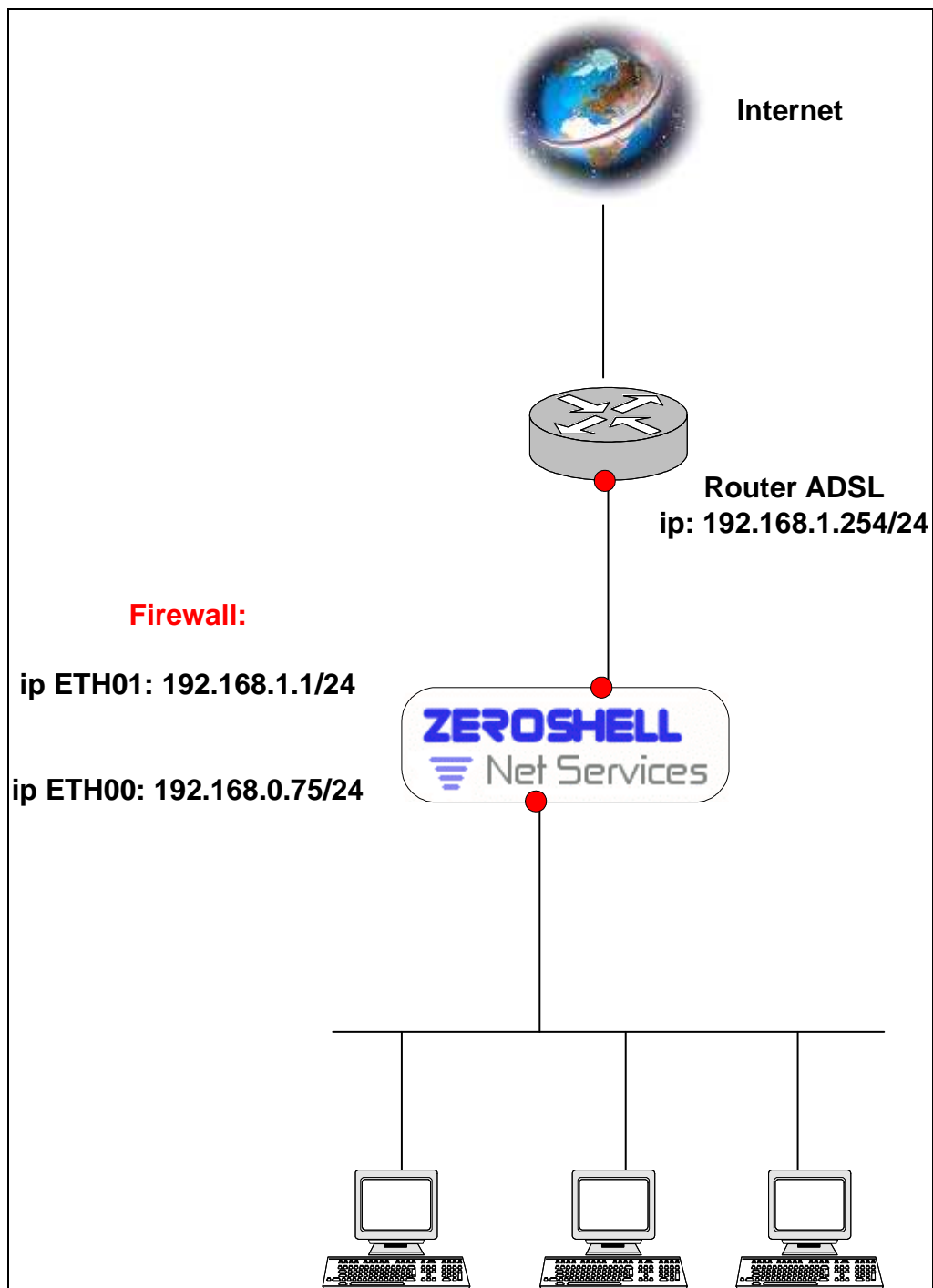
STATIC ROUTES
Add Change Delete

| | Destination | Netmask | Type | Metric | Gateway | Interface | State |
|---|-----------------|---------|------|--------|---------------|-----------|-------|
| • | 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

So this is my network:

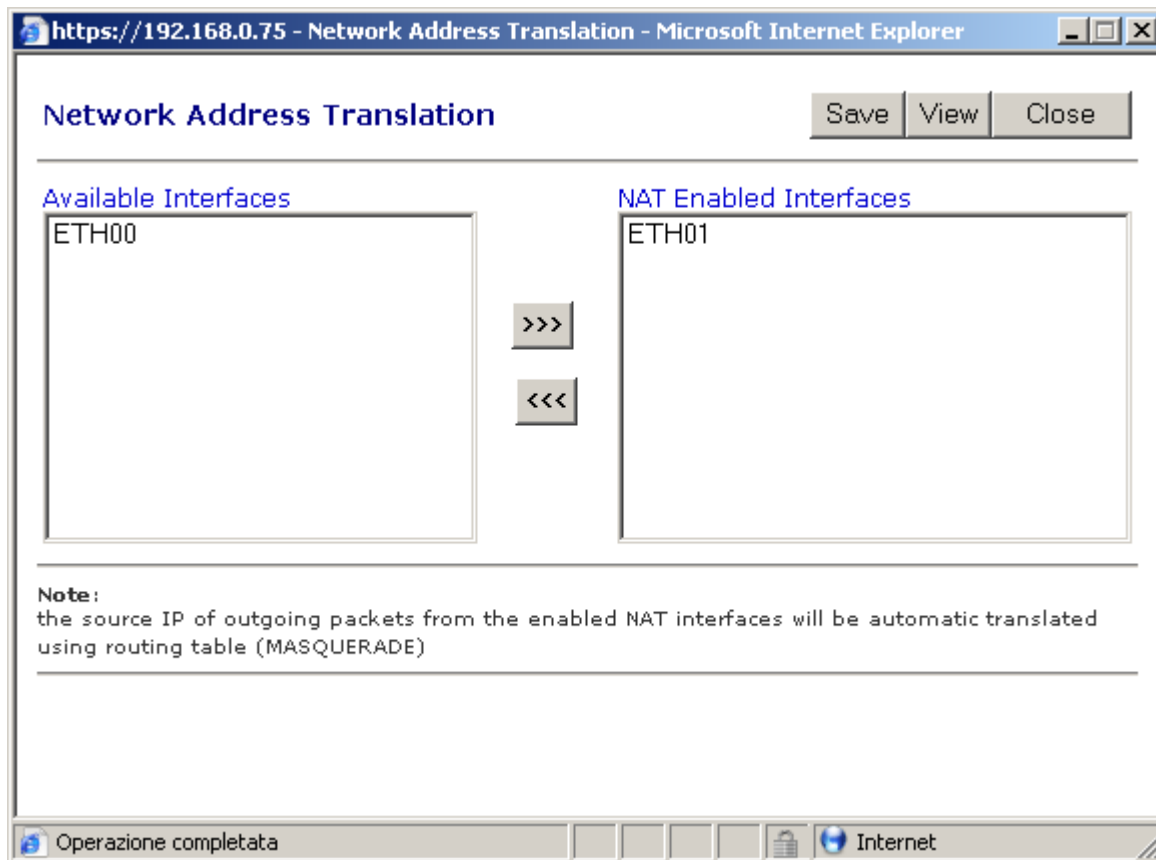


It's is to understand that this network thopology is very scalable by Zeroshell; we can now begin to create policies for our internal network (192.168.0.0/24); or we can user Captive Portal to create user and password for internal users that want to use internet browser; we can create virtual server to share our services with external networks, etc.

Internet surfing:

To let internal clients use internet connection, we must activate Network Address Translation (NAT) to protect them.

Using **ROUTER** menu, click on **NAT** tag and set that ETH00 is translated by ETH01:



Now we can use internet connection on our clients.

Captive Portal activation:

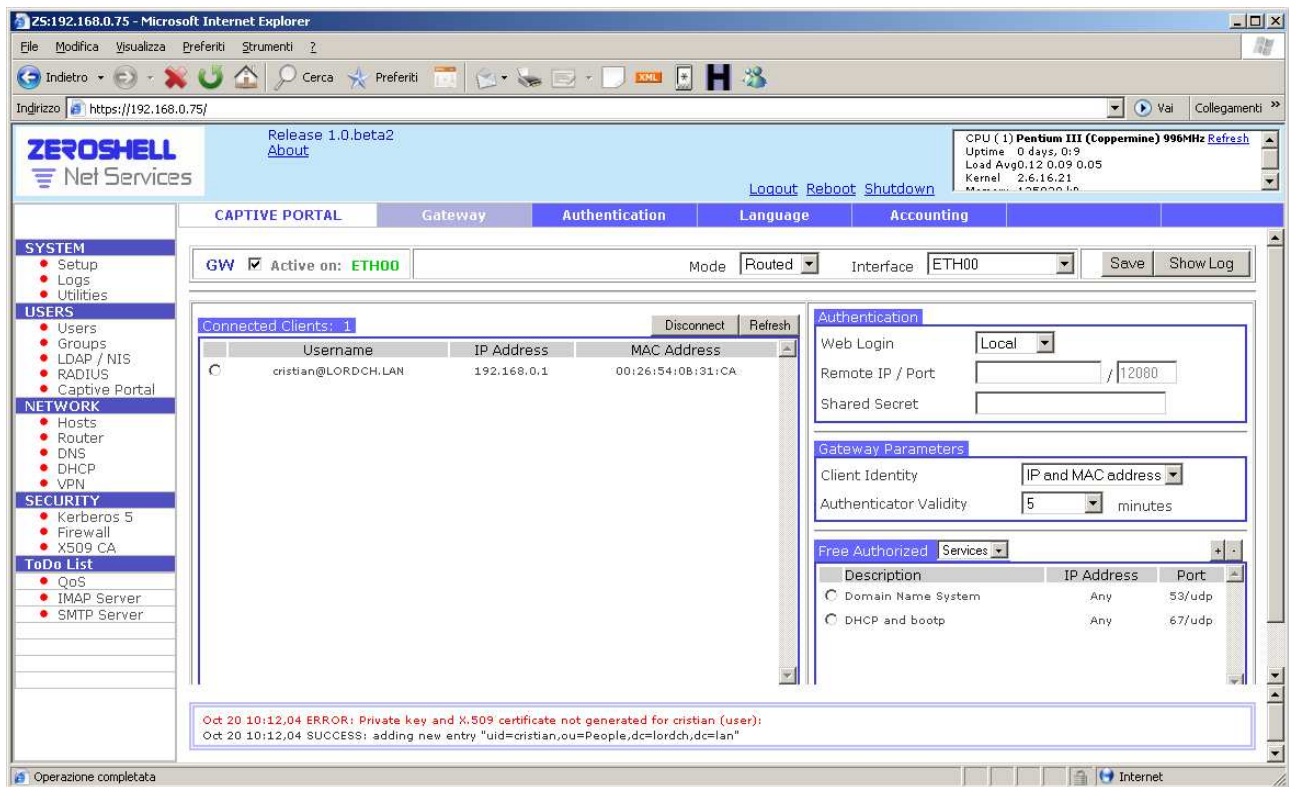
These useful features let us set internet users and password to filter connection to external (internet). In this way a user on internal network must authenticate against Zeroshell before opening connections to internet (for web browsing, mail download, etc...)

Before activating Captive Portal we must create users in **USERS**, **ADD** tag; fill the fields as below:

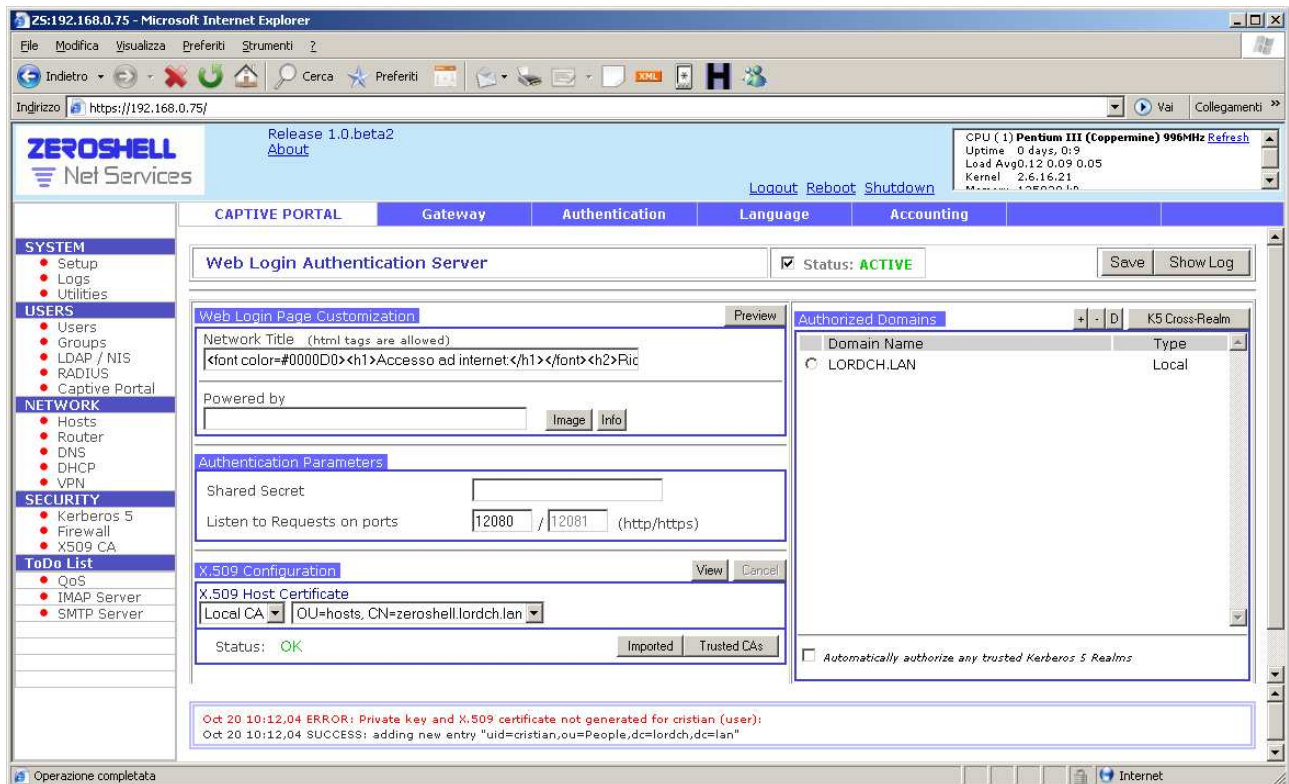
The screenshot shows the Zeroshell Net Services web interface in a Microsoft Internet Explorer browser window. The address bar shows the URL <https://192.168.0.75/>. The interface has a sidebar menu on the left with categories: SYSTEM (Setup, Logs, Utilities), USERS (Users, Groups, LDAP / NIS, RADIUS, Captive Portal), NETWORK (Hosts, Router, DNS, DHCP, VPN), and SECURITY (Kerberos 5, Firewall, X509 CA). The main content area is titled 'USERS' and shows a list of users. The user 'cristian colombini (cristian)' is selected. The 'Account' section shows fields for Username (cristian), UID (1), Primary Group (nobody), and GID (85534). The 'Home Directory' is /home/cristian and the 'Default Shell' is sh. The 'User Information' section includes fields for Firstname (cristian), Lastname, Organization, Description (cristian), E-Mail, and Phone. The 'User Password' section has fields for Password and Confirm. The 'Enabled Services' section has checkboxes for Kerberos 5 Authentication, Host-to-Lan VPN (L2TP/IPsec), and 802.1X Access (VLAN). At the bottom, a log shows an error message: 'Oct 20 10:12:04 ERROR: Private key and X.509 certificate not generated for cristian (user);' and a success message: 'Oct 20 10:12:04 SUCCESS: adding new entry "uid=cristian,ou=People,dc=lordch,dc=lan"'. The status bar at the bottom indicates 'Operazione completata'.

USERNAME contains the name of the user for authentication.

Once created our users, click **CAPTIVE PORTAL** menu; set a flag on **GW**, choose **ROUTED MODE** and internal ethernet adapter on which authentication process will happen (in our client the ETH00's ip is the default gateway).



Activate **AUTHENTICATION** :



Now we can close our web browser and reopen it; it will ask us to authenticate. Here below I have customized my authentication page:



Using correst user and password:



we can see this popup: we can use internet resources until this page is open.

You can customize this page using **AUTHENTICATION** tag with an HTML script:

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

In **GATEWAY** tag you can see connected users and you can drop 'hem if necessary using **DISCONNECT** button:

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 |
|---|---------------------|-------------|-------------------|
| C | 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 |

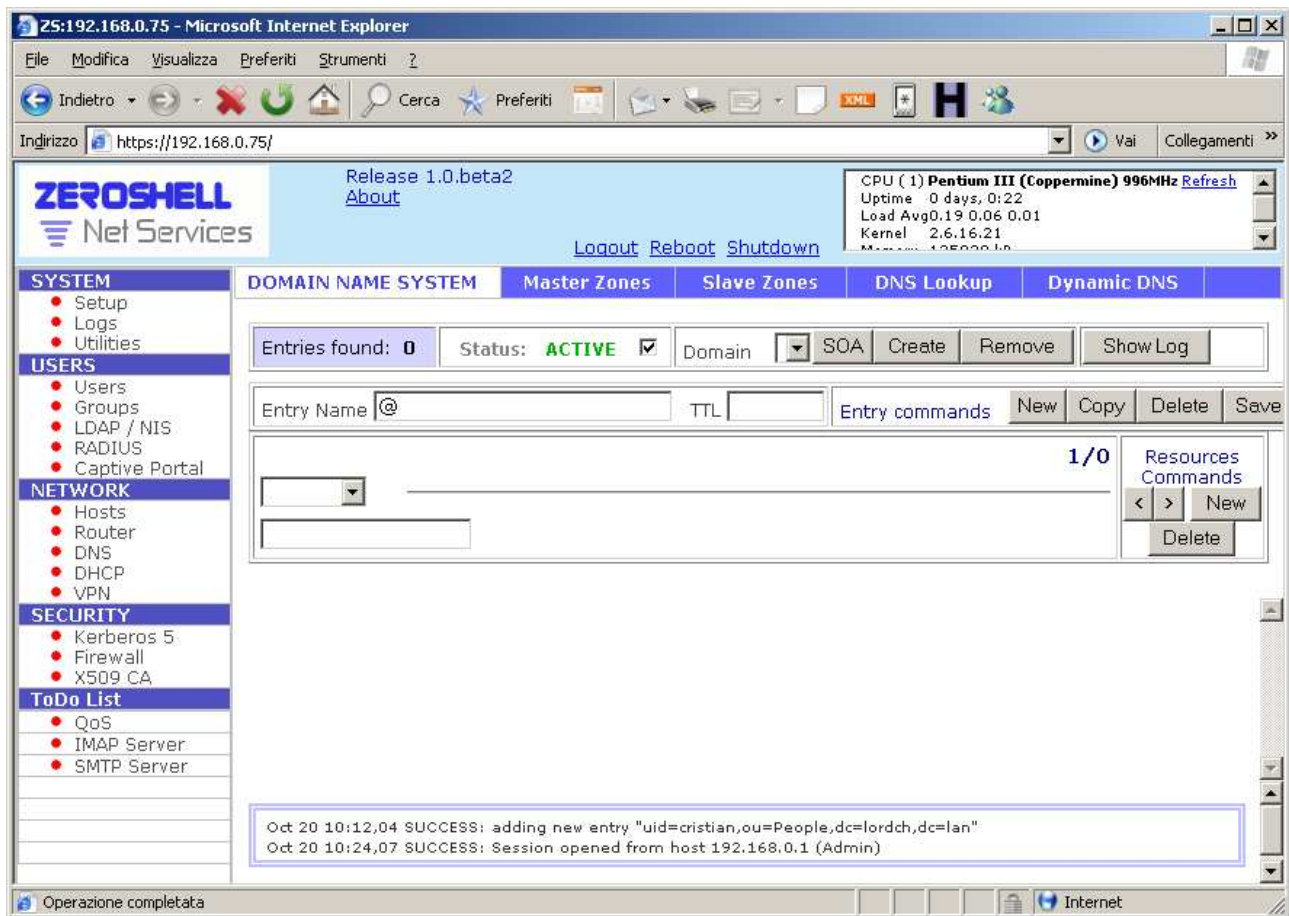
Oct 20 10:12:04 SUCCESS: adding new entry "uid=cristian,ou=People,dc=lordch,dc=lan"
Oct 20 10:24:07 SUCCESS: Session opened from host 192.168.0.1 (Admin)

Operazione completata

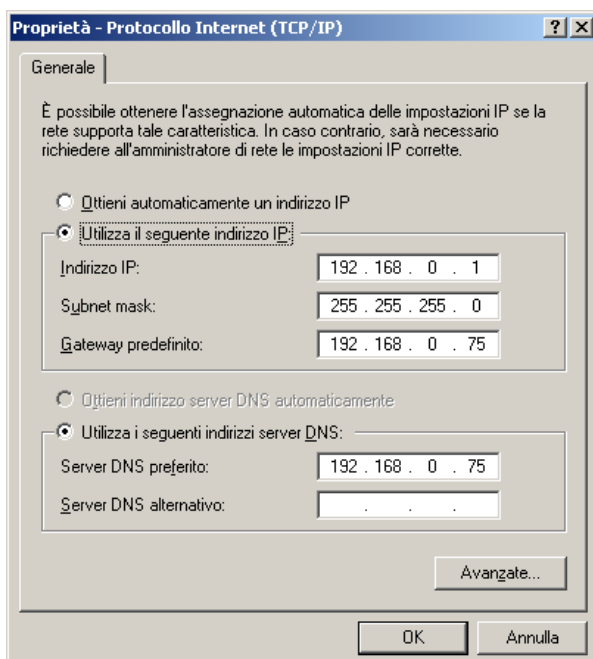
Internet

DNS Service:

Home xDSL lines use external DNS servers to resolve internet names. Sometimes these external DNS servers are down or not working for any reasons; Zeroshell can be also a DNS server! It's very easy to be used: click on left **DNS** voice..and flag **ACTIVATE**:

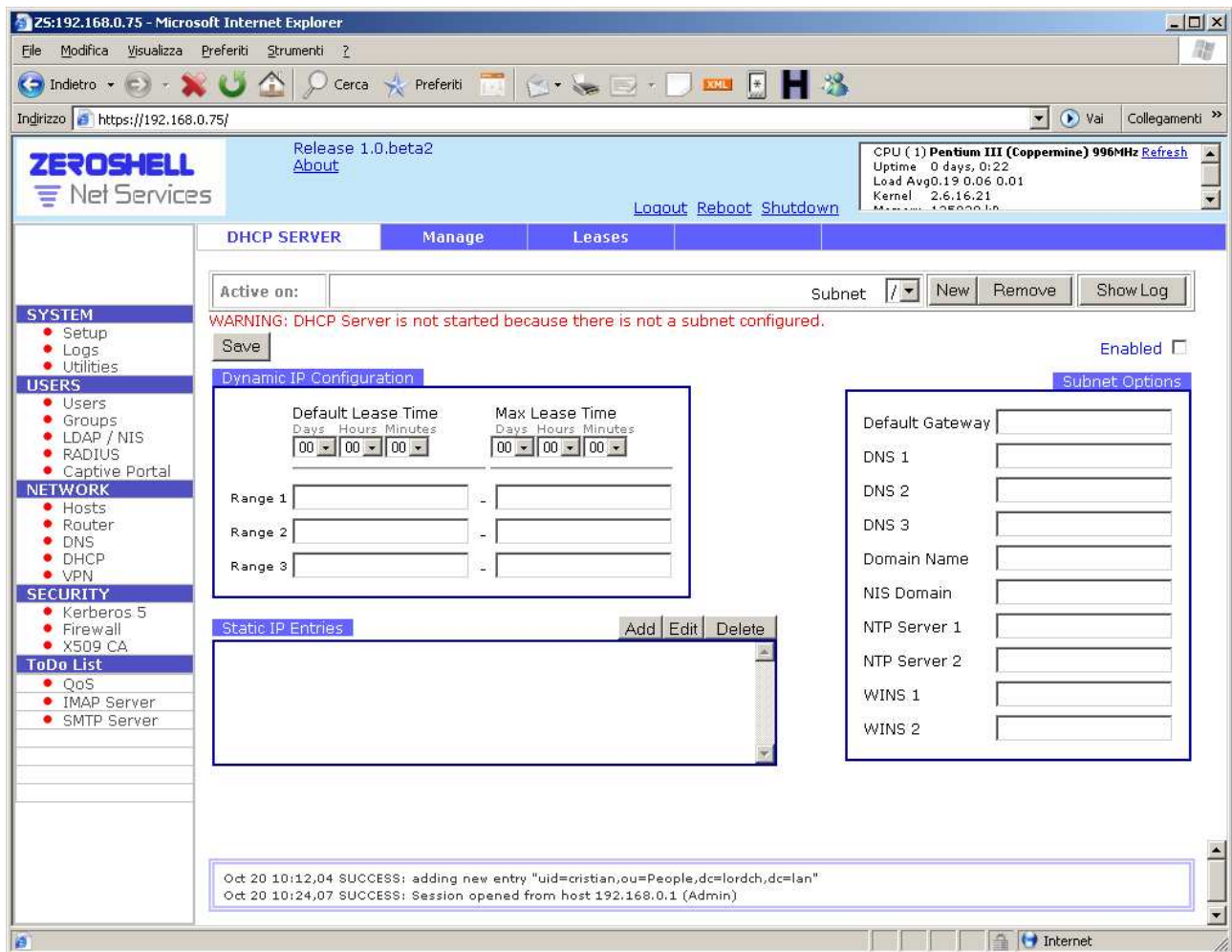


Done!...Now you can set your client in this way (192.168.0.75 is Zeroshell..):

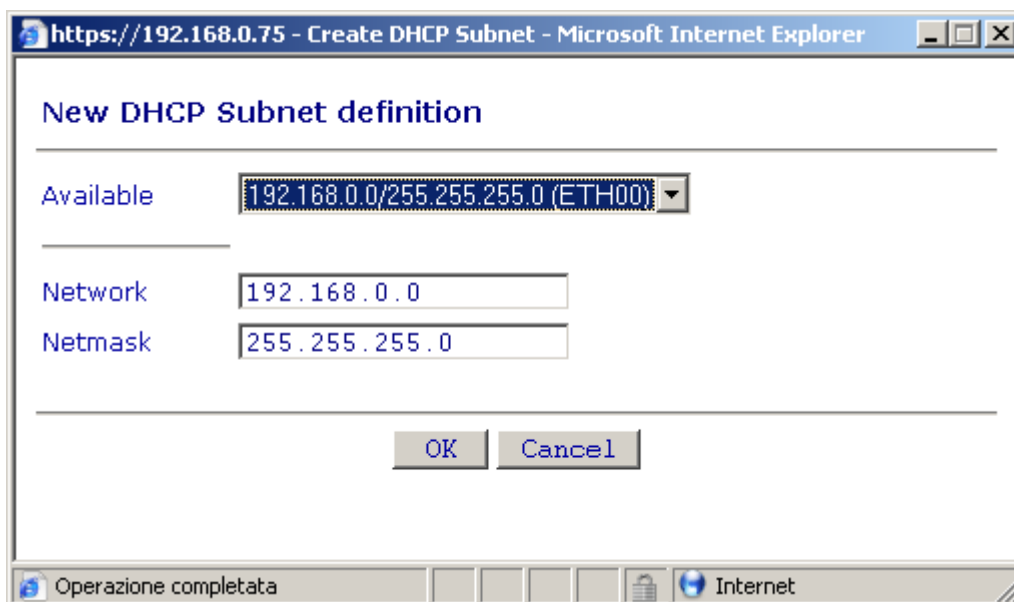


DHCP Service:

Zeroshell can be also a DHCP server; in this way the clients of our internal network don't need static ip addressing.
Choose **DHCP**:



create **NEW** and choose the network interface where Zeroshell will distribute ip addresses:



and so:

25:192.168.0.75 - Microsoft Internet Explorer

File Modifica Visualizza Preferiti Strumenti ?

Indietro Cerca Preferiti XML H

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 128000.0k

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 Days Hours Minutes
00 08 00

Max Lease Time Days Hours Minutes
00 12 00

Range 1 -
Range 2 -
Range 3 -

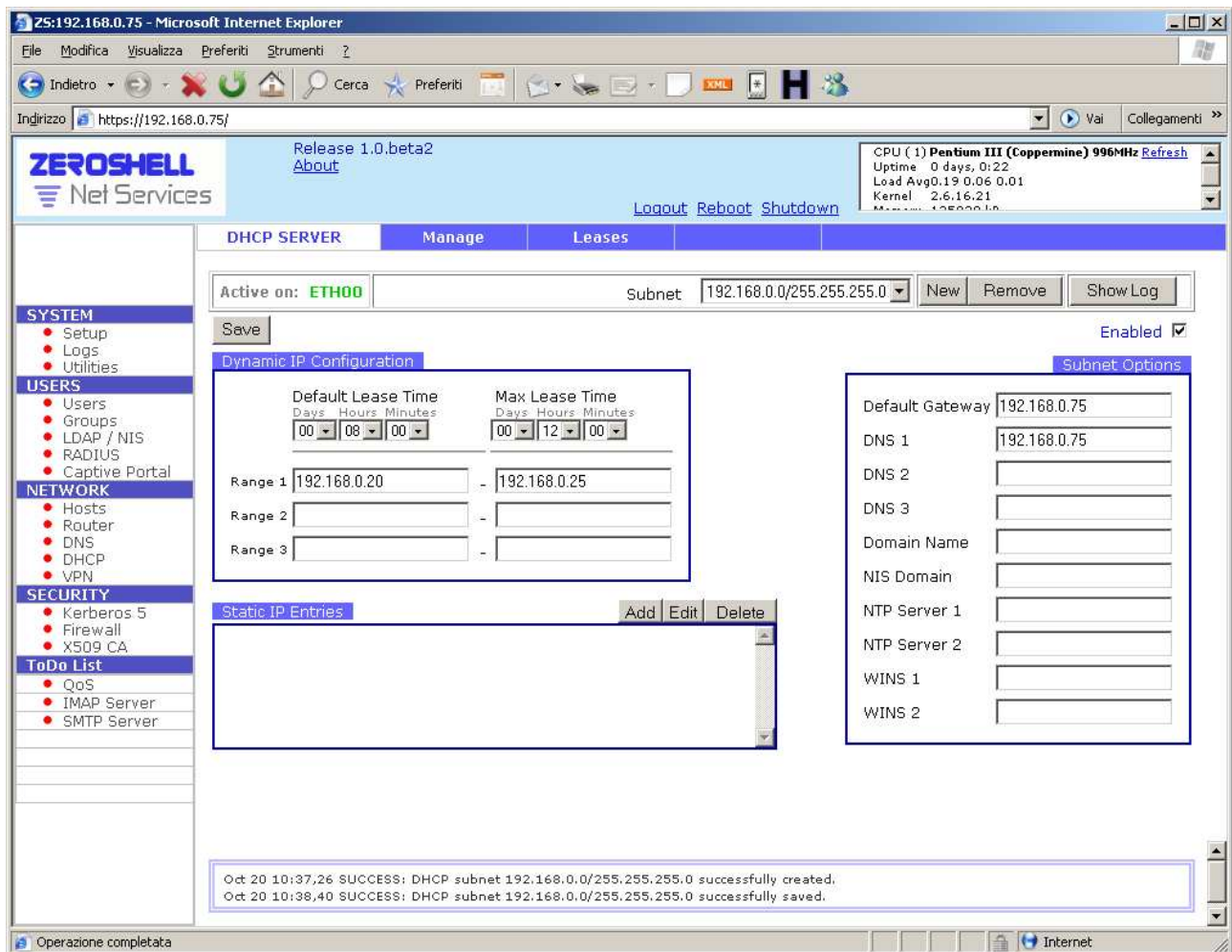
Static IP Entries Add Edit Delete

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

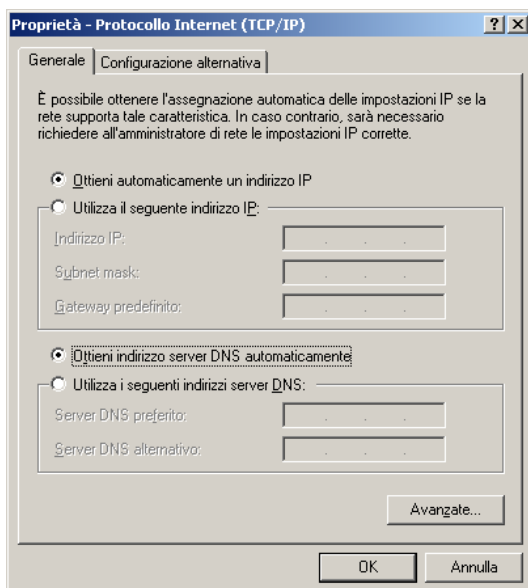
Now we choose the range of ip addresses available to be distributed:



and save.

ZeroShell is also our default gateway and DNS server!

Our client network configuration:



few seconds and we can verify that:

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

Static routes to remote networks:

If we have any remote networks connected through a router, we can set static routes.

For example if we must reach remote network: 192.168.50.0/24 through the router 192.168.0.254 , we can set this using **ROUTER** and **ADD**:

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: ACTIVE' status and a table of 'STATIC ROUTES'. The table has columns: Destination, Netmask, Type, Metric, Gateway, Interface, and State. A single entry is shown: Destination: DEFAULT GATEWAY, Netmask: 0.0.0.0, Type: Net, Metric: 0, Gateway: 192.168.1.254, Interface: (empty), State: Up. At the bottom, a status bar shows two messages: 'Oct 20 10:38,40 SUCCESS: DHCP subnet 192.168.0.0/255.255.255.0 successfully saved.' and 'Oct 20 10:47,35 SUCCESS: Session opened from host 192.168.0.25 (Admin)'.

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

'Metric' is the cost , the priority to follow if many different routes exists for the same destination network.

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 Internet

We can activate also RIP v2 protocol. It is used to let more existing routers dynamically share informations about known remote networks.

Virtual Servers:

It is possible to share internal network services with external network (internet). We can for example choose to publish a website.

Using **ROUTER** , choose **VIRTUAL SERVER** :

The screenshot shows a web browser window titled "https://192.168.0.75 - Port Forwarding - Microsoft Internet Explorer". The page is titled "Virtual Server" and has "View" and "Close" buttons in the top right. Below the title is a form with five input fields: "Input Interface" (a dropdown menu showing "ALL"), "Protocol" (a dropdown menu showing "TCP"), "Local Port" (an empty text box), "Remote IP" (an empty text box), and "Remote Port" (an empty text box). To the right of these fields are "Add" and "Delete" buttons. Below the form is a table with four columns: "Interface", "Protocol", "Local Port", and "Real Servers". The table is currently empty. Below the table is a "Notes:" section with the following text: "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". At the bottom of the page, there is a status bar with the text "Operazione completata" and an "Internet" icon.

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

We must chose the interface , the protocol and the port listening for this service on Zeroshell system. Then we must set where is the service in our secure network: 192.168.0.100. It's the webserver publishing our homepage on port 80 TCP.

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

We must be sure that xDSL router has not NAT enabled. If NAT is enabled we must be sure that requests on port 80 tcp arrive Zeroshell ETH01. For example in my 3com router I have set that every kind of request from internet must reach my Zeroshell External Interface:

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

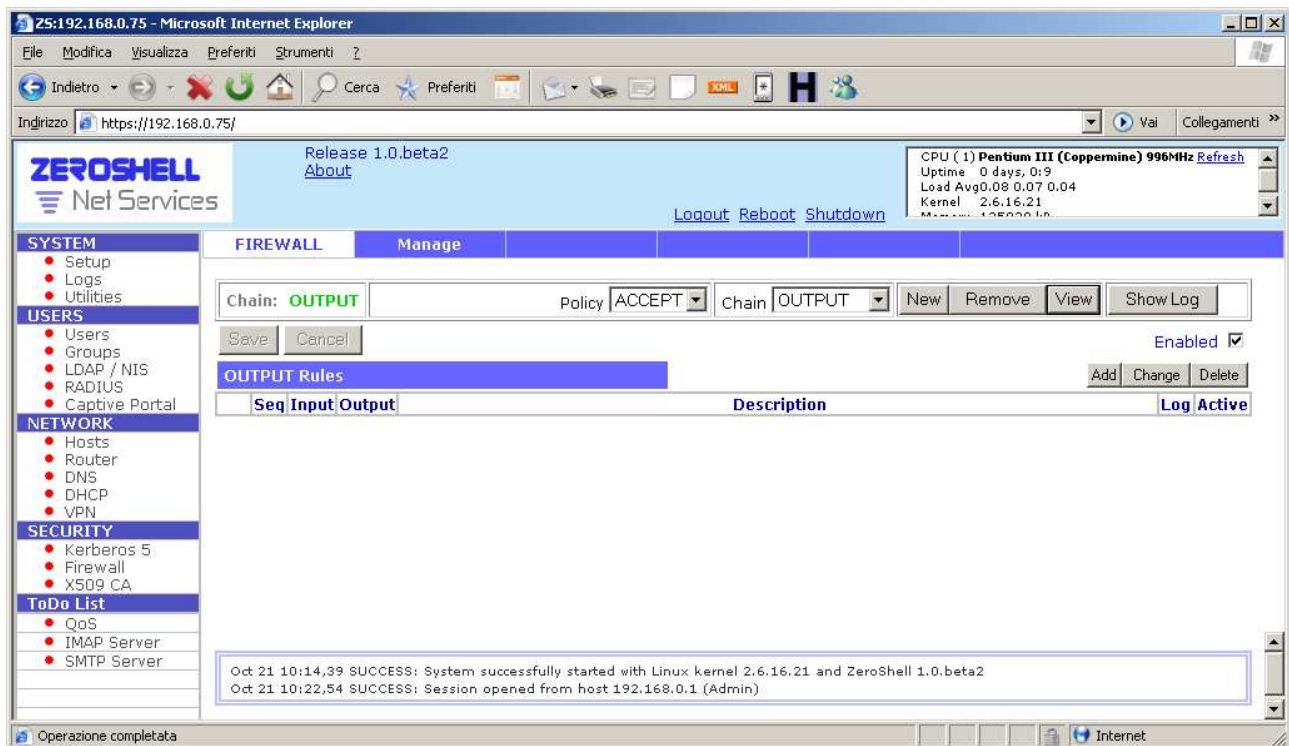
IP Address of Virtual DMZ Host

| | 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 |

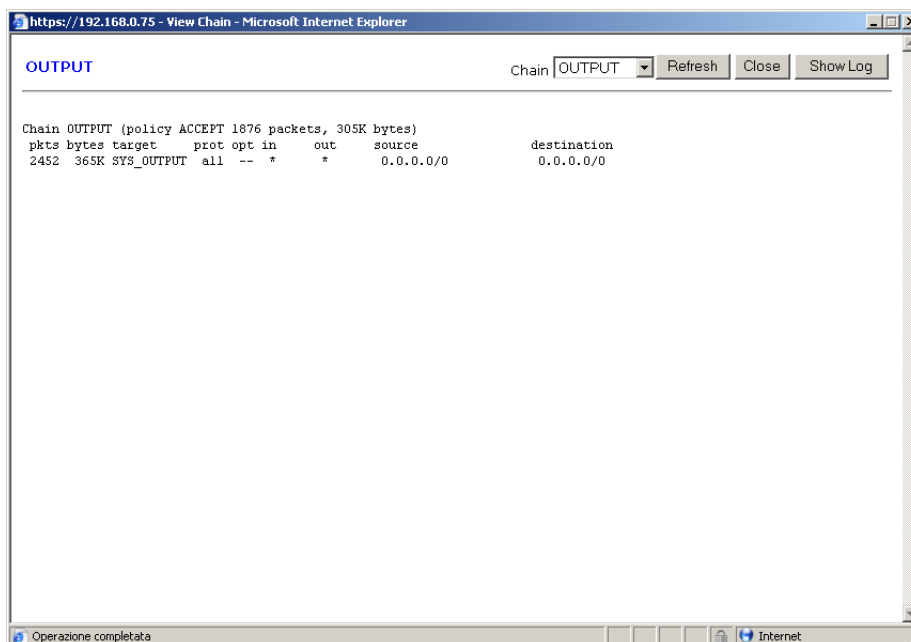
Help Apply Cancel

Security: check default policies

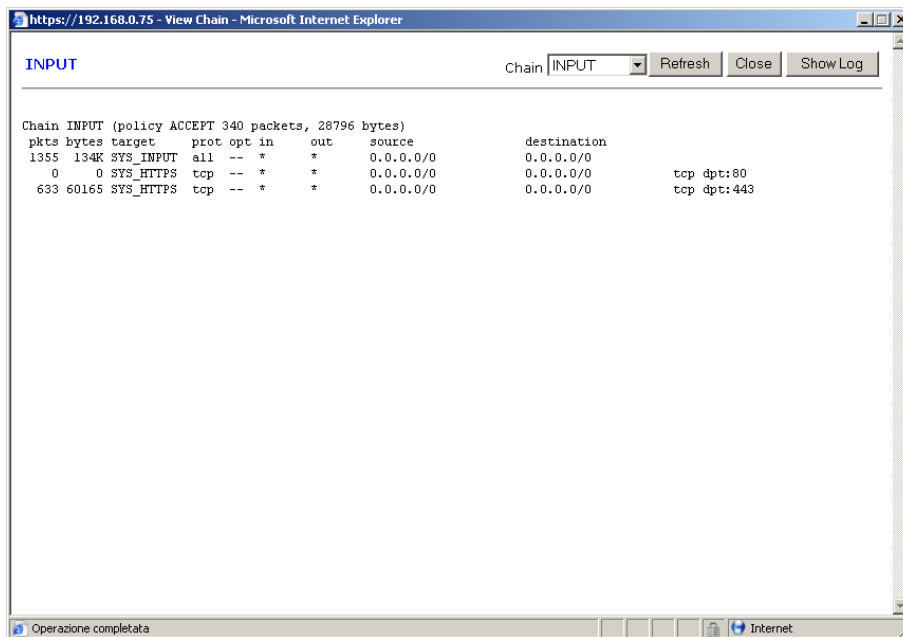
Using **FIREWALL** we can check the default network policies on our firewall.
Choose **CHAIN OUTPUT** and click **VIEW**:



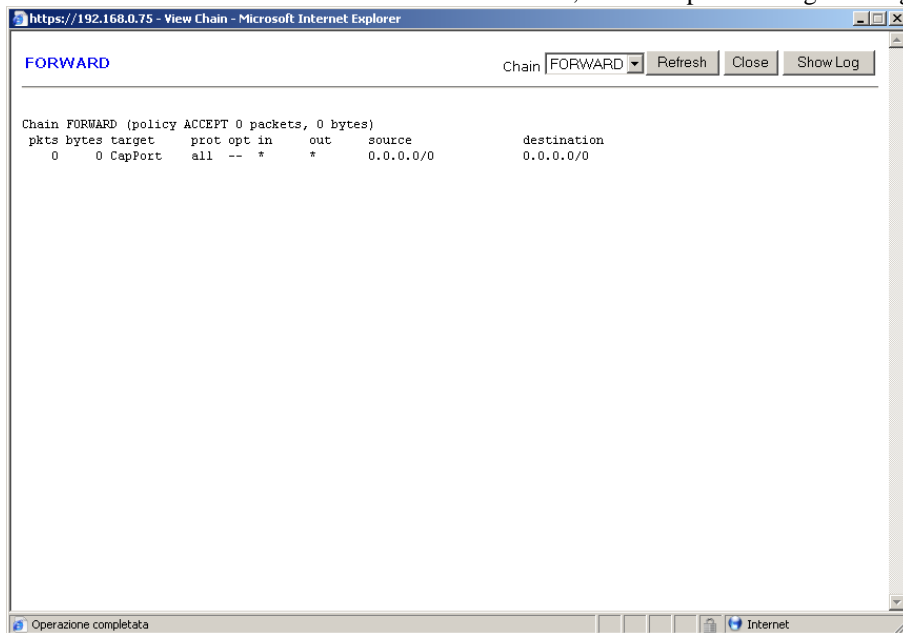
These are output policies:



Choose now **CHAIN INPUT** and click **VIEW** , these are the default incoming policies:



Choose now **CHAIN FORWARD** and click **VIEW** , these are policies to get through the firewall:



We can see that requests from internal ETH00 to external ETH01 are allowed; Nothing is set from ETH01 to ETH00 so nothing will pass through.