

Zeroshell: VPN Host-to-Lan



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

www.zeroshell.net

Securing the connection between a host and a network

(Author: cristiancolombini@libero.it)

Securing the connection between a host and a network:

This short guide will lead us to create a tunnel VPN (secure and protected connection) between a host and a network. This VPN will give us security in communication during the data exchange. We could also write down security policies between the host and the network using the firewall in the between.

Here the steps to be followed

Logical scheme of the solution

Preparing the firewall

Preparing certificates

Creating users and hosts

Exporting the certificates for the remote host

Creating VPN Tunnel

Microsoft client configuration

Communication policies

Logical scheme of the solution:

Before starting we have to understand what we are doing:

We have to connect in a secure way a host to a network through internet.

I have realized this configuration in my room, at home, where I have not real public ip addresses; only for this reason I had to use addresses of the same subnet mask on the host and on the external interface of Zeroshell.

In a real situation these addresses will not belong to the same subnet. Most of the times the client will be connected to internet using a dialup connection with dynamic ip address.

We must disable NAT on the router connected to Zeroshell external uinterface.

Ip addresses:

SiteA:

Private Lan: 192.168.0.0/24

Public Ip on Zeroshell External interface: 62.62.62.1

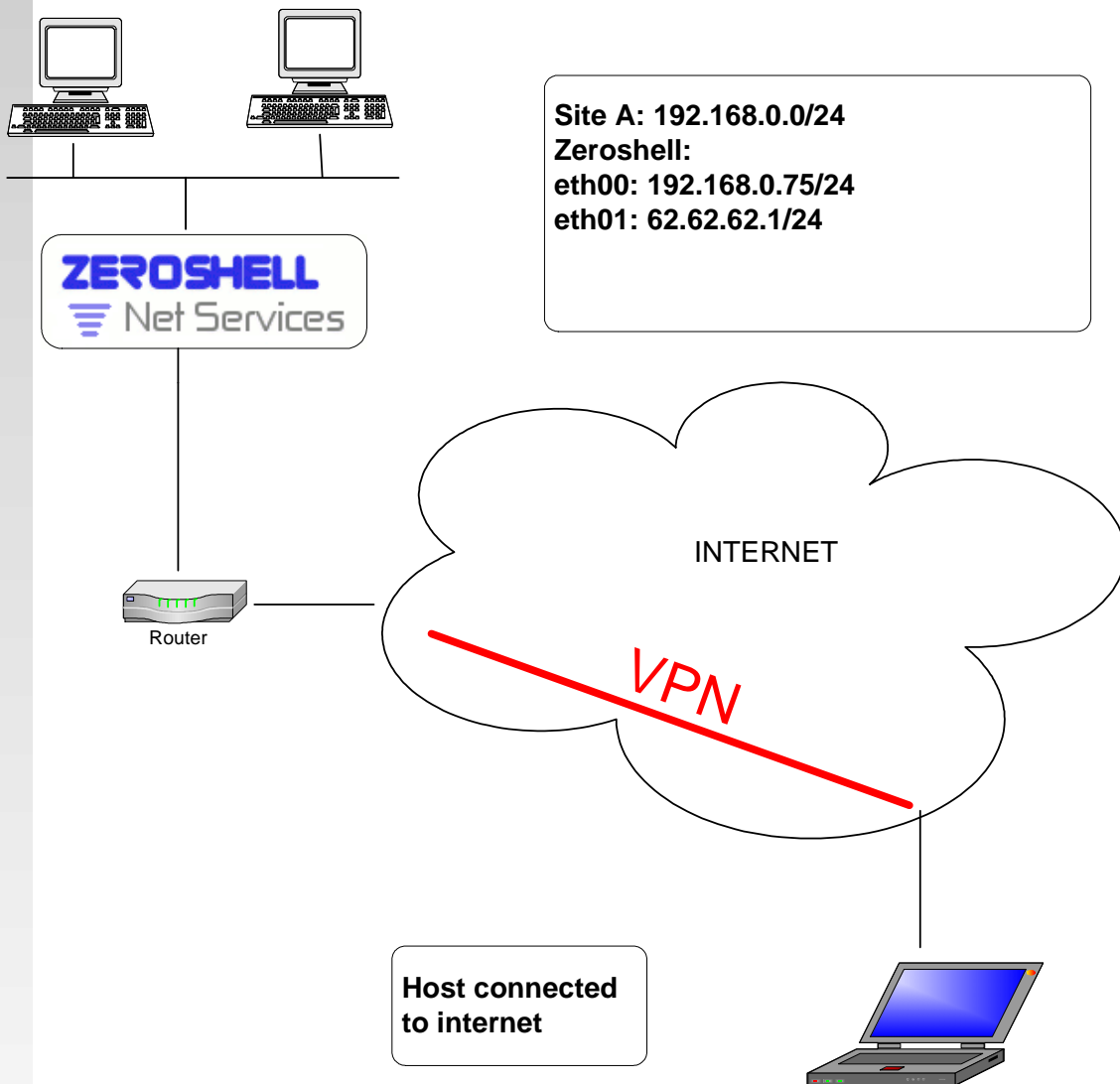
Host:

Dynamic ip address (in my test is 62.62.62.2)

In the following image the red line is the VPN Tunnel.

VPN con Zeroshell

Mercoledì 7 Marzo 2007

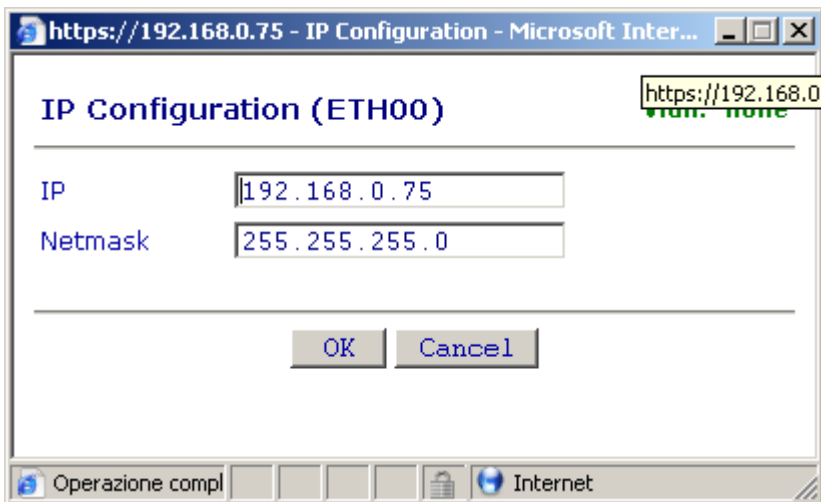


Preparing the firewall

Using the document “How to secure my private network” at www.zeroshell.net, you will find an easy way to prepare the firewall:

- 1 – setup of Zeroshell
- 2 – Set ip address on internal interface:

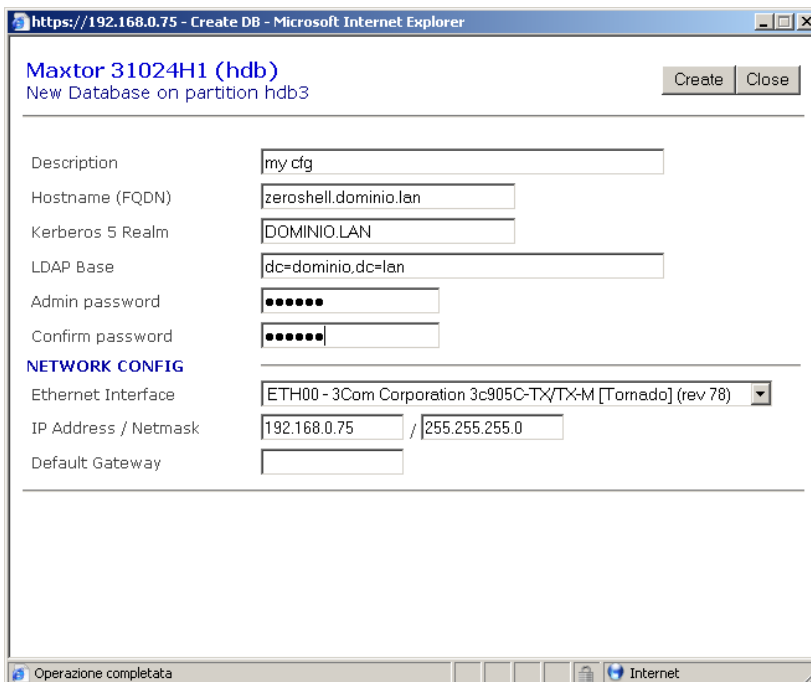
SiteA:



The screenshot shows a web browser window titled "https://192.168.0.75 - IP Configuration - Microsoft Inter...". The main content is a form titled "IP Configuration (ETH00)". The form has two input fields: "IP" with the value "192.168.0.75" and "Netmask" with the value "255.255.255.0". Below the fields are "OK" and "Cancel" buttons. The browser's status bar at the bottom shows "Operazione compl" and "Internet".

- 3 – Create a configuration DB:

SiteA:

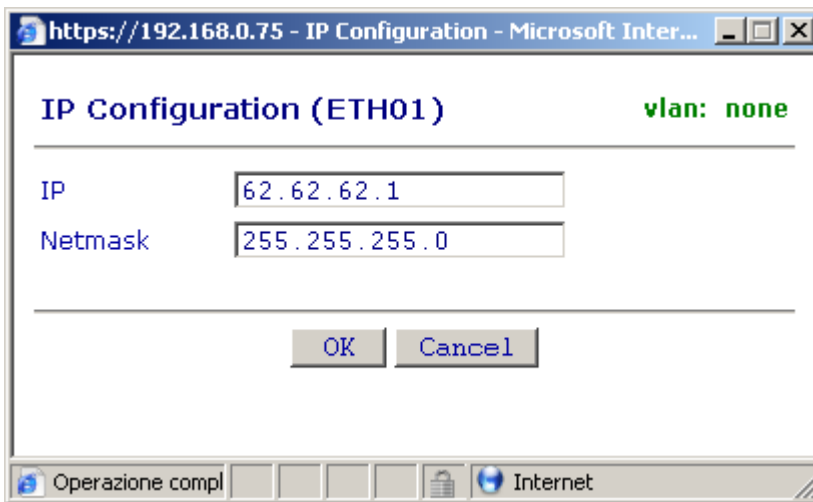


The screenshot shows a web browser window titled "https://192.168.0.75 - Create DB - Microsoft Internet Explorer". The main content is a form titled "Maxtor 31024H1 (hdb)" with the subtitle "New Database on partition hdb3". There are "Create" and "Close" buttons. The form has several input fields: "Description" (my cfg), "Hostname (FQDN)" (zeroshell.dominio.lan), "Kerberos 5 Realm" (DOMINIO.LAN), "LDAP Base" (dc=dominio,dc=lan), "Admin password" (masked with dots), and "Confirm password" (masked with dots). Below these is a section titled "NETWORK CONFIG" with a dropdown menu for "Ethernet Interface" (ETH00 - 3Com Corporation 3c905C-TX/TX-M [Tomado] (rev 78)), and input fields for "IP Address / Netmask" (192.168.0.75 / 255.255.255.0) and "Default Gateway". The browser's status bar at the bottom shows "Operazione completata" and "Internet".

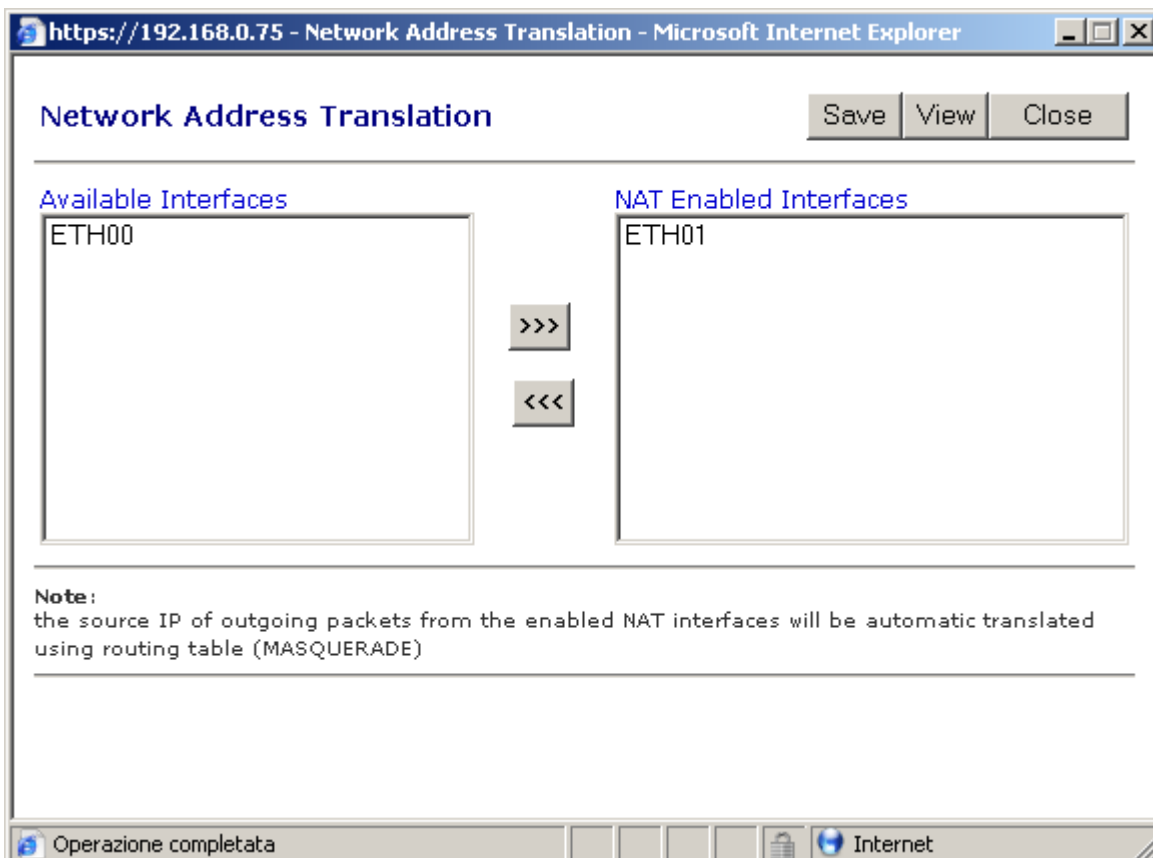
- 4 – Enabling the database configuration

5 – Set ip address on external interface:

SiteA:



6 – In Router menu, choose NAT and set Network Address Translation as follow:



Preparing certificate:

Create the Firewall certificate:

In menu "X509 CA", click "SETUP":

The screenshot shows the ZeroShell X509 Certification Authority Setup page. The browser window title is "25:192.168.0.75 - Microsoft Internet Explorer". The page header includes "ZEROSHELL Net Services" and "Release 1.0.beta4". The main content area is titled "X509 CERTIFICATION AUTHORITY" and has tabs for "List", "Manage", "CRL", "Imported", "Trusted CAs", and "Setup". The "Setup" tab is active, showing a form for "CA Certificate and Private Key".

The form fields are as follows:

- Common Name: my CA
- Key Size: 1024 bits
- Validity (Days): 3650
- Country Name: IT
- State or Province:
- Locality:
- Organization: dominio.lan
- Organizational Unit:
- E-Mail Address: info@dominio.lan
- CA Default Parameters: Key Size 1024 bits, Certificate Validity (days) 365

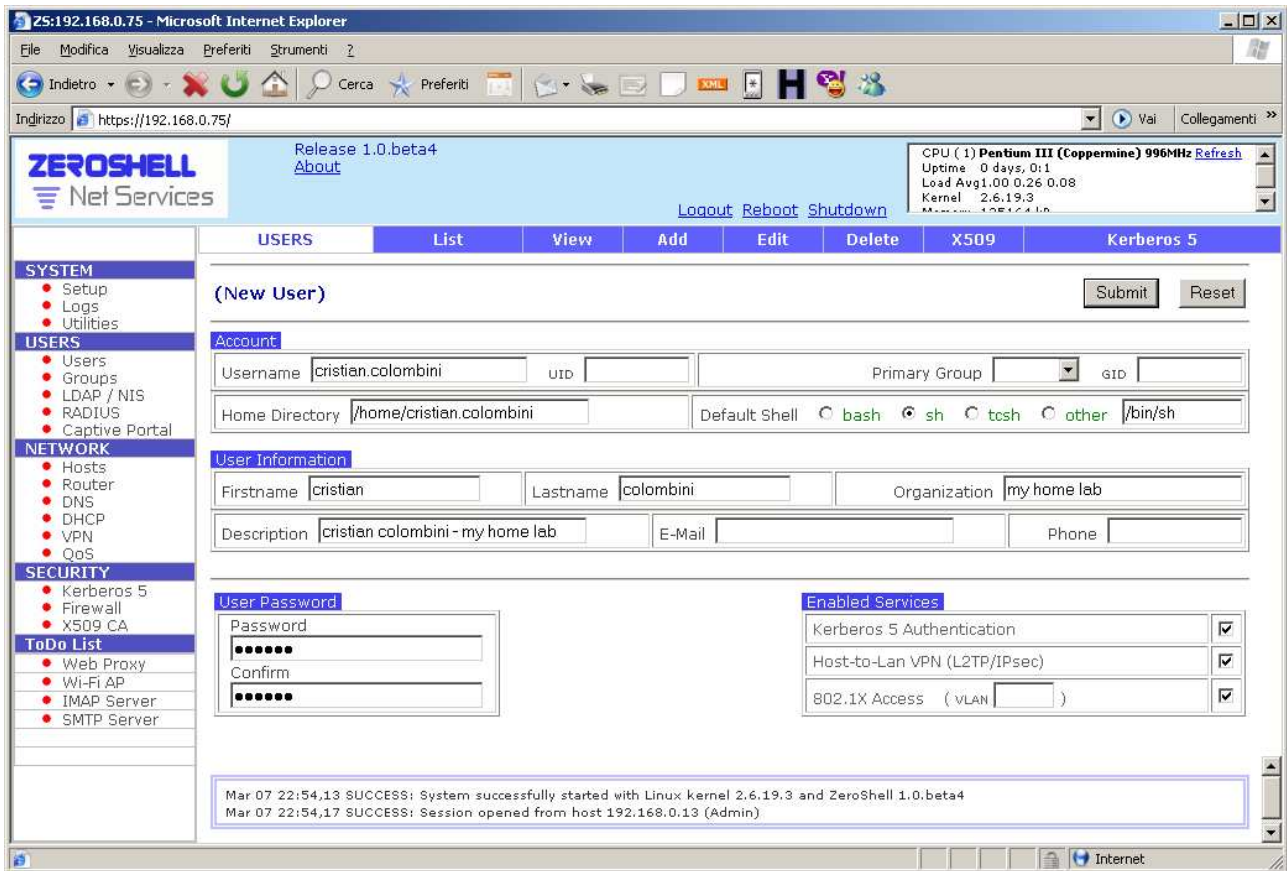
Buttons include "Generate", "Export", "Import", "Stoglia...", and "Apply". A status indicator shows "Status: OK". A log window at the bottom displays the following messages:

```
Mar 07 22:54.13 SUCCESS: System successfully started with Linux kernel 2.6.19.3 and ZeroShell 1.0.beta4
Mar 07 22:54.17 SUCCESS: Session opened from host 192.168.0.13 (Admin)
```

Fill up the fields and GENERATE the certificate.

Creating users and hosts:

Now we create users and host that will be allowed to connect using VPN. In USERS click ADD:



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 page title is "ZEROSHELL Net Services" and the version is "Release 1.0.beta4". 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), SECURITY (Kerberos 5, Firewall, X509 CA), and ToDo List (Web Proxy, Wi-Fi AP, IMAP Server, SMTP Server). The main content area is titled "USERS" and has tabs for "List", "View", "Add", "Edit", "Delete", "X509", and "Kerberos 5". The "Add" tab is active, showing a "New User" form. The form has several sections: "Account" with fields for Username (cristian.colombini), UID, Primary Group, and GID; Home Directory (/home/cristian.colombini) and Default Shell (sh); "User Information" with fields for Firstname (cristian), Lastname (colombini), Organization (my home lab), Description (cristian colombini - my home lab), E-Mail, and Phone; "User Password" with Password and Confirm fields; and "Enabled Services" with checkboxes for Kerberos 5 Authentication, Host-to-Lan VPN (L2TP/IPsec), and 802.1X Access (VLAN). A status bar at the bottom shows system logs: "Mar 07 22:54,13 SUCCESS: System successfully started with Linux kernel 2.6.19.3 and ZeroShell 1.0.beta4" and "Mar 07 22:54,17 SUCCESS: Session opened from host 192.168.0.13 (Admin)".

Fill up the fields setting up a strong password (es: %RF45£"Se) ..this also is security. Be sure to flag Host-to-Lan VPN (L2TP/Ipsec); this will let user to establish a secure connection.

Now choose HOSTS e click ADD:

25:192.168.0.75 - Microsoft Internet Explorer

File Modifica Visualizza Preferiti Strumenti ?

Indietro Cerca Preferiti

Inirizzo https://192.168.0.75/ Vai Collegamenti >>

ZEROSHELL Release 1.0.beta4
Net Services About Logout Reboot Shutdown

CPU (1) Pentium III (Coppermine) 996MHz Refresh
Uptime: 0 days, 0:4
Load Avg: 0.03 0.12 0.06
Kernel: 2.6.19.3

HOSTS	List	View	Add	Edit	Delete	X509	Kerberos 5
-------	------	------	-----	------	--------	------	------------

SYSTEM

- Setup
- Logs
- Utilities

USERS

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

NETWORK

- Hosts
- Router
- DNS
- DHCP
- VPN
- QoS

SECURITY

- Kerberos 5
- Firewall
- X509 CA

ToDo List

- Web Proxy
- Wi-Fi AP
- IMAP Server
- SMTP Server

Hostname: CrisMobile
Domain: dominio.lan
Description: my mobile pc
Administrator's E-Mail: ?

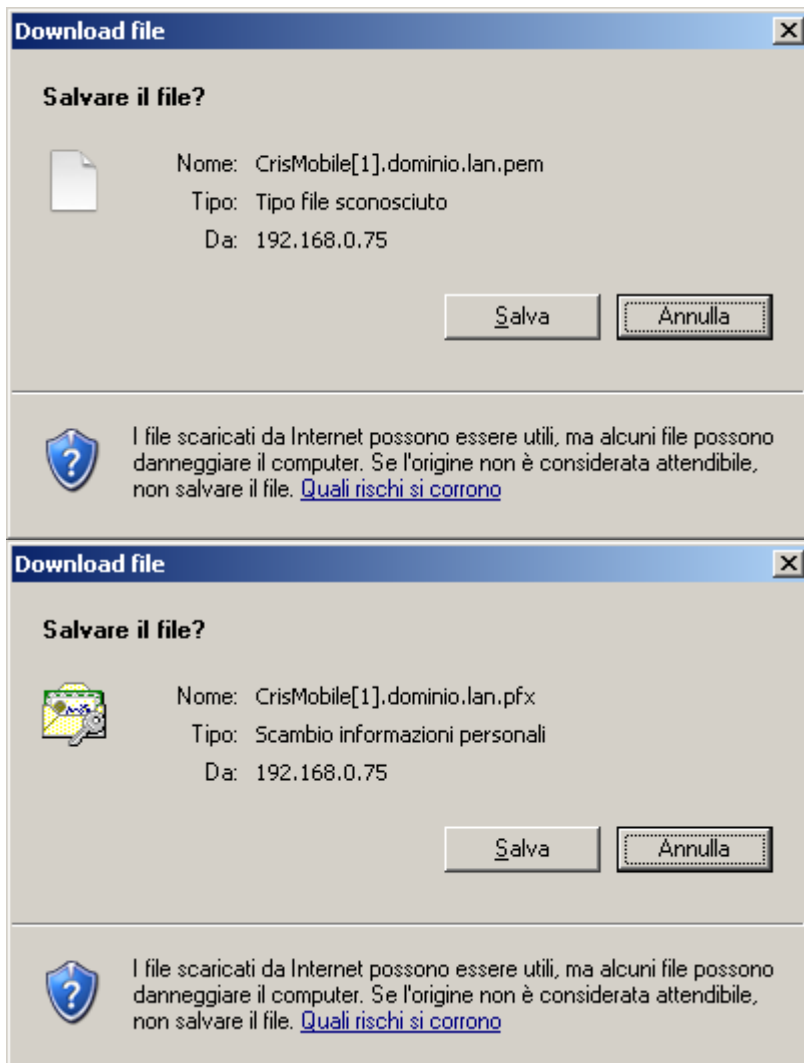
Kerberos 5 Authentication: Enabled Disabled

```
Mar 08 22:24,49 SUCCESS: Private key and X.509 certificate successfully generated for CrisMobile.dominio.lan (host)
Mar 08 22:24,49 SUCCESS: adding new entry "cn=CrisMobile.dominio.lan,ou=Computers,dc=dominio,dc=lan"
```

Operazione completata Internet

Exporting the certificates for the remote host

While creating the host CisMobile.dominio.lan the firewall create a certificate file for this host. Using EXPORT button we have to save in PEM and in PKCS#12 (PFX):



Creating VPN Tunnel

Click on VPN in the left frame and check that **L2TP over IPsec with X.509 IKE and MSCHAPv2 client authentication** is ENALED:

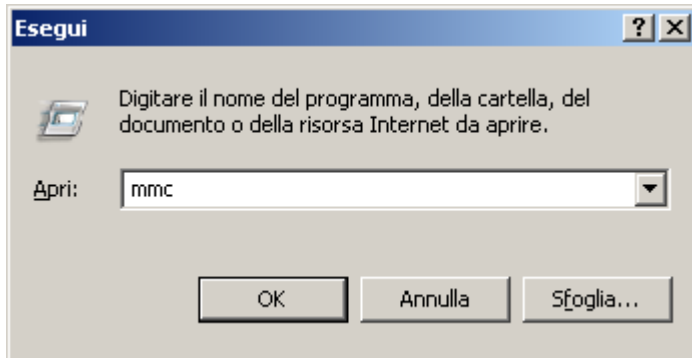
The screenshot shows the Zeroshell Net Services web interface in Microsoft Internet Explorer. The browser address bar shows `https://192.168.0.75/`. The interface has a left sidebar with a navigation menu containing categories like SYSTEM, USERS, NETWORK, SECURITY, and a To Do List. The main content area is titled "VPN" and shows the configuration for "L2TP over IPsec with X.509 IKE and MSCHAPv2 client authentication". The status is "ACTIVE" and "Enabled". The "IPsec IKE Configuration" section shows "X.509 Host Certificate" set to "Local CA" and "OU=Hosts, CN=zeroshell.dominio.lan". The "Client IP Address Assignment" section shows a range from "10.10.10.1" to "10.10.10.250". The "Routing Method" is set to "Source NAT". A "Some Notes" section explains that this VPN type combines L2TP and IPsec. A log window at the bottom shows successful operations: "adding new entry" and "deleting entry".

Now we have to set a new network addressing that will be used in the tunnel. It is important to use here a network addressing never used before in our networks. Of course we have to use private network addressing. I have set that the remote clients connecting in Vpn will be assigned addresses from 10.10.10.1 to 10.10.10.250.

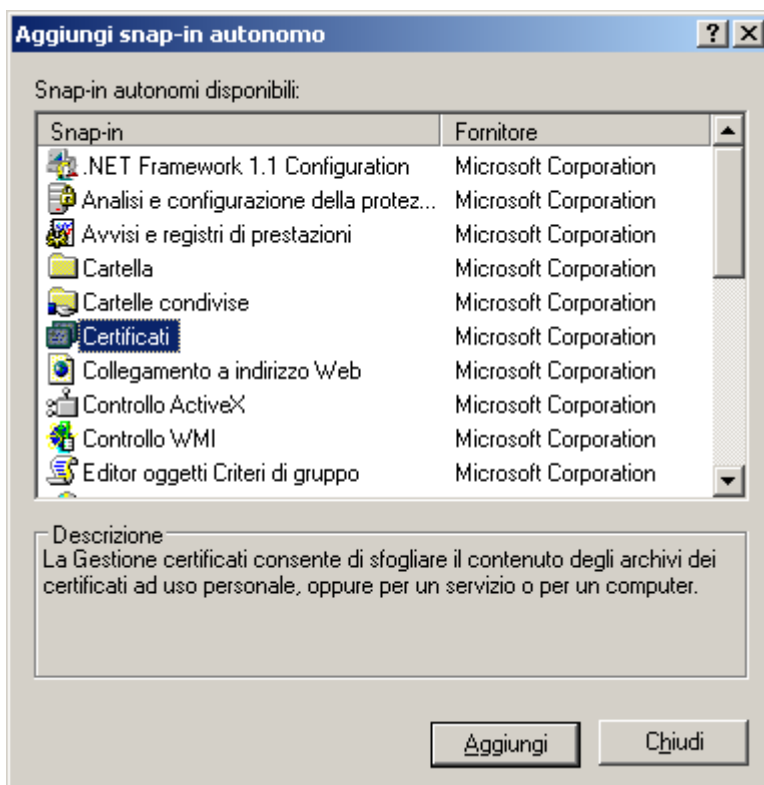
Microsoft client configuration:

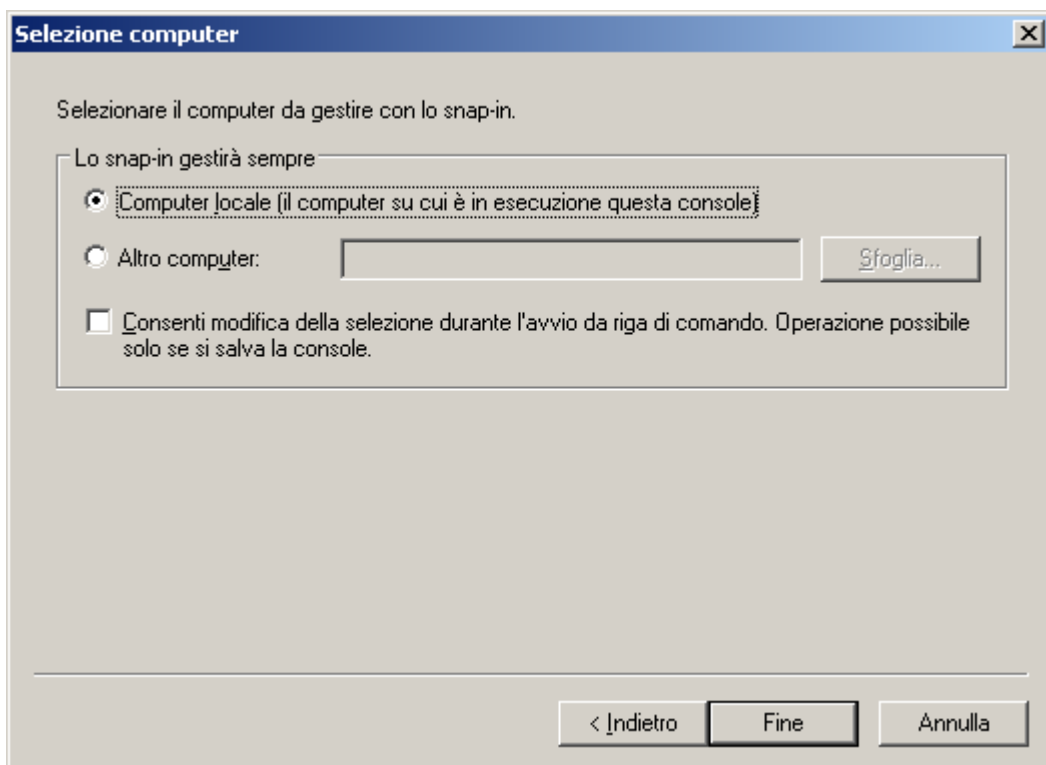
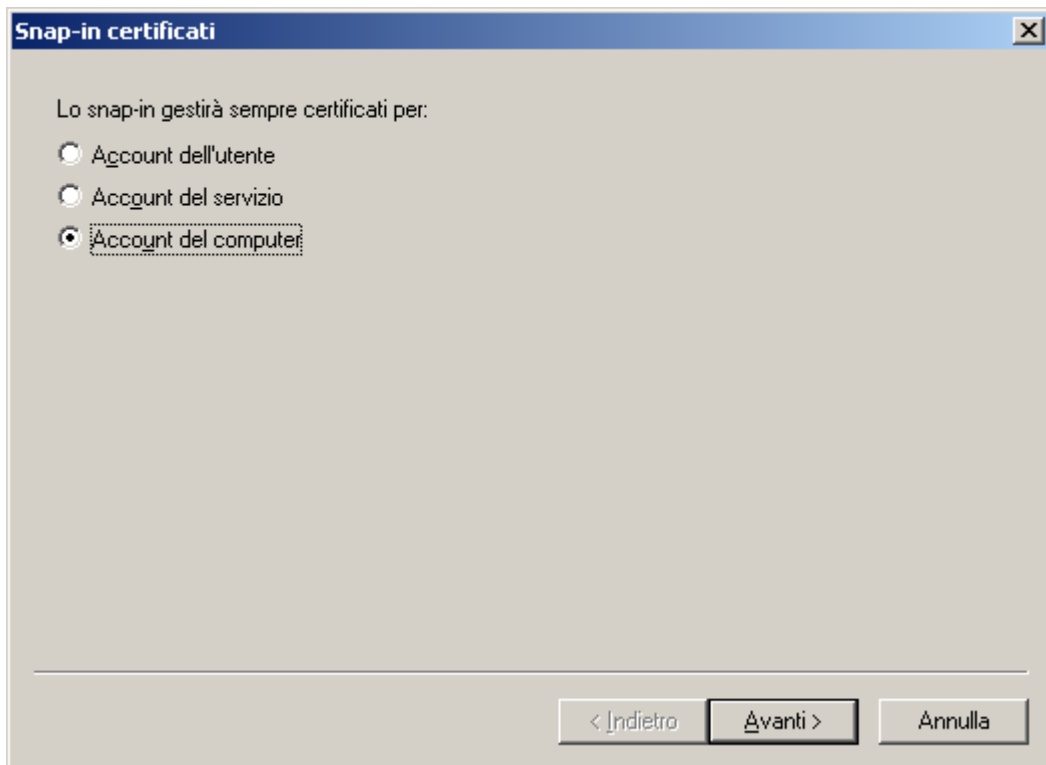
Now we are ready to configure the VPN host. I have a Ms Windows Xp Prof...
Import the caertificate:

Open Ms Management Console in Run :



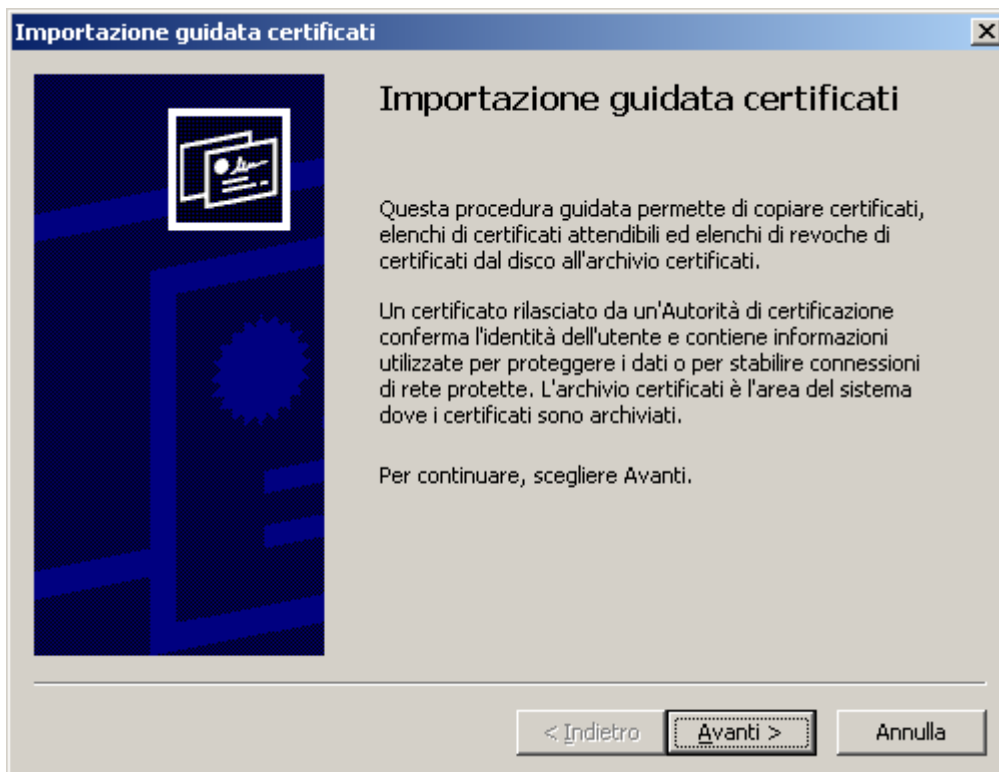
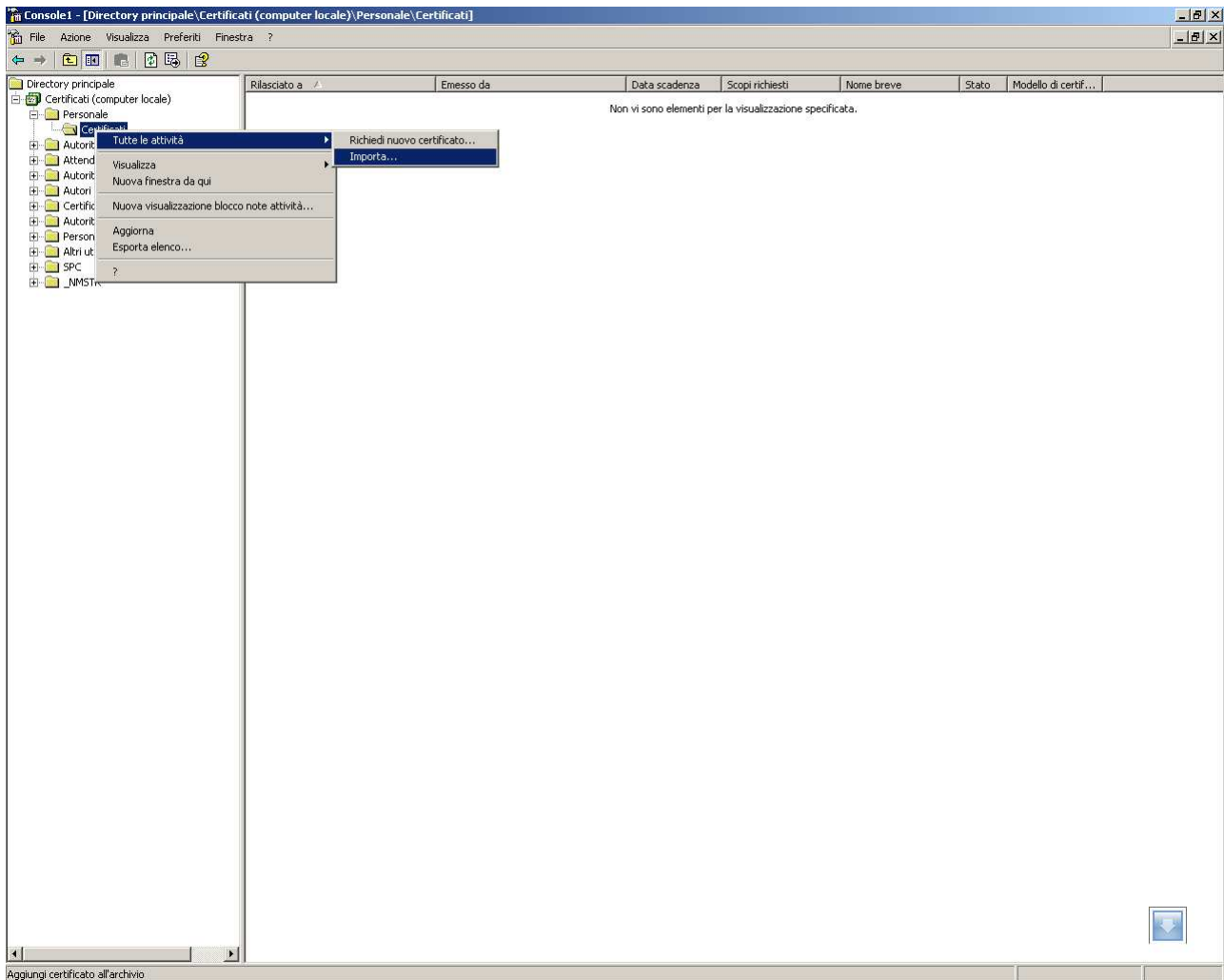
In the console open menu FILE → ADD Snap-in
choose ADD → Certificates

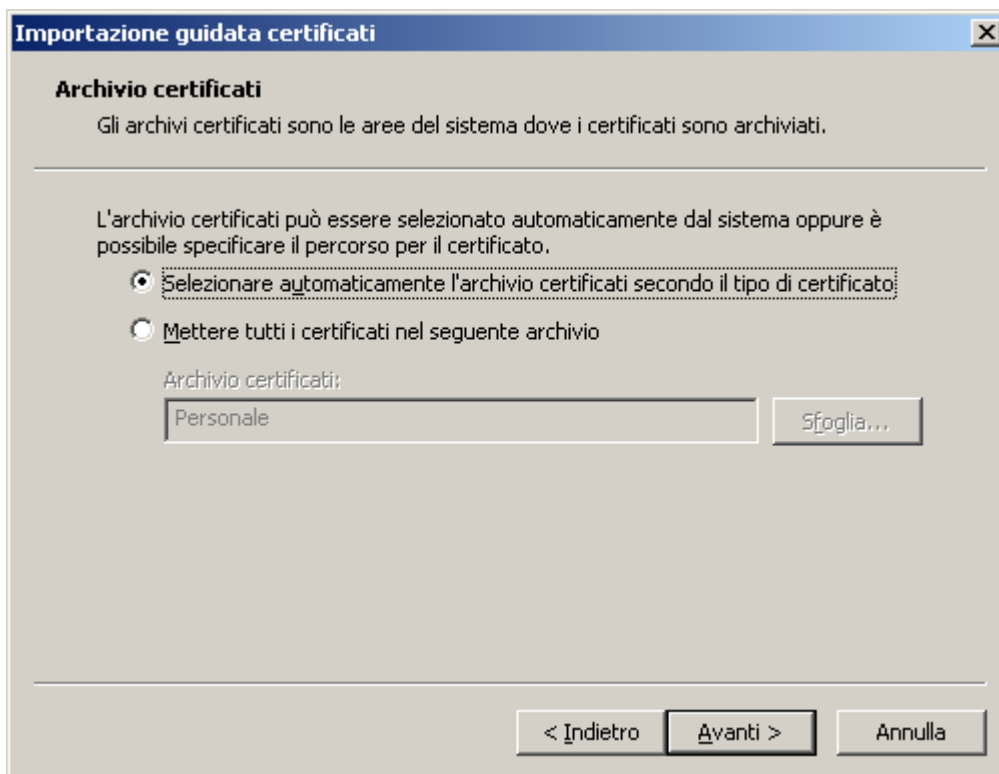
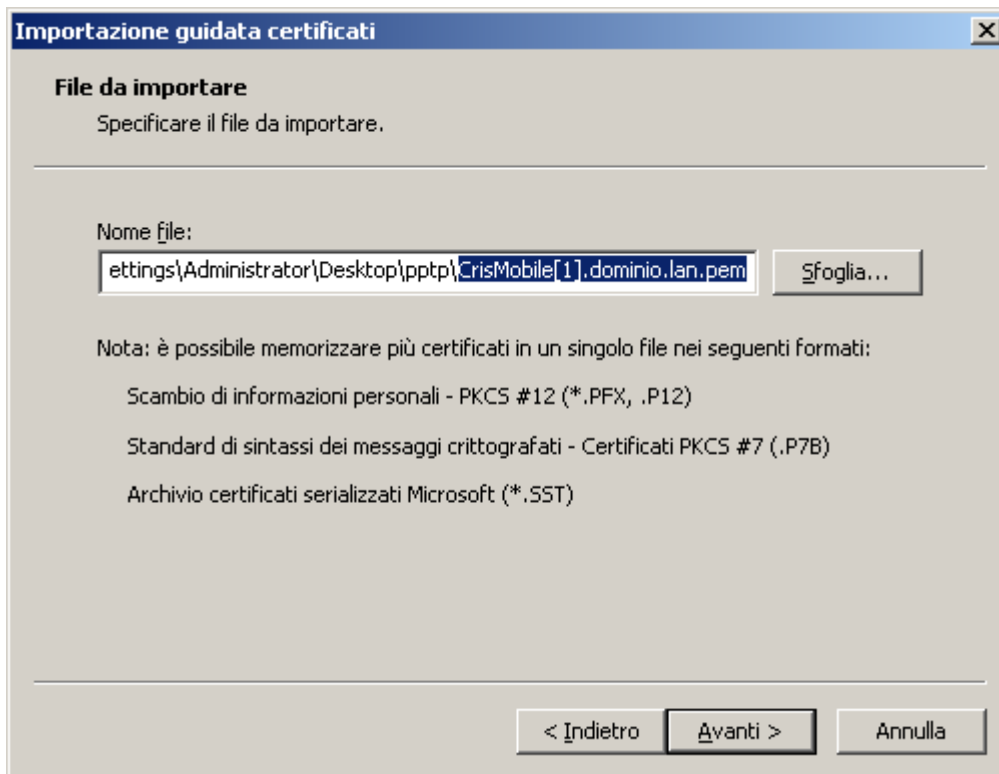




ok.

Right click on PERSONAL – CERTIFICATES choose IMPORT:





We do the same with PKCS#12 (PFX):

Importazione guidata certificati

File da importare

Specificare il file da importare.

Nome file:

ettings\Administrator\Desktop\pftp\CrisMobile[1].dominio.lan.pfx

Sfogli...

Nota: è possibile memorizzare più certificati in un singolo file nei seguenti formati:

Scambio di informazioni personali - PKCS #12 (*.PFX, .P12)

Standard di sintassi dei messaggi crittografati - Certificati PKCS #7 (.P7B)

Archivio certificati serializzati Microsoft (*.SST)

< Indietro

Avanti >

Annulla

Importazione guidata certificati

Password

Per motivi di sicurezza, la chiave privata è stata protetta da password.

Digitare la password della chiave privata.

Password:

Abilita protezione avanzata chiave privata. Attivando questa opzione si verrà avvisati ogni volta che si utilizzerà la chiave privata da un'applicazione.

Contrassegna questa chiave come esportabile. Questa opzione consente di eseguire il backup o di trasportare le chiavi in un secondo momento.

< Indietro

Avanti >

Annulla

Importazione guidata certificati



Archivio certificati

Gli archivi certificati sono le aree del sistema dove i certificati sono archiviati.

L'archivio certificati può essere selezionato automaticamente dal sistema oppure è possibile specificare il percorso per il certificato.

- Selezionare automaticamente l'archivio certificati secondo il tipo di certificato
- Mettere tutti i certificati nel seguente archivio:

Archivio certificati:

Personale

Sfogli...

< Indietro


Avanti >

Annulla

Now we have to create a new network connection:

Creazione guidata nuova connessione

Tipo di connessione di rete
Scegliere l'operazione da effettuare.




- Connessione a Internet**
Consente di connettere il computer a Internet e di esplorare il Web e leggere la posta elettronica.
- Connessione alla rete aziendale**
Consente di connettere il computer a una rete aziendale, mediante connessione remota o VPN e di lavorare da casa, da una filiale o da un'altra ubicazione.
- Installazione di una rete domestica o di una piccola rete aziendale**
Consente di connettere il computer a una rete domestica o a una piccola rete aziendale esistente o di installarne una nuova.
- Installazione di una connessione avanzata**
Consente di connettere il computer direttamente a un altro computer mediante la porta seriale, parallela o a infrarossi o di impostarlo per consentire la connessione di altri computer.

< Indietro Avanti > Annulla

Creazione guidata nuova connessione

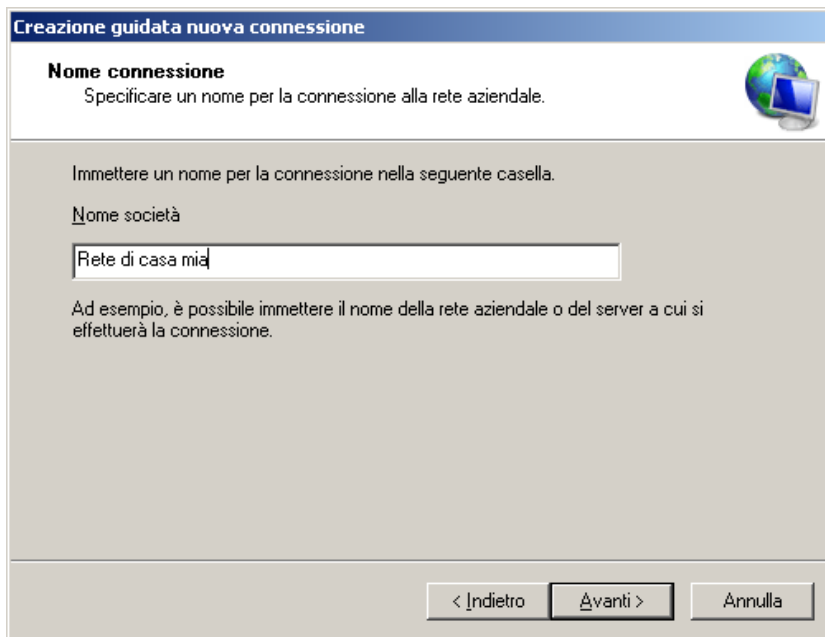
Connessione di rete
Scegliere la modalità di connessione alla rete aziendale.



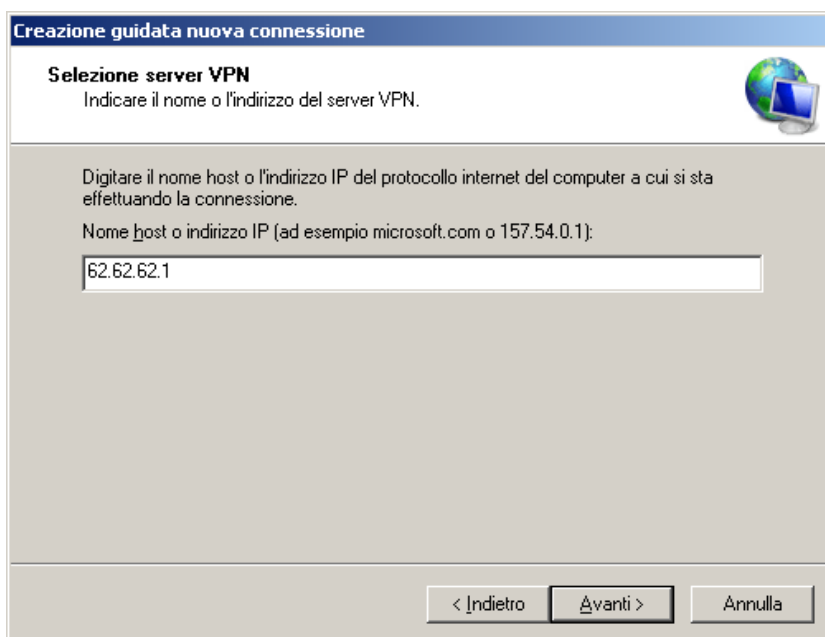
Crea la seguente connessione:

- Connessione remota**
Consente di connettere il computer alla rete mediante un modem e una normale linea telefonica oppure mediante una linea ISDN.
- Connessione VPN**
Consente di connettere il computer alla rete mediante una connessione VPN (Virtual Private Network) su Internet.

< Indietro Avanti > Annulla

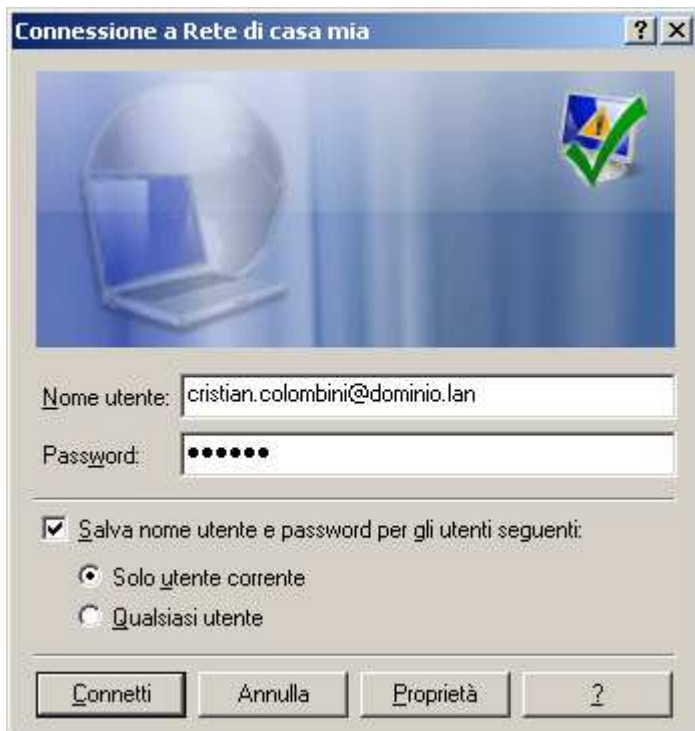


In the next image we have to set the endpoint of the tunnel (the external ip address of Zeroshell). If we have not static Ip address on Zeroshell external interface we can choose to use the free service of DynDns.org.

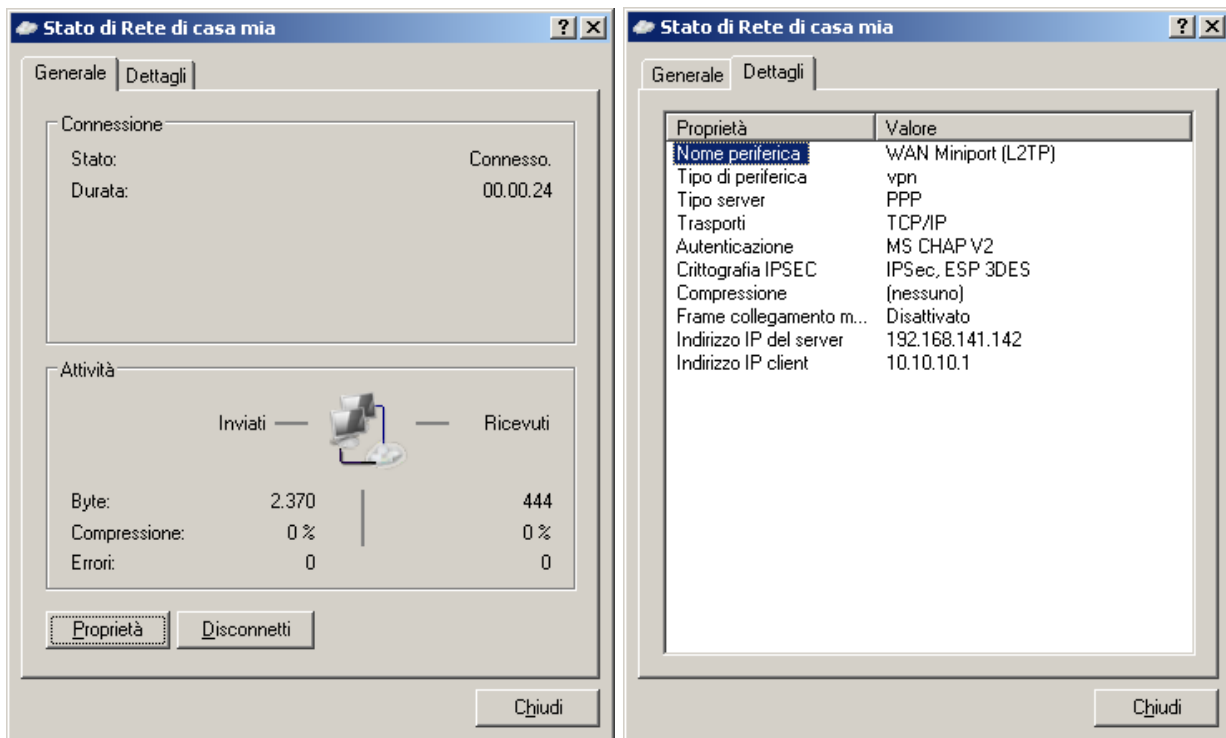


End

Now we fill up the following fields being carefull that they are case sensitive:



The username must be followed by the domain name at which it belongs to. (domain name configured in Zeroshell). Connect:



We can see the ip address assigned to our host connection by Zeroshell: 10.10.10.1. OK!!
Now we can check on the firewall in VPN click Show Clients and we can see :

22:14:25 Starting: 0 connections L2TP/IPsec dropped
22:44:36 Starting: 0 connections L2TP/IPsec dropped
22:54:07 Starting: 0 connections L2TP/IPsec dropped
22:54:32 User "cristian@dominio.lan" successfully authenticated (IP:
10.10.10.1)
23:17:56 User "cristian.colombini@dominio.lan" successfully authenticated (IP:
10.10.10.1)

Look at the Radius server logs:

22:44:36 Ready to process requests.
22:54:07 Ready to process requests.
23:17:56 Login OK: [cristian.colombini@dominio.lan] (from client localhost port
10)

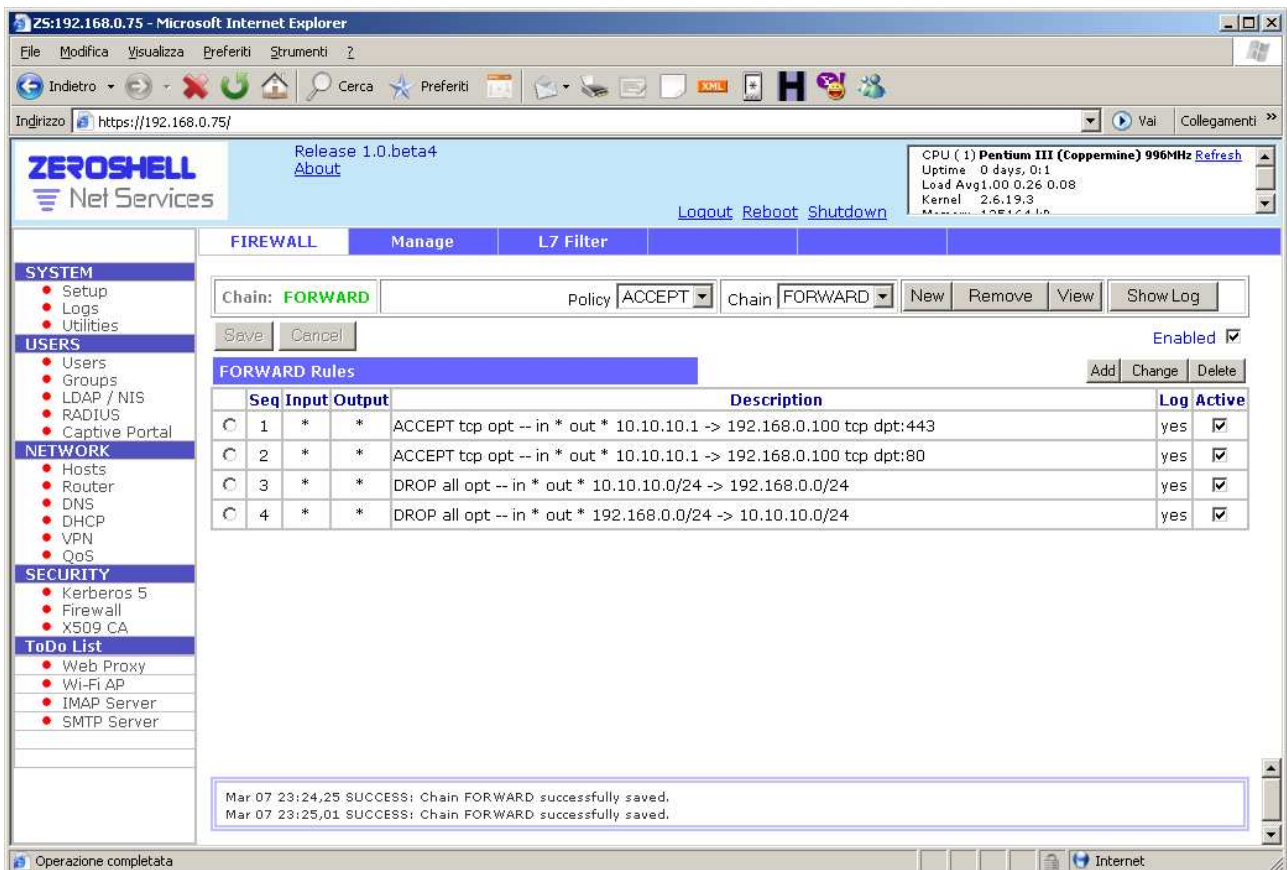
Communication policies

Now we can set what protocol ports must be open (or closed) in this VPN.

In the following image we can see that:

External host (10.10.10.1) can only browse an internal webserver (192.168.0.100) using 80 and 443 tcp ports (http and https).

Nothing else will pass through the VPN (see last 2 DROP lines):



The screenshot shows the ZeroShell Firewall configuration interface. The main window displays the 'FORWARD Rules' configuration for the 'FORWARD' chain. The rules are as follows:

Seq	Input	Output	Description	Log	Active
1	*	*	ACCEPT tcp opt -- in * out * 10.10.10.1 -> 192.168.0.100 tcp dpt:443	yes	<input checked="" type="checkbox"/>
2	*	*	ACCEPT tcp opt -- in * out * 10.10.10.1 -> 192.168.0.100 tcp dpt:80	yes	<input checked="" type="checkbox"/>
3	*	*	DROP all opt -- in * out * 10.10.10.0/24 -> 192.168.0.0/24	yes	<input checked="" type="checkbox"/>
4	*	*	DROP all opt -- in * out * 192.168.0.0/24 -> 10.10.10.0/24	yes	<input checked="" type="checkbox"/>

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

```
Mar 07 23:24,25 SUCCESS: Chain FORWARD successfully saved.  
Mar 07 23:25,01 SUCCESS: Chain FORWARD successfully saved.
```

These policies are read from high to low ... in the last lines everything else (that is not matched in the first two lines) is DROPPED between 10.10.10.0/24 → 192.168.0.0/24 and between 192.168.0.0/24 → 10.10.10.0/24.