

Realizzazione di un HotSpot su rete Fastweb con ZeroShell su VMWare



Il sistema operativo multifunzionale

creato da [Fulvio Riccardi](#)

www.zeroshell.net

Autore: Antonio C.

Hardware e software utilizzato:

Pentium Celeron 2,53GHz, 768MB, MB Biostar P4VMA-M, 160GB Hard Disk, Ati Radeon 9250

Access Point Edimax EW-7206APg, LAN PCI 10/100Mb e LAN on-board

Windows XP Pro SP2, VMWare Workstation, ZeroShell 1.0 beta12.

Utilizzo della macchina:

Fornire accesso regolato dal gestore ad Internet per un locale pubblico. È stato utilizzato VMware poiché la stessa macchina deve fornire anche supporto per audio e video.

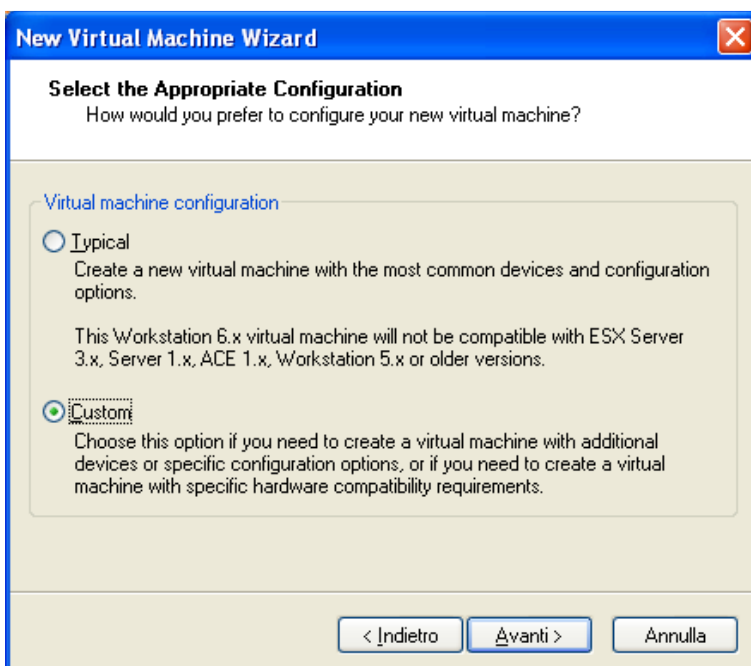
Tutorial:

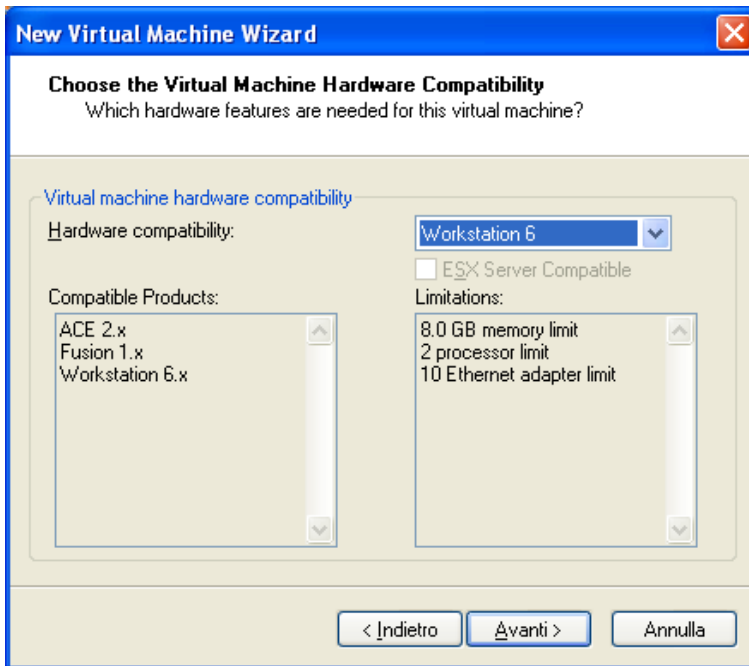
Ho realizzato una sistema che funzionerà da player audio/video e HotSpot WiFi per un locale pubblico. L'utilizzo di VMware (e l'aiuto preziosissimo dei ragazzi sul forum) ha permesso di utilizzarne solo una per entrambe le funzioni. Nel mio caso è stato utilizzato un Celeron 2,53GHz con 768MB di RAM recuperato da una precedente applicazione. E' stata necessariamente aggiunta un'altra scheda di rete PCI (quindi un totale di 2 interfacce LAN) per poter connettere un Access Point (AP) tramite un cavo crossed.

Preparate la macchina con tutto il software necessario (ovviamente anche VMware Workstation!).

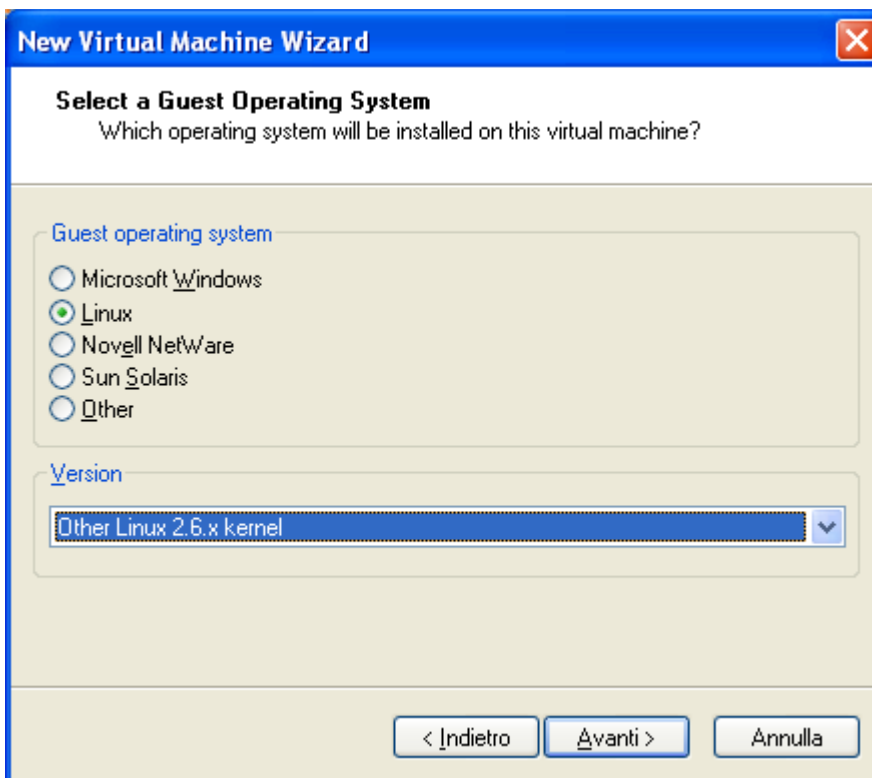
Siamo pronti per cominciare: lanciate VMware Workstation.

Create una nuova macchina virtuale con vmware:



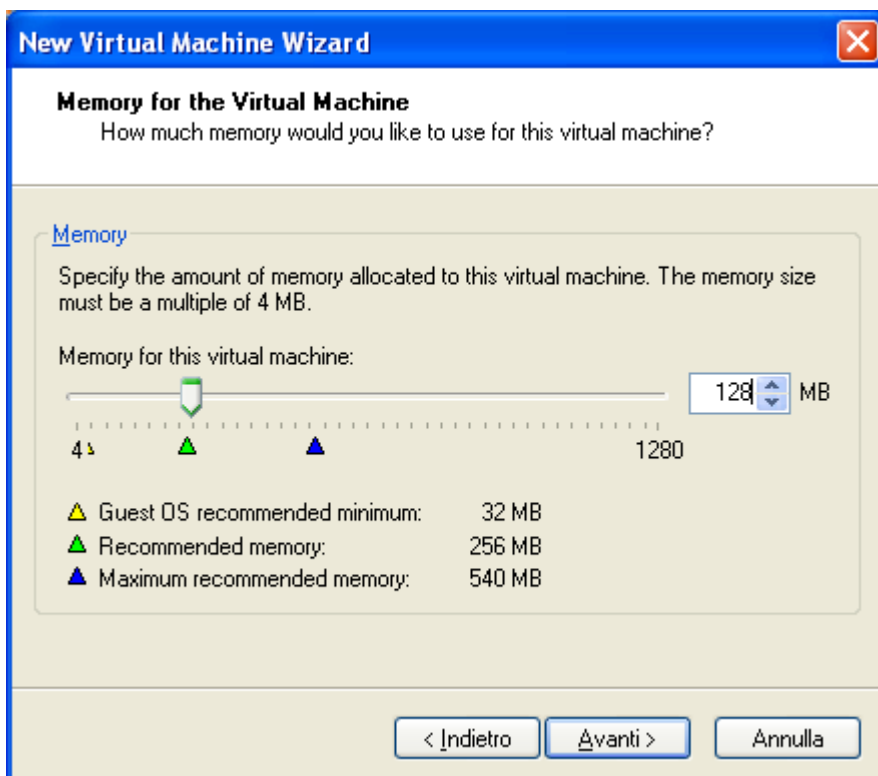
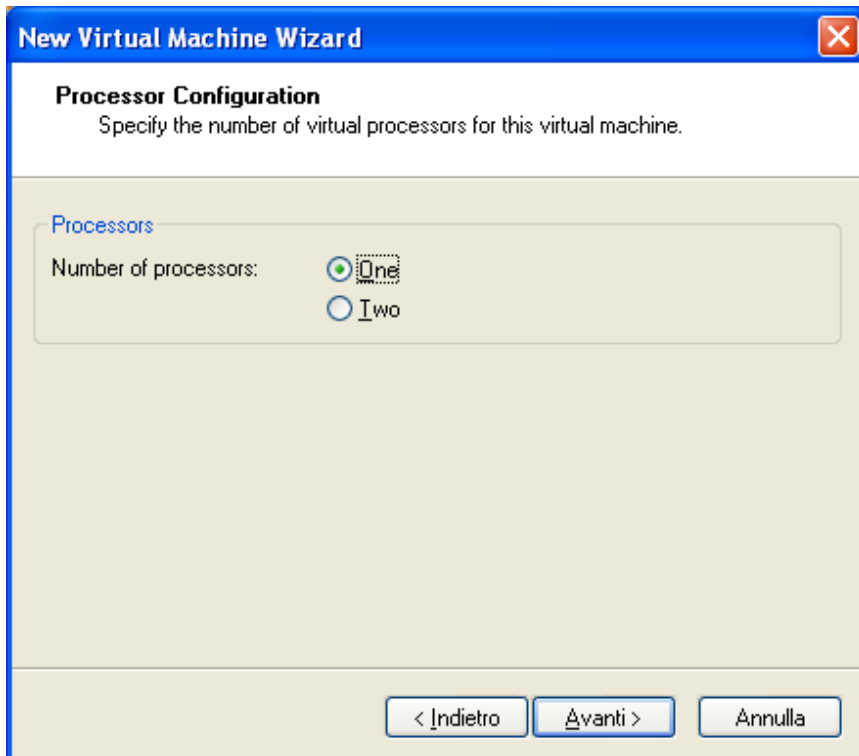


Selezionare come sistema operativo Linux:

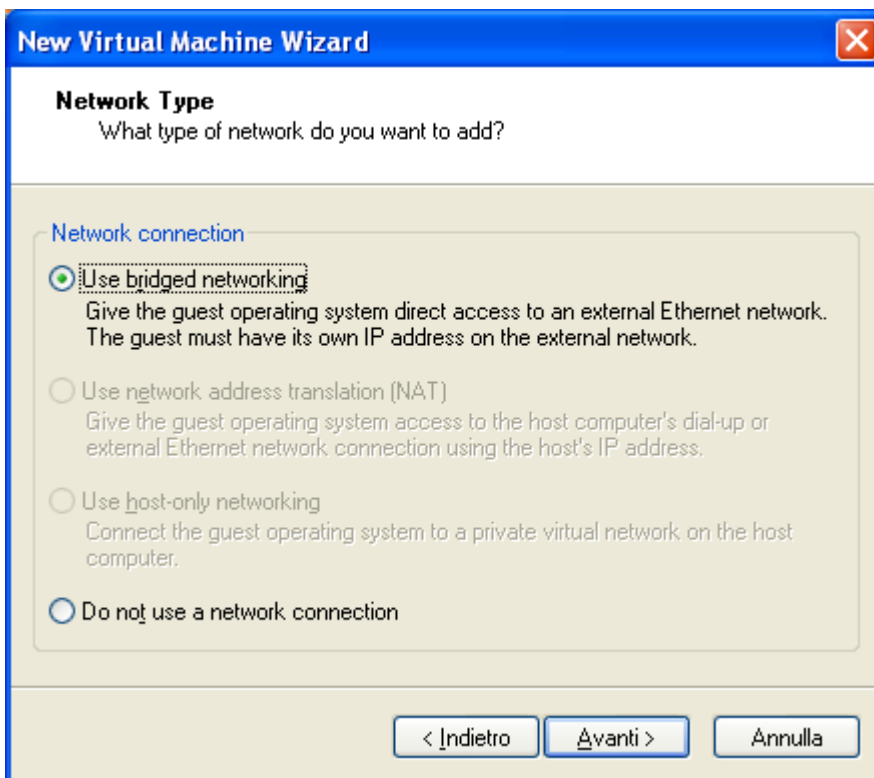


In seguito, verrà chiesto di salvare la virtual machine in una posizione dell'host, scegliete la directory che preferite. In questa verranno salvate le cartelle di stato, la virtual machine, il disco virtuale e gli altri files necessari al corretto funzionamento di questa.

Anche su macchine multicore è sufficiente utilizzare un solo processore e un quantitativo basso di memoria, 128MB.

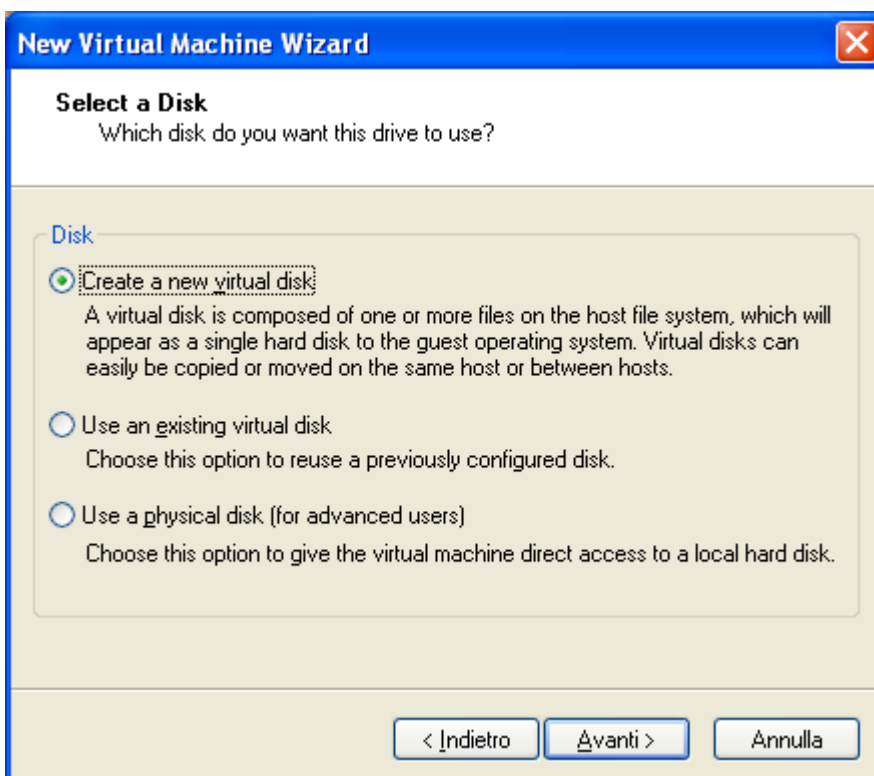


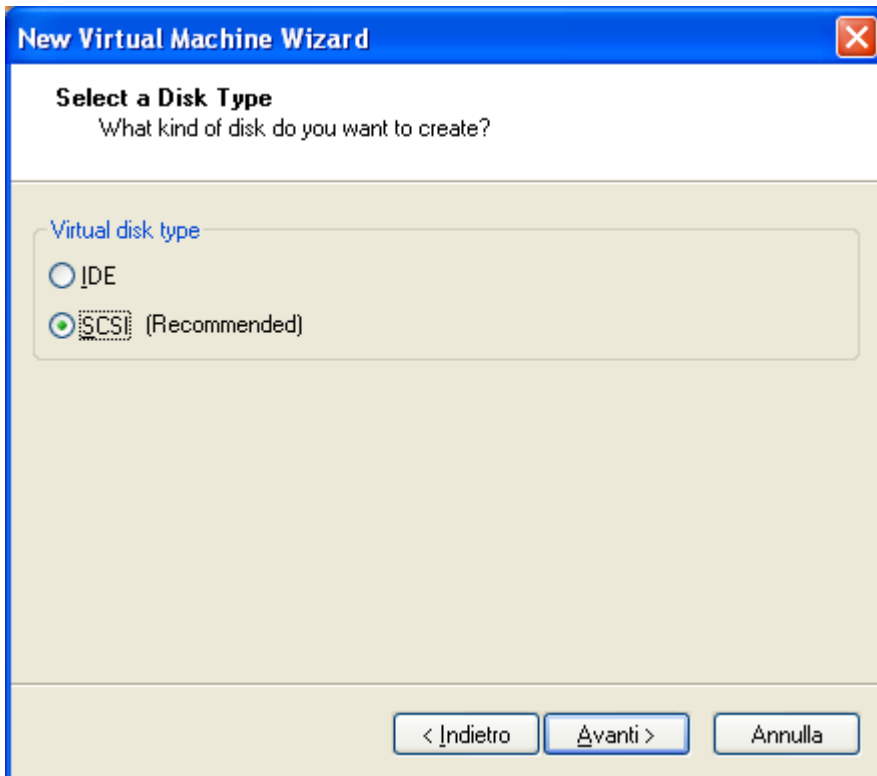
Selezionate quindi la connessione bridged che poi andremo a modificare in seguito.



Dopo questo, vi verrà chiesto di selezionare il tipo di interfaccia per le unità ottiche, lasciate la scelta di default.

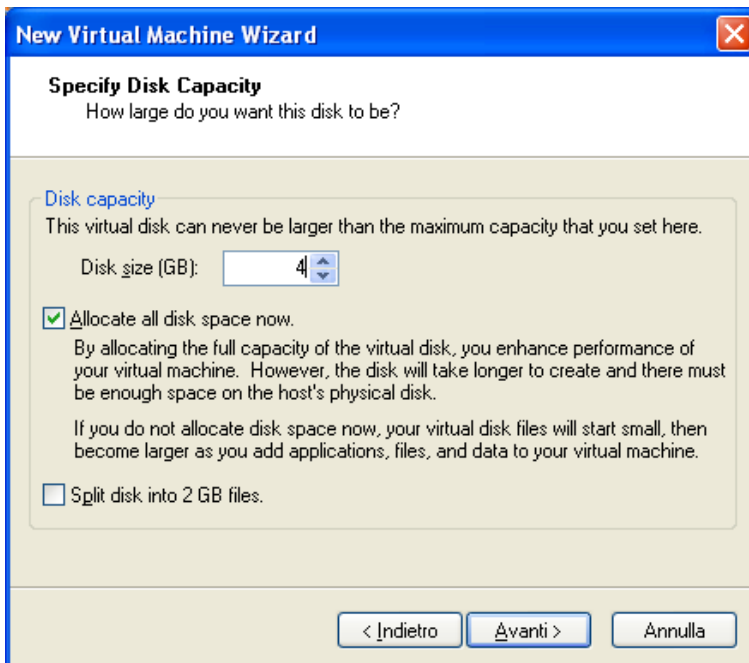
Ora bisogna impostare l'hard disk virtuale: createne uno nuovo SCSI.



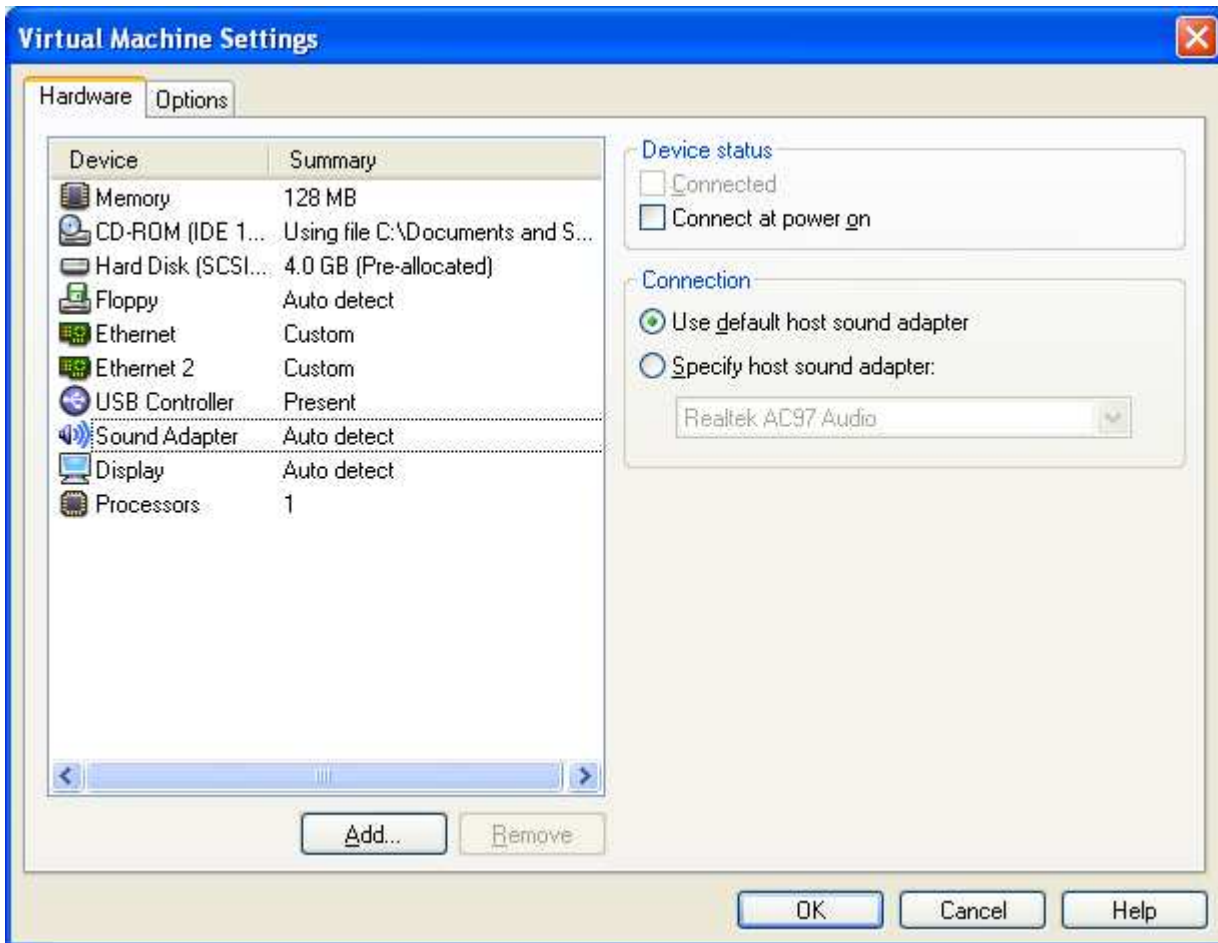


Come dimensioni 4GB dovrebbero bastare nella maggior parte dei casi. Selezionate anche l'allocazione dello spazio al momento della creazione della VM.

Una volta selezionato il nome dell'hard disk virtuale, VMWare procederà ad allocare lo spazio.



Ora che la macchina virtuale è stata creata bisogna configurarne i dettagli.



Aggiungete una scheda ethernet e scegliete la configurazione custom. La "Ethernet" connessetela in bridge su VMNet0, mentre la "Ethernet2" in bridge sulla VMNet1.

Ho anche disattivato il floppy, il controller audio e il controller USB, inutili nella realizzazione.

Nella configurazione del CD-ROM dovete utilizzare l'ISO di ZeroShell che avete scaricato dal sito.

Passiamo ora a configurare le interfacce di rete su XP: l'interfaccia LAN che verrà connessa a Internet l'ho chiamata WAN e ho impostato il bridge su VMNet1, mentre l'interfaccia a cui è connesso l'Access Point l'ho rinominata AP (fantastico, eh?) e impostato il bridge su VMNet0.

Dal manuale di istruzioni del vostro AP trovate l'indirizzo IP di base (nel mio caso 192.168.2.1) ed entrate nel menù di configurazione dello stesso. Oltre a cambiare ovviamente la password di admin, configuratelo come Access Point nelle modalità di funzionamento, impostate l'SSID che preferite (sarà il nome della rete visto dai client) e disattivate il DHCP. Disattivate anche ogni feature di sicurezza (WEP o WPA), visto che verrà utilizzato il Captive Portal di ZS per effettuare l'accesso.

Tanto per rimanere in tema, ho impostato come indirizzo di accesso all'AP 192.168.2.75, mentre il gateway predefinito l'ho impostato su 192.168.2.1, come sarà poi più chiaro.

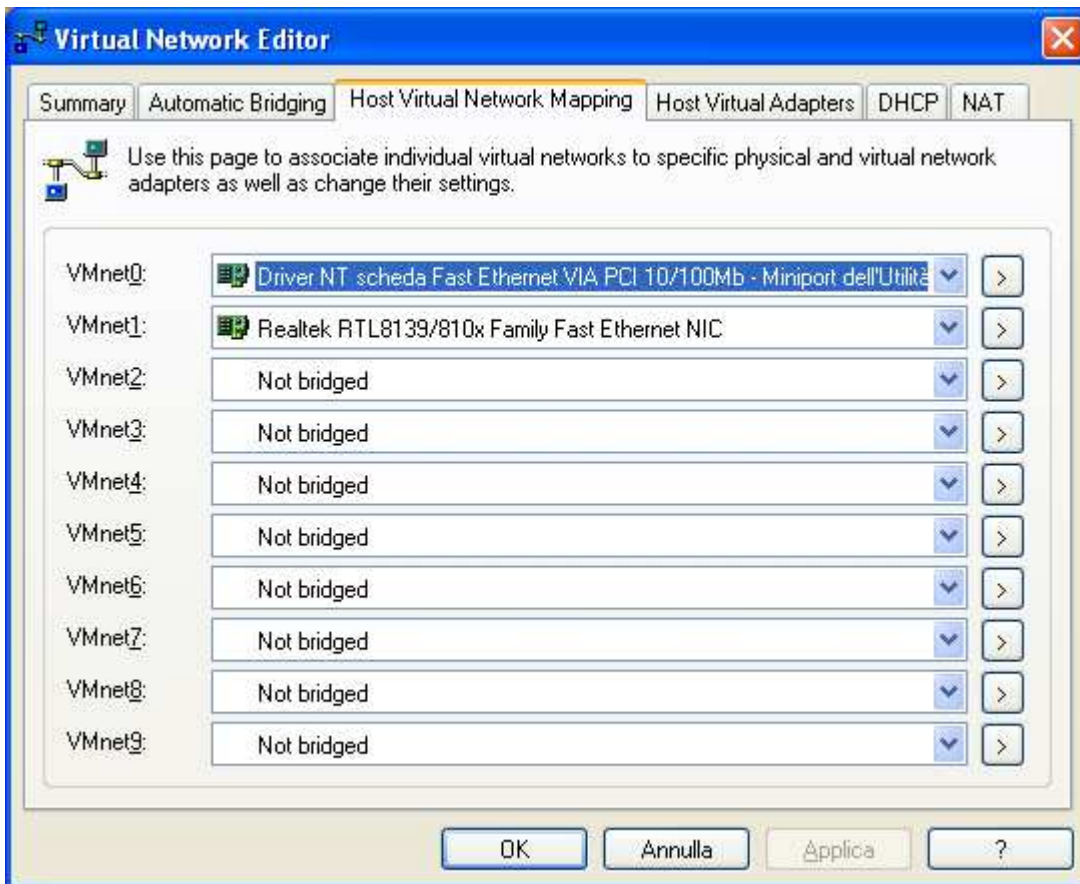
Una volta fatto ciò salvate le modifiche sull'AP e disattivate dalle proprietà di XP tutti i protocolli tranne il bridge di VMWare e il protocollo TCP/IP.



Nelle impostazioni del TCP/IP di questo NIC, imponete l'indirizzo 192.168.2.2, in modo tale da avere accesso a ZS.

Durante la configurazione del sistema mi sono scontrato con un problema: se non imposto un indirizzo IP fisso da XP non riesco ad accedere da host a ZS. Probabilmente c'è il modo di evitarlo, ma nei miei tentativi di configurazione non l'ho trovato.

Su VMWare, nelle opzioni di rete disattivate l'automatic bridging, rimuovete e stoppate i servizi DHCP e NAT ed effettuate il bridge tra le schede fisiche e virtuali: AP su VMNet0 e WAN su VMNet1:



Rimuovete anche gli adattatori virtuali sull'host, tanto il bridge lo fa direttamente VMWare ed evitate di avere mille e più adattatori nelle connessioni di rete di XP.

Nel mio caso la porta WAN è connessa all'HAG di fastweb, di conseguenza IP, Gateway e DNS mi vengono forniti da DHCP. Dal lato AP avendo disattivato anche il protocollo TCP/IP ogni configurazione verrà fatta da ZS.

Avviamo quindi la macchina virtuale. Per sveltire il boot, accedete con F2 al BIOS della VM e mettete come primo dispositivo di boot il CD-ROM. Una volta caricato ZS, accedete all'IP Manager con "I".

Dobbiamo aggiungere un IP sulla ETH00 (quella connessa all'AP): selezionate "A" e aggiungete un IP della stessa classe dell'AP. Nel mio caso il menù l'ho spostato su 192.168.2.75, ho quindi scelto come indirizzo IP 192.168.2.1.

Attivate quindi il Dynamic IP sulla ETH01 con "H". Scrivete "ETH01" per selezionare l'interfaccia, e "enabled" alla richiesta successiva. Così facendo ZS è in grado di ricevere dinamicamente IP e Gateway.

A questo punto se aprite il browser sull'host e digitate 192.168.2.1 nella barra degli indirizzi dovrebbe apparire la richiesta per accettare il certificato di sicurezza, fatelo, salvatelo in modo permanente e accedete tramite "admin" e "zeroshell".

Se tutto è andato bene sarete loggati su ZS, il quale già vede internet (nel riquadro a destra vedete la cronologia degli aggiornamenti e nessuna scritta rossa che vi comunica che ZS non vede il suo sito).

Se cliccate su "Network" dovrebbe apparire una schermata simile a questa:

The screenshot shows the ZeroShell web interface in Mozilla Firefox. The browser address bar shows `https://192.168.2.1/`. The page title is "ZS:192.168.2.1 - Mozilla Firefox". The interface includes a navigation menu on the left with categories: 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), and To Do List (IMAP Server, SMTP Server). The top navigation bar has tabs: SETUP, AutoUpdate, Profiles, Network, Time, https, SSH, Startup/Cron, and Logs. The Network tab is selected, showing a table of network interfaces. The table has columns for interface name, description, IP address, and status. The interfaces listed are ETH00, ETH01, and VPN99. ETH00 and ETH01 are up, while VPN99 is down. The status bar at the top right shows system information: CPU (1) Intel(R) Celeron(R) CPU 2.53GHz, Uptime 0 days, 0:17, Load Avg. 0.18 0.15 0.15. The bottom status bar shows "Completato" and the IP address "192.168.2.1".

Interface	Description	IP Address	Status
ETH00	Duplex Advanced Micro Devices [AMD] 79c970 [PCnet32 LANCE] (rev 10)	192.168.2.1	UP
ETH01	Duplex Advanced Micro Devices [AMD] 79c970 [PCnet32 LANCE] (rev 10)		UP
VPN99	Connections from Road Warrior clients not accepted Host-to-LAN OpenVPN Interface	192.168.250.254	DOWN

Se non richiesto per l'utilizzo che si deve fare del sistema, si può rimuovere la rete virtuale.

Cliccate ora su Profiles, selezionate lo spunta su “**Model: VMware, VMware Virtual S(sda)**” e cliccate su New Partition:

New Partition - Mozilla Firefox

https://192.168.2.1/cgi-bin/kerbynet?Section=Storage&STk=db8b8e1e1789fe1890ed593524b76ed093d74ea9&Action=NewPartiti

VMware, VMware Virtual S (sda) Refresh Close

Disk /udev/sda: 4294 MB, 4294967296 bytes
255 heads, 63 sectors/track, 522 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes

Partition Size

Fixed Size GB

Max Available

Label

Filesystem type Format now

Extended 3 (journald)

Reiserfs (journald)

Extended 2 (unjournald)

FAT 32 (unjournald)

Completato 192.168.2.1

Aggiungete la Label che preferite e cliccate su Create Partition.

Selezionate ora l'sda1 e cliccate "Create Profile". Aggiungete i dati che preferite e cliccate su Create.

Create Profile - Mozilla Firefox

https://192.168.2.1/cgi-bin/kerbynet?Section=Storage&STk=db8b8e1e1789fe1890ed593524b76ed093d74ea9&Action=

VMware, VMware Virtual S (sda)

New Profile on partition sda1

Description	<input type="text" value="I Califfi"/>
Hostname (FQDN)	<input type="text" value="zeroshell.example.com"/>
Kerberos S Realm	<input type="text" value="EXAMPLE.COM"/>
LDAP Base	<input type="text" value="dc=example,dc=com"/>
Admin password	<input type="password"/>
Confirm password	<input type="password"/>

NETWORK CONFIG

Ethernet Interface	<input type="text" value="ETH01 - Advanced Micro Devices [AMD] 79c970 [PCnet32 LANCE] (rev 1C)"/>
IP Address / Netmask	<input type="text" value="192.168.2.1"/> / <input type="text" value="255.255.255.0"/>
Default Gateway	<input type="text"/>

Completato 192.168.2.1

A questo punto abbiamo creato il database per ZS.

Fate un log-out e tornate sulla VM. Attivate (Activate Profile) il profilo appena creato. ZS si riavvierà e potremo controllare dall'IP manager se tutto è rimasto come prima. Nel mio caso ho dovuto riattivare il dynamic IP e aggiungere nuovamente l'IP 192.168.2.1 alla ETH00.

In Setup->https settings selezionate come unica interfaccia autorizzata la ETH00, così che ZS sia accessibile solo dall'host.

HTTPS Settings - Mozilla Firefox

https://192.168.2.1/cgi-bin/kerbynet

HTTPS Web Interface Settings

Save Close

Allow access only from IP Interface + -

Interface ETH00

Notes: the IP addresses can be a single IP (ex. 192.168.0.15) or a subnet (ex. 192.168.0.0/255.255.255.0 or 192.168.0.0/24). If the server becomes unreachable you could need to put the system into Fail-Safe mode using the local console to disable the Firewall.

X.509 Configuration

View Cancel

X.509 Host Certificate

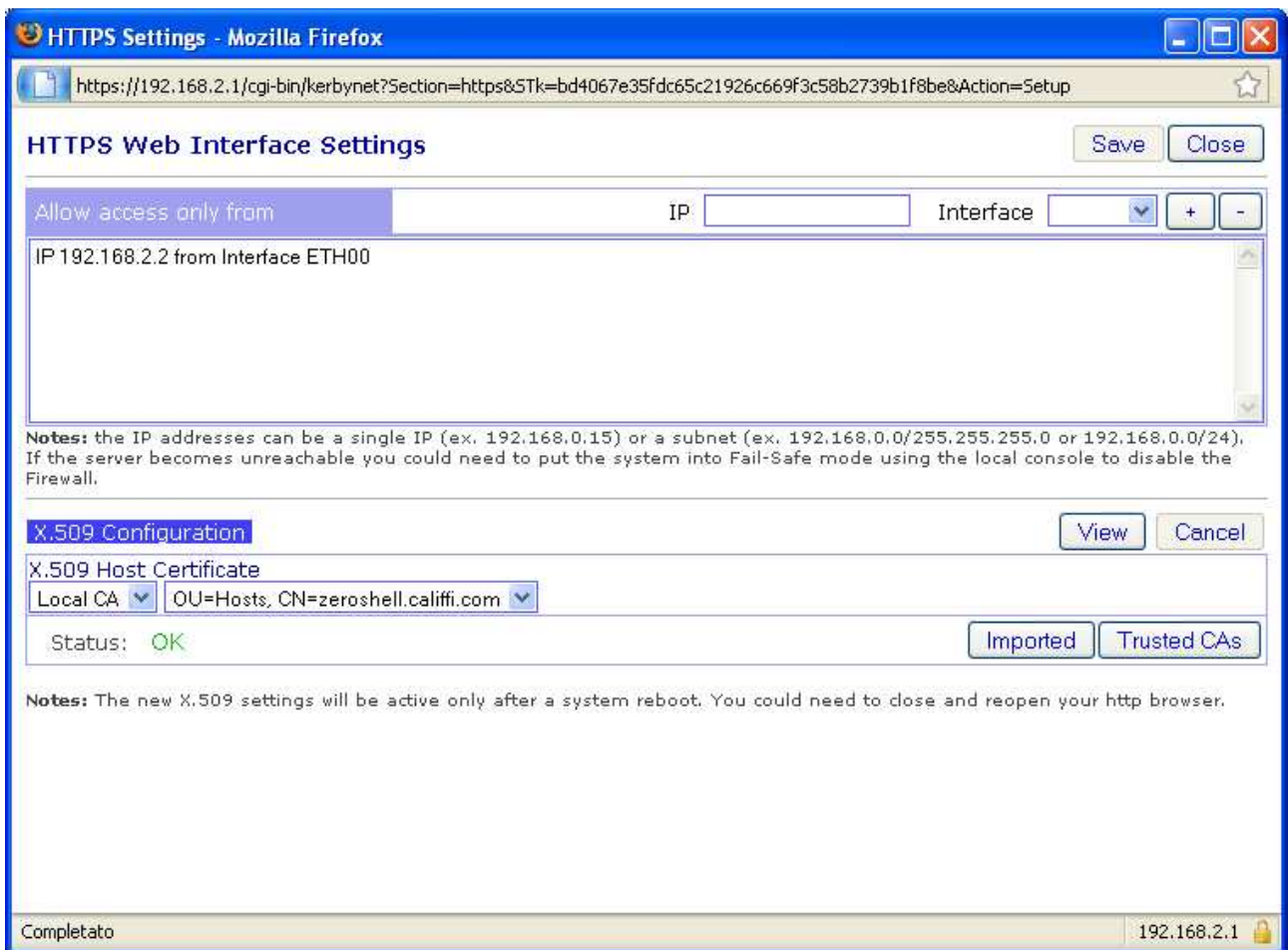
Local CA OU=Hosts; CN=zeroshell.califfi.com

Status: OK Imported Trusted CAs

Notes: The new X.509 settings will be active only after a system reboot. You could need to close and reopen your http browser.

Completato 192.168.2.1

Per migliorare la sicurezza del sistema, è inoltre possibile (se non avete necessità di accedere al setup di zeroshell dai client) aggiungere l'IP della scheda interna (assegnato prima nelle proprietà del TCP/IP su XP) come unico accettato:



Andate ora nella configurazione del DHCP.

Cliccate su NEW e aggiungete la sottorete 192.168.2.0:

Available: 192.168.2.0/255.255.255.0 (ETH01)

Network: 192.168.2.0

Netmask: 255.255.255.0

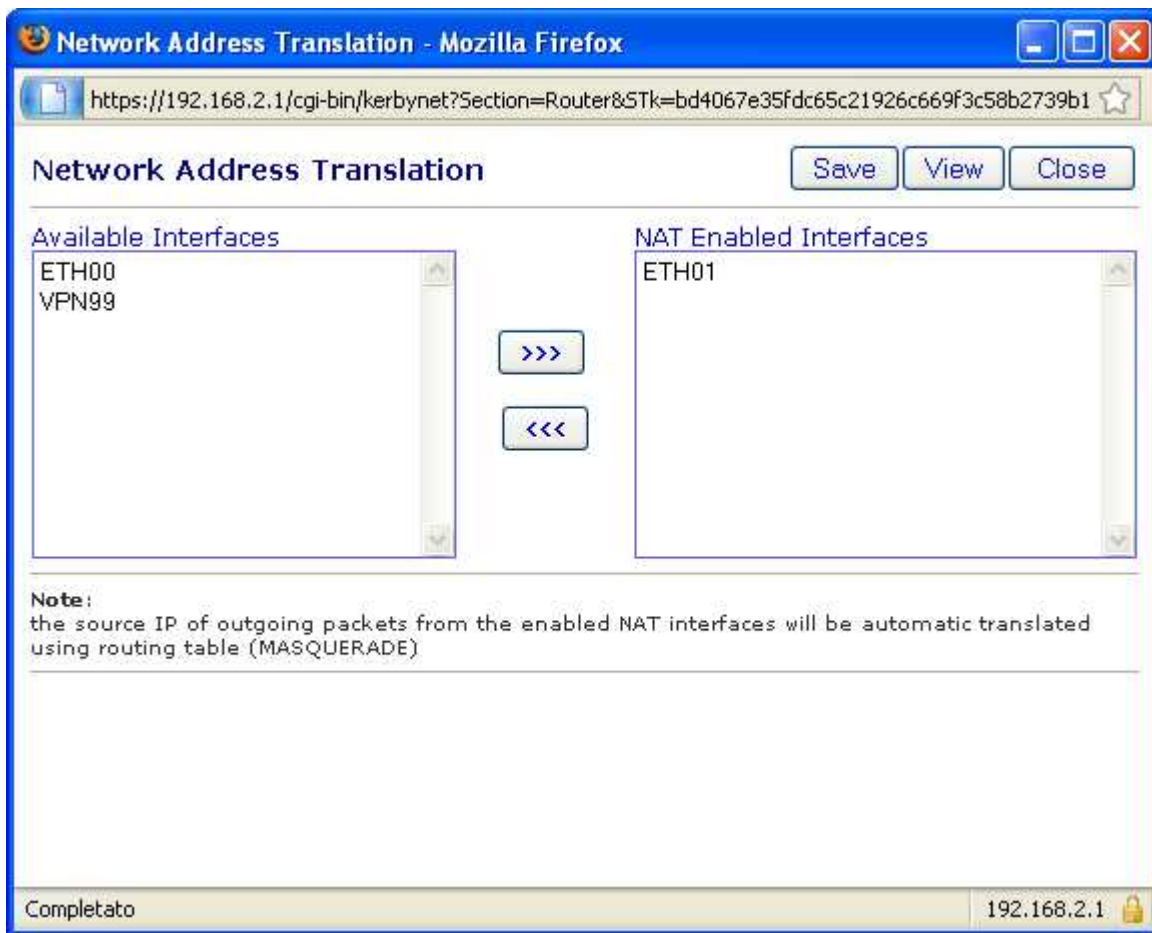
OK Cancel

Completato 192.168.2.1

Risulteranno come default gateway e dns 192.168.2.1: è corretto.

Negli intervalli IP di competenza del DHCP ho selezionato da 192.168.2.100 a 192.168.2.200. Salvate.

Ora andate in Router->NAT e attivate il NAT sulla ETH01:



Attivate il Captive Portal, selezionando la ETH00, mettendo lo spunta su GW e selezionando "not allowed" le connessioni simultanee. Salvare.

Andate in Captive Portal -> Authentication e selezionate il "Do not use https". Così facendo i client non devono accettare il certificato di sicurezza e si evitano paranoie inutili. Da notare che l'HotSpot nel mio caso sarà gratuito, quindi una minor sicurezza in questo caso non crea problemi.

Per come è configurato ora il sistema, l'accesso al setup di ZS avviene tramite la ETH00, sulla quale è attivo il Captive Portal. Per evitare di dover inserire due volte username e password, è possibile aggiungere nella finestra in basso a destra un "Free Authorized" client (ricordatevi di selezionare dal menù a tendina "Clients"). Una volta impostato indirizzo IP e MAC, il Captive Portal non richiederà le credenziali.

The screenshot displays the ZeroShell web interface in Mozilla Firefox. The browser address bar shows `https://192.168.2.1/`. The interface includes a top navigation bar with tabs for **CAPTIVE PORTAL**, **Gateway**, **Authentication**, **Language**, **Accounting**, and **Graphics**. The **CAPTIVE PORTAL** tab is selected, showing the following configuration:

- GW**: Active on: **ETH00**
- Mode**: Routed
- Interface**: ETH00
- Buttons**: Save, Show Log

On the right side, there are configuration sections:

- Authentication**: Web Login (Local), Remote IP / Port (12080), Shared Secret.
- Gateway Parameters**: Client Identity (IP and MAC address), Simultaneous Connections (Not allowed), Authenticator Validity (5 minutes).
- Free Authorized Clients**: A table with columns for Description, IP Address, and MAC Address. One entry is visible: Host (192.168.2.2) with a redacted MAC address.

A left sidebar contains a menu with categories: **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), and **To Do List** (IMAP Server, SMTP Server).

At the bottom, a log window shows the following messages:

```
Jun 14 01:11:38 SUCCESS: Session closed for Admin user
Jun 14 01:11:50 SUCCESS: Session opened from host 192.168.2.2 (Admin)
```

The status bar at the bottom indicates "Completato" and the IP address "192.168.2.1".

Ho anche aggiunto nella sezione DNS->Dynamic DNS Clients OPENDNS (anche se non sono certo della necessità dell'operazione):

The screenshot shows a web browser window titled "Dynamic DNS Client - Mozilla Firefox". The address bar contains the URL: <https://192.168.2.1/cgi-bin/kerbynet?Section=DNS&STk=bd4067e35fdc65c21926c669f3>. The page title is "Dynamic DNS Updater".

At the top right, there is a checkbox labeled "Enabled" which is currently unchecked. Next to it are "Save" and "Close" buttons. Below these is a "Show Log" button.

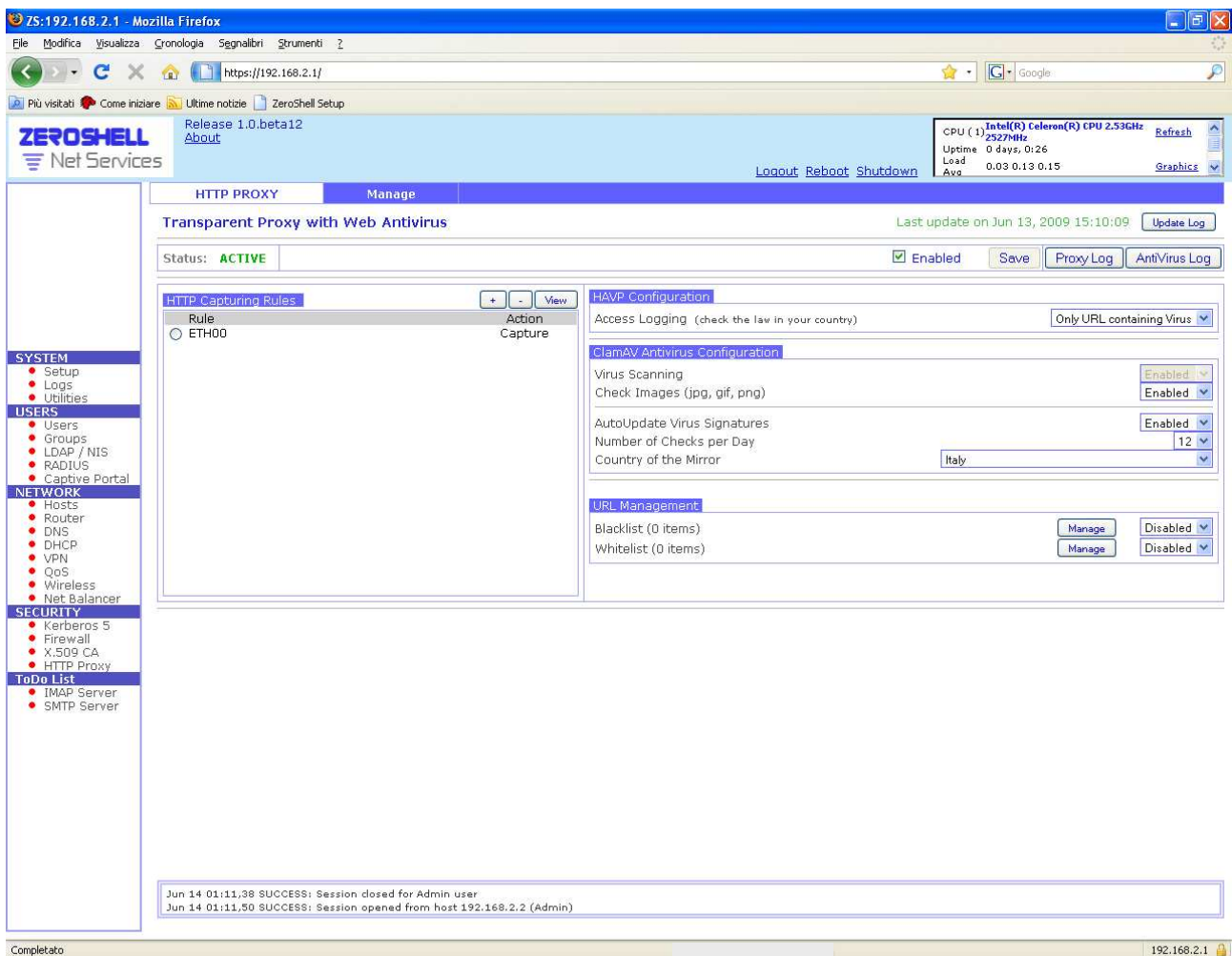
The form contains the following fields:

- Hostname: N/A
- Domain: OpenDNS (dropdown menu)
- Username: user
- Password: (empty text box)
- Confirm: (empty text box)

Below the form, a note reads: "Note: To use this dynamic DNS you need an account on <http://www.dyndns.com> or on <http://www.opendns.com>."

The status bar at the bottom shows "Completato" on the left and "192.168.2.1" with a lock icon on the right.

Ho infine attivato il Proxy http imponendo il controllo sulla ETH00:



Aggiungete ora uno user di prova dall'apposito menù e provate a navigare via WiFi. Dovrebbe andare tutto.

Quanto alle altre personalizzazioni e funzionalità, vi rimando alla sezione documentazione e al forum.

Buon lavoro!

Credits:

Un grazie sincero a Fulvio per la realizzazione di questo sistema e grazie ai ragazzi sul forum, sempre pronti ad aiutare!

Questa guida è stata fatta da un niubbo per niubbi.

Antonio C.

auzmann@hotmail.com