

## Zeroshell: VPN Host-to-Lan



Il sistema operativo multifunzionale  
creato da [Fulvio.Ricciardi@zeroshell.net](mailto:Fulvio.Ricciardi@zeroshell.net)  
[www.zeroshell.net](http://www.zeroshell.net)

Assicurare la comunicazione fra un host ed una rete

( Autore: [cristiancolombini@libero.it](mailto:cristiancolombini@libero.it) )

Assicurare la comunicazione fra un host ed una rete:

Questa breve guida pratica ci consentirà di attivare un Tunnel VPN fra un host ed una sede collegata ad internet. Questo tipo di comunicazione garantisce sicurezza nello scambio di informazioni fra le i due oggetti tramite certificato. Sarà poi possibile scrivere le politiche di comunicazione fra l'host e la rete interna della sede e viceversa.

Ecco di seguito i passi da seguire :

**Schema logico della soluzione**

**Preparazione del firewall**

**Preparazione del certificato del firewall**

**Preparazione degli utenti, degli hosts**

**Esportazione dei certificati per i clients**

**Creazione del tunnel vpn su client ms windows**

**Filtri di sicurezza sul tunnel**

## **Schema logico della soluzione:**

Prima di cominciare è opportuno avere le idee chiare su ciò che si sta per fare: avendo connessa ad internet con ip pubblici statici è possibile creare una relazione ( tunnel vpn ) di comunicazione verso di essa con un host collegato ad internet in modo che avvenga uno scambio di dati sicuro.

L'esempio che andrò ad implementare è stato eseguito in laboratorio; solo per questo motivo gli ip pubblici sulla interfaccia esterna del firewall e dell'host appartengono alla stessa sottorete. Nella realtà solo la sede avrà ip pubblici statici, il client nella maggior parte dei casi avrà un ip dinamico fornito da un provider. Il router della sede dovrà essere privo di nat dinamico per permettere al mondo esterno di raggiungere l'ip pubblico sulla interfaccia di rete esterna del suo firewall.

Nell'immagine seguente vediamo gli indirizzamenti delle reti private:

SiteA:

rete privata: 192.168.0.0/24

ip pubblico del firewall: 62.62.62.1

Host:

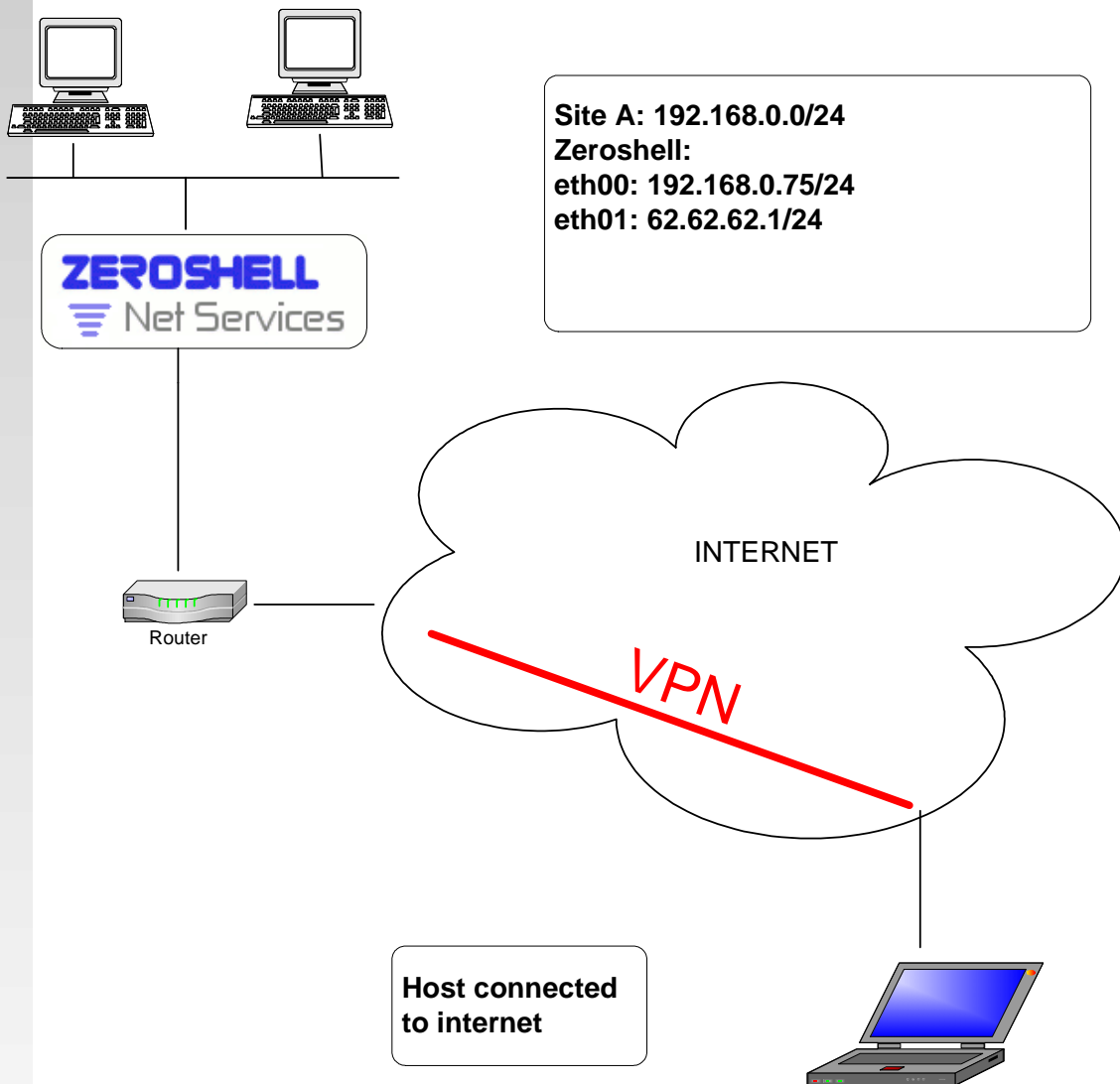
ip dinamico ( in questo caso di laboratorio 62.62.62.2 )

Il tunnel VPN rappresentato col colore rosso ( nell'immagine seguente) connette l'host al firewall in modo esclusivo e un tramite certificato.

Una volta stabilita la relazione sicura fra l'host ed il firewall, potremo stabilire cosa realmente dovrà passare in questo Tunnel.

# VPN con Zeroshell

Mercoledì 7 Marzo 2007

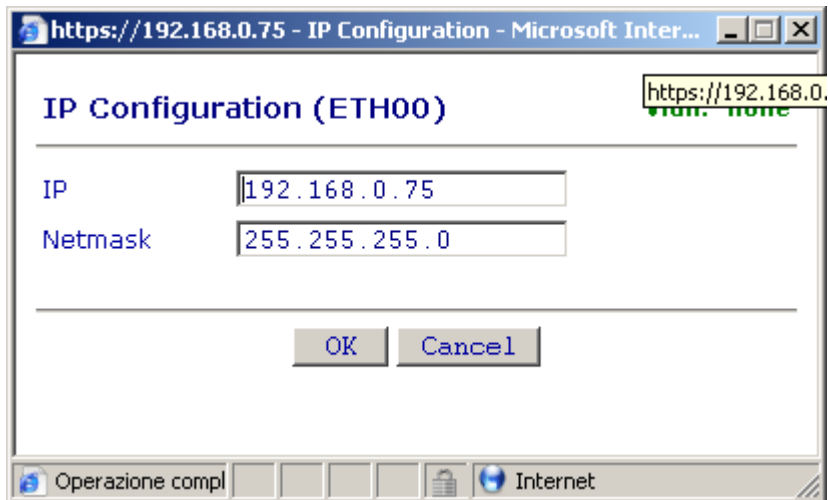


## Preparazione dei firewall

Facendo riferimento alla guida “Proteggere una piccola rete con stile” già presente fra la documentazione nel sito ufficiale [www.zeroshell.net](http://www.zeroshell.net), è facile preparare la configurazione base dei due firewall:

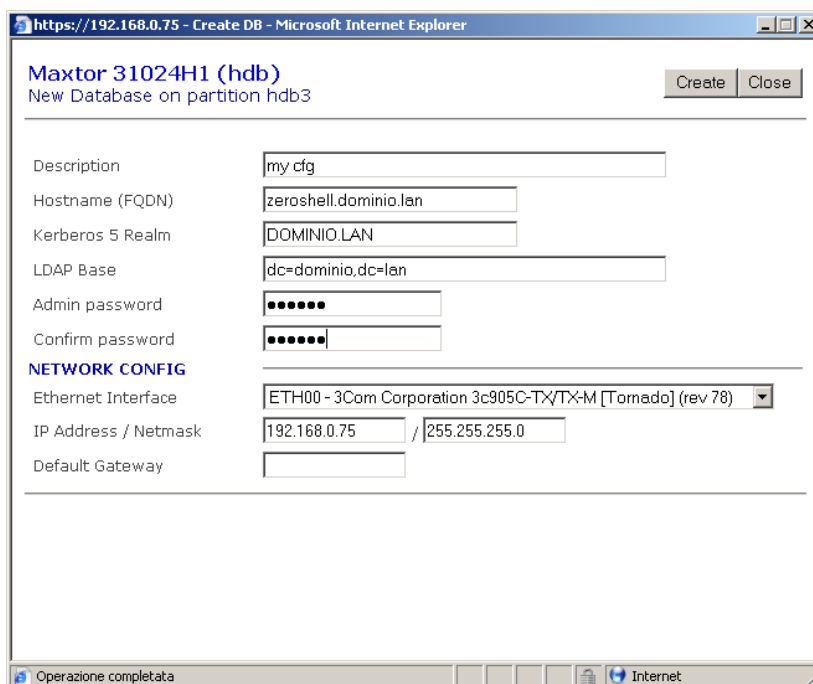
- 1 – primo accesso al firewall
- 2 – impostazione dell’indirizzo ip sulla scheda di rete interna:

SiteA:



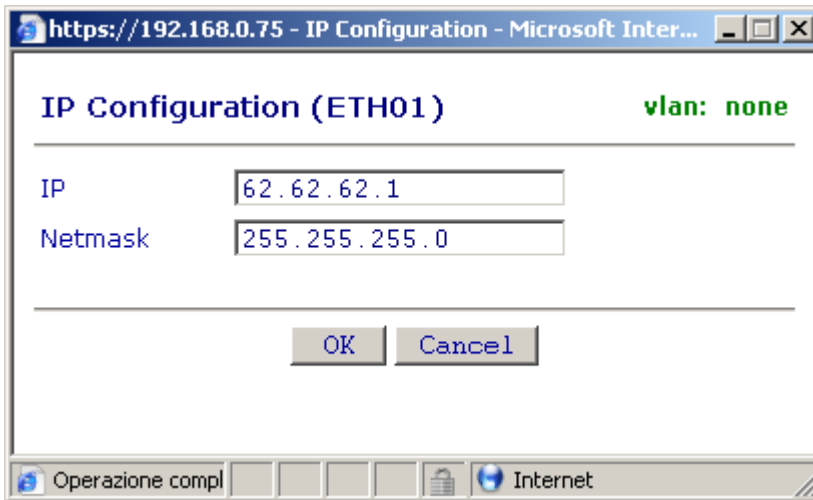
- 3 – Creare un database di configurazione:

SiteA:

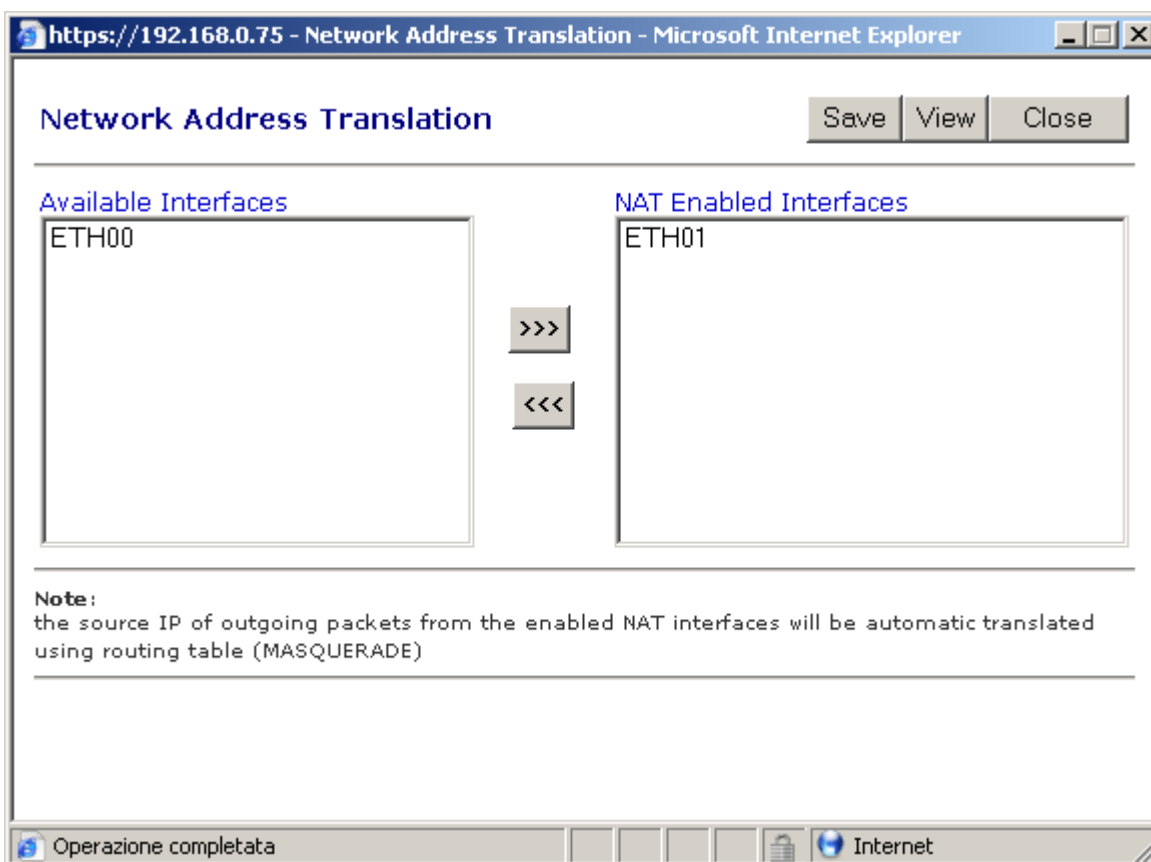


- 4 – Attivare sul firewall il database ed attendere il riavvio del sistema
- 5 – Impostare l' indirizzo ip sulla scheda di rete esterna:

SiteA:



- 6 – Nel Router, alla voce NAT spostiamo la ETH01 in modo che vada a mascherare la nostra rete sulla ETH00:



## Preparazione del certificato del firewall:

Creare il certificato del firewall:

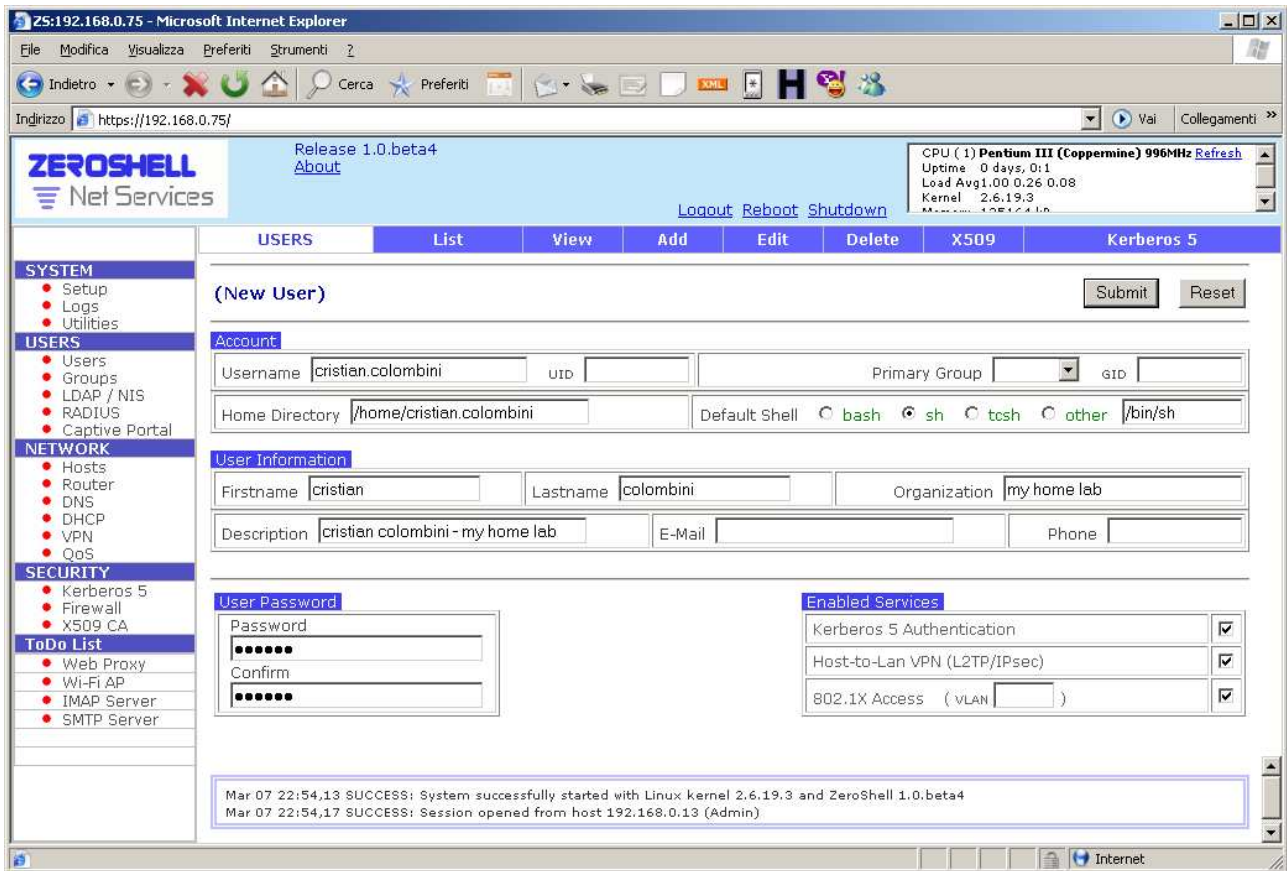
Nel menu “X509 CA”, portarsi alla voce “SETUP”:

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 the "CA Certificate and Private Key" configuration page. The page contains several form fields for setting up the CA, including "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), and "CA Default Parameters" (Key Size: 1024 bits, Certificate Validity: 365). There are buttons for "Generate", "Export", "Import", and "Apply". A status indicator shows "Status: OK". The bottom of the page displays 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)". The browser status bar at the bottom shows "Operazione completata" and "Internet".

Compilare i campi e cliccando su “GENERATE” procedere con la creazione del certificato.

## Preparazione degli utenti e degli hosts:

Creiamo le utenze e gli hosts di chi si dovrà collegare in VPN. Recarsi al menu USERS e cliccare su ADD:



The screenshot shows the ZeroShell 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 selected). "User Information" includes fields for Firstname (cristian), Lastname (colombini), Organization (my home lab), Description (cristian colombini - my home lab), E-Mail, and Phone. "User Password" has fields for Password and Confirm. "Enabled Services" includes 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)".

Riempire i campi tenendo presente che è sempre meglio usare una password strong ( per esempio: %RF45£”Se ) ..anche questo fa parte della sicurezza..no? Accertarsi che sia flaggata la voce Host-to-Lan VPN (L2TP/Ipsec).

Recarsi al menu HOSTS e cliccare su 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

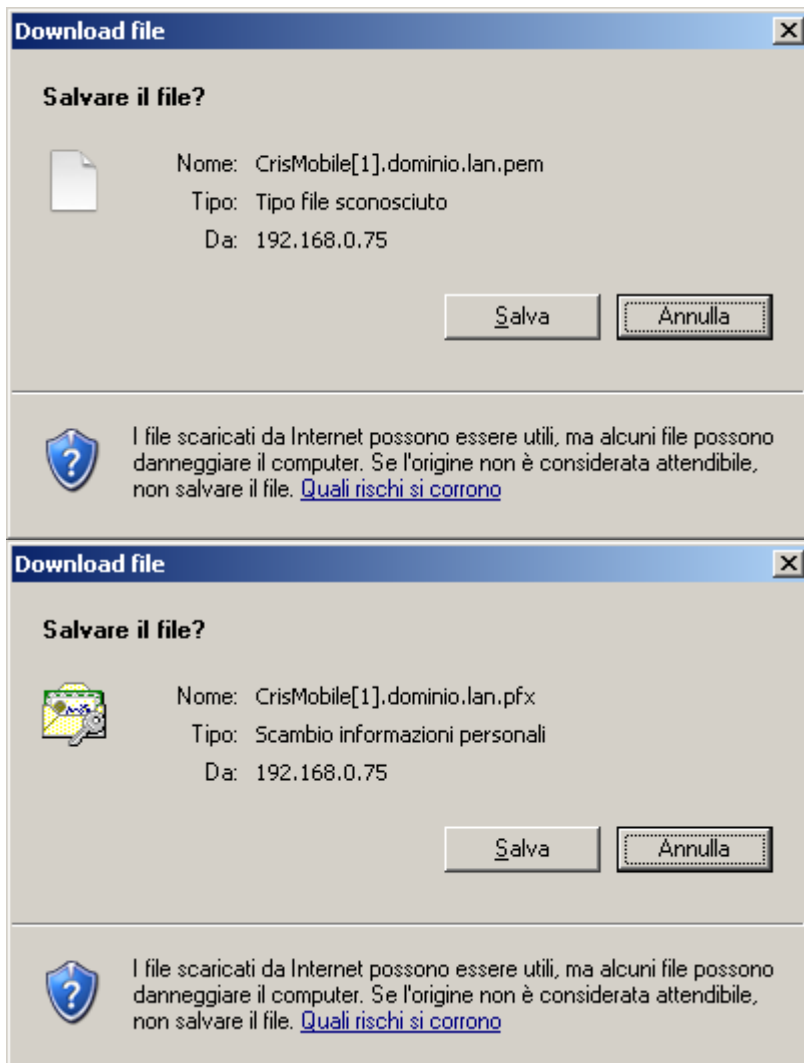
CPU (1) Pentium III (Coppermine) 996MHz Refresh  
 Uptime: 0 days, 0:4  
 Load Avg: 0.03 0.12 0.06  
 Kernel: 2.6.19-3  
 Memory: 125124 kb

HOSTS	List	View	Add	Edit	Delete	X509	Kerberos 5
<p><b>SYSTEM</b></p> <ul style="list-style-type: none"> <li>Setup</li> <li>Logs</li> <li>Utilities</li> </ul> <p><b>USERS</b></p> <ul style="list-style-type: none"> <li>Users</li> <li>Groups</li> <li>LDAP / NIS</li> <li>RADIUS</li> <li>Captive Portal</li> </ul> <p><b>NETWORK</b></p> <ul style="list-style-type: none"> <li>Hosts</li> <li>Router</li> <li>DNS</li> <li>DHCP</li> <li>VPN</li> <li>QoS</li> </ul> <p><b>SECURITY</b></p> <ul style="list-style-type: none"> <li>Kerberos 5</li> <li>Firewall</li> <li>X509 CA</li> </ul> <p><b>ToDo List</b></p> <ul style="list-style-type: none"> <li>Web Proxy</li> <li>Wi-Fi AP</li> <li>IMAP Server</li> <li>SMTP Server</li> </ul>							
<p><b>CrisMobile.dominio.lan</b></p> <p>Hostname: <input type="text" value="CrisMobile"/></p> <p>Domain: <input type="text" value="dominio.lan"/></p> <p>Description: <input type="text" value="my mobile pc"/></p> <p>Administrator's E-Mail: <input type="text" value="?"/></p> <p>Kerberos 5 Authentication: <input checked="" type="radio"/> Enabled <input type="radio"/> Disabled</p>							
<p>Mar 08 22:24,49 SUCCESS: Private key and X.509 certificate successfully generated for CrisMobile.dominio.lan (host)</p> <p>Mar 08 22:24,49 SUCCESS: adding new entry "cn=CrisMobile.dominio.lan,ou=Computers,dc=dominio,dc=lan"</p>							

Operazione completata Internet

## Esportazione dei certificati per i clients

Subito per questo host viene generato il relativo certificato. Abbiamo cura di esportarli tramite il tasto EXPORT in PEM ed in PKCS#12 (PFX):



## Creazione del tunnel vpn

Recarsi al menu VPN e verificare che **L2TP over IPsec with X.509 IKE and MSCHAPv2 client authentication** sia attivato:

The screenshot displays the Zeroshell Net Services web interface for configuring a VPN. The main configuration area is titled "L2TP over IPsec with X.509 IKE and MSCHAPv2 client authentication" and shows a status of "Connected: 0". The configuration is currently "ACTIVE" and "Enabled".

Key configuration sections include:

- IPsec IKE Configuration:** X.509 Host Certificate is set to "Local CA" and "OU=Hosts, CN=zeroshell.dominio.ian". The status is "OK".
- Client IP Address Assignment:** The IP range is set from "10.10.10.1" to "10.10.10.250".
- Routing Method:** Set to "Source NAT".

A log window at the bottom shows the following messages:

```
Mar 07 23:07,42 SUCCESS: adding new entry "uid=cristian.colombini,ou=People,dc=dominio,dc=lan"
Mar 07 23:07,54 SUCCESS: deleting entry "uid=cristian,ou=People,dc=dominio,dc=lan"
```

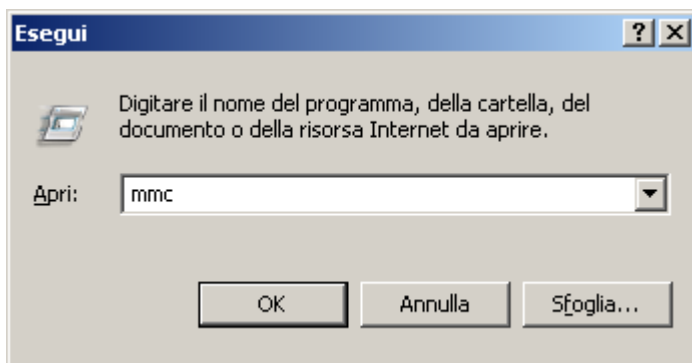
Verificare inoltre che gli ip assegnati appartengano ad una nuova rete non esistente nelle nostre ( nel mio caso gli hosts remoti che si conetteranno riceveranno gli ip dal 10.10.10.1 al 10.10.10.250).

## Creazione del tunnel vpn su client ms windows:

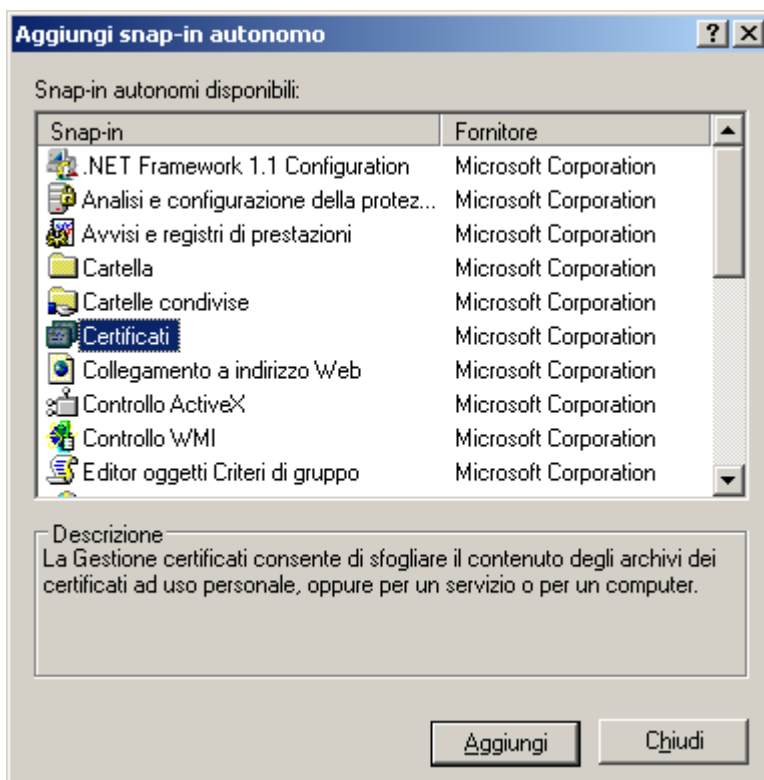
A questo punto possiamo configurare il client VPN sull'host. Nel mio caso si tratta di un sistema Ms Windows Xp Prof... ma il concetto vale per tutti i sistemi.

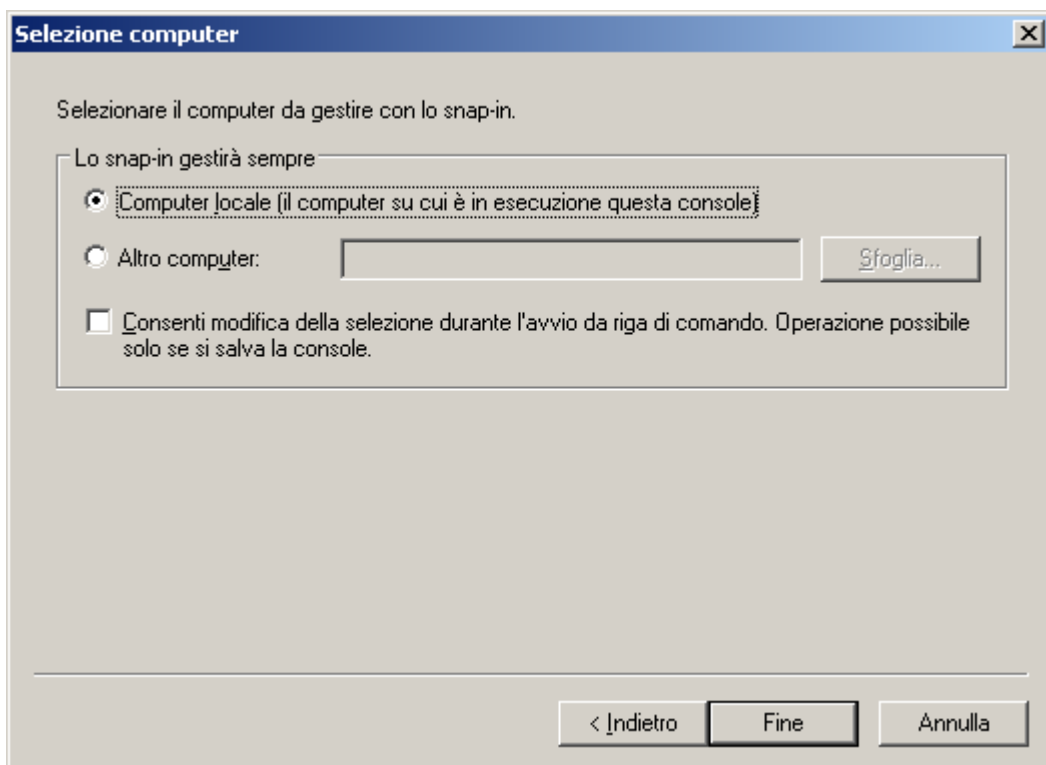
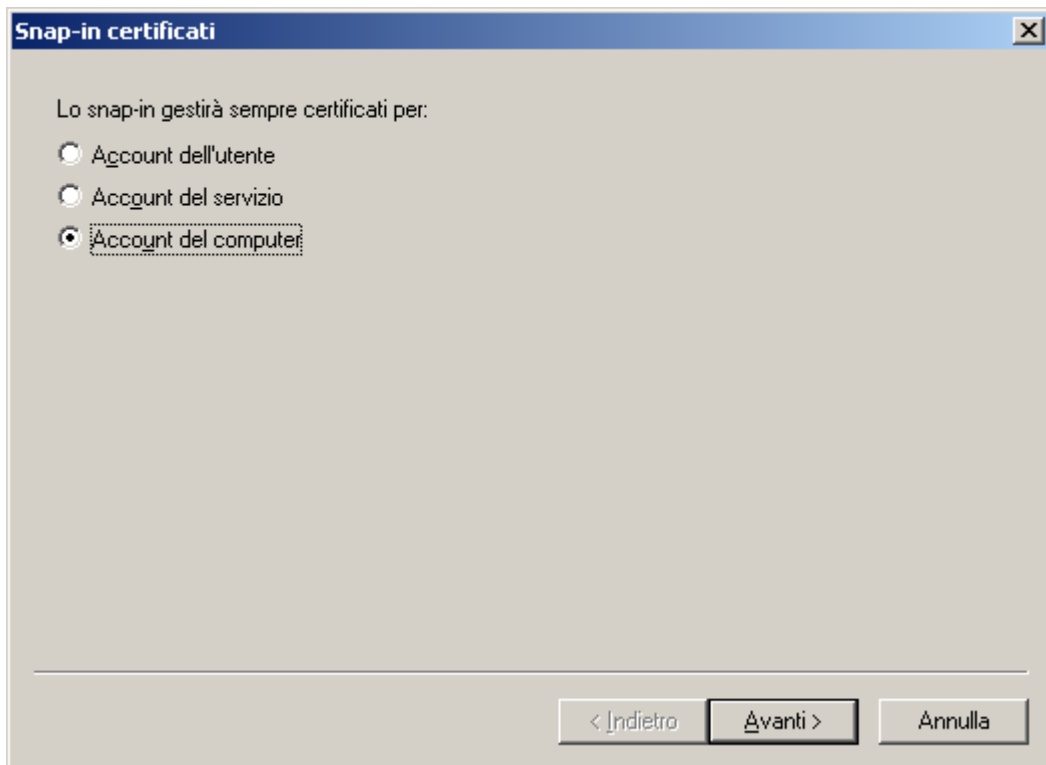
Importiamo il certificato che abbiamo salvato dal firewall:

apriamo la console di microsoft con "mmc":



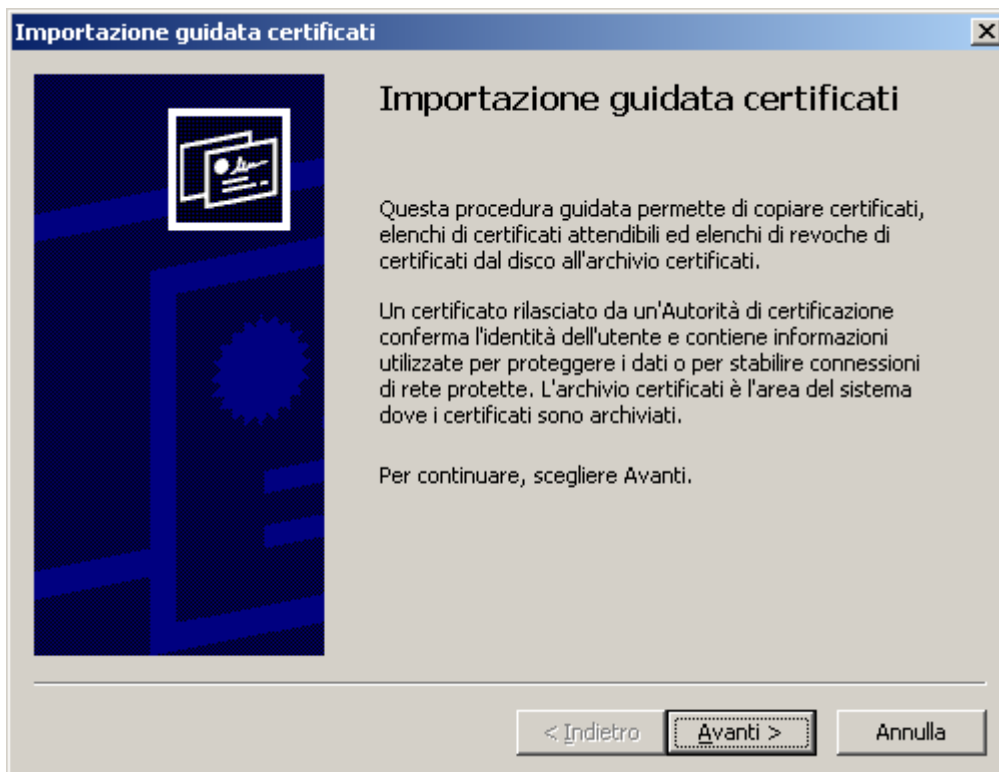
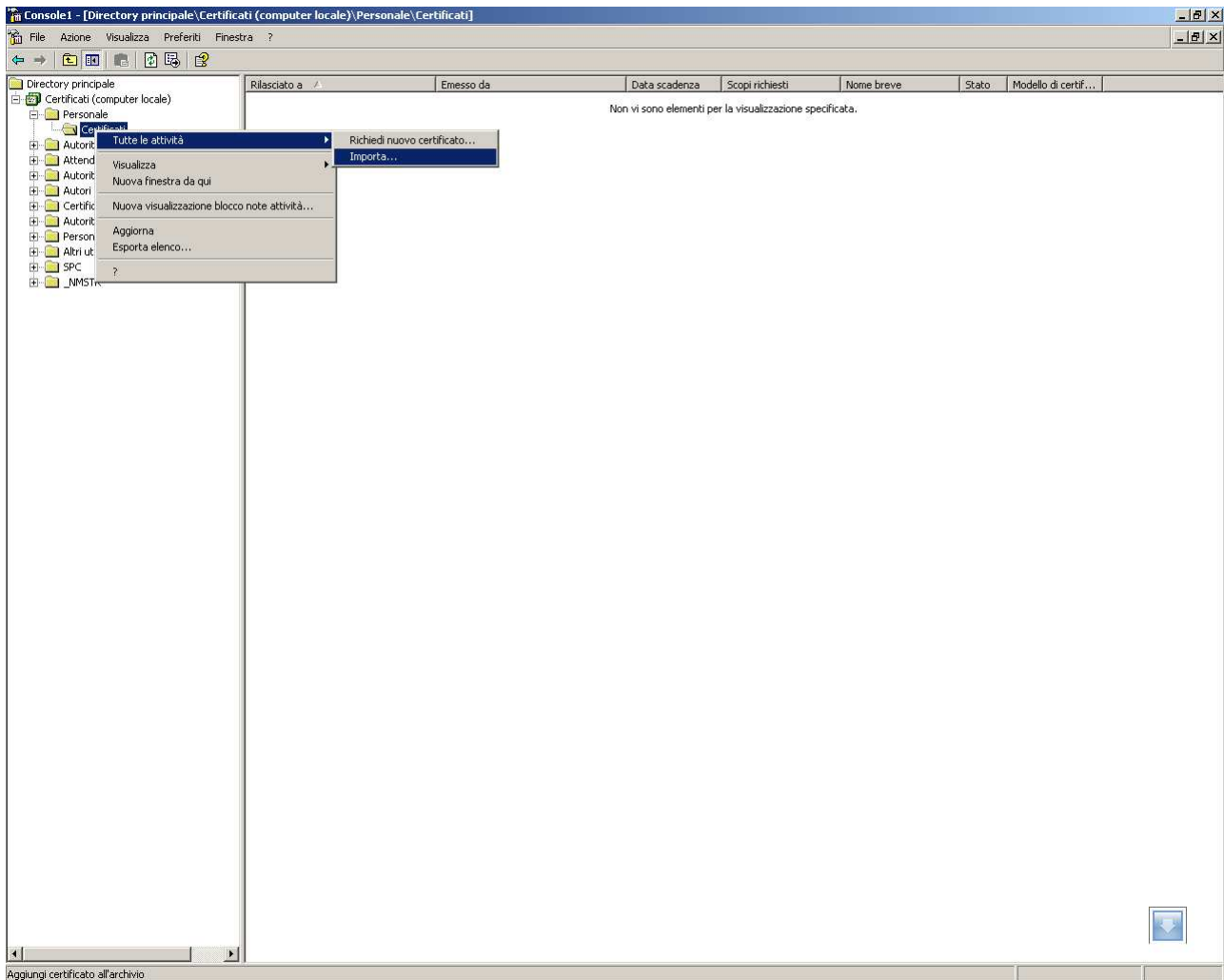
dal menu file → aggiungi Snap-in  
scegliere Aggiungi → Certificati

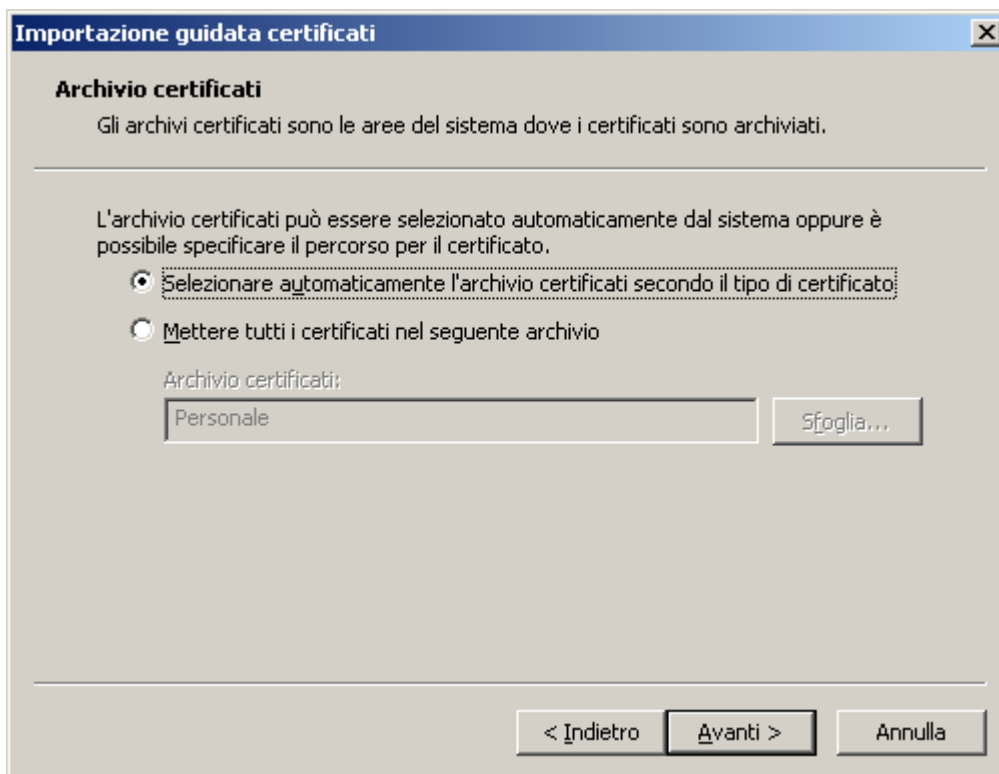
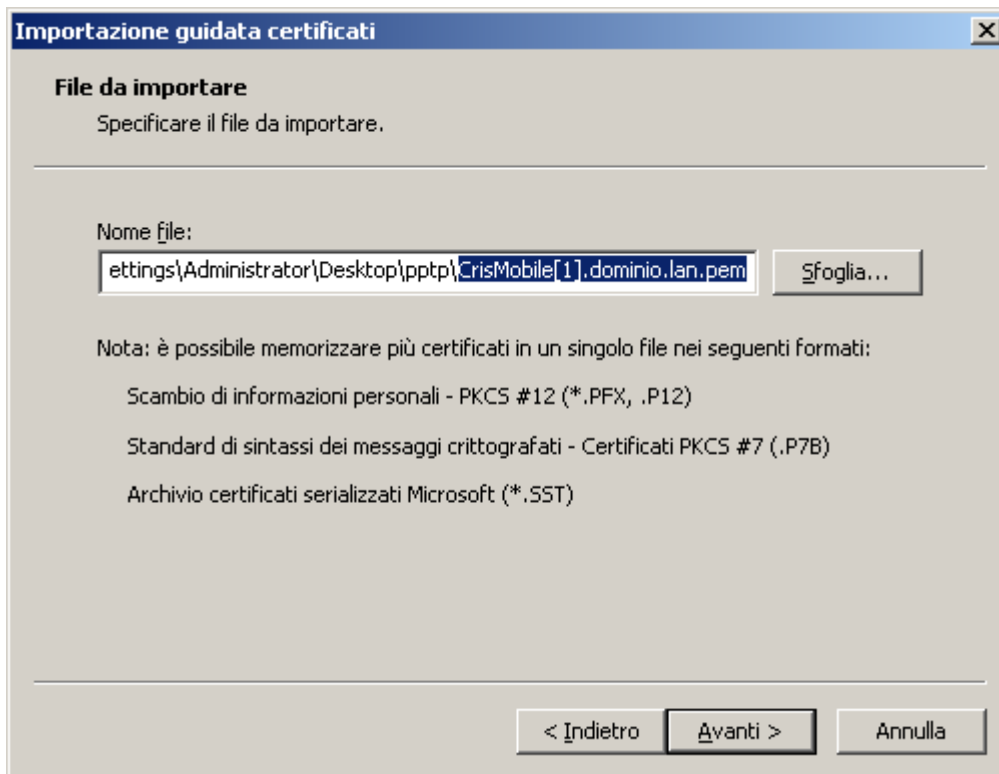




Fine – Chiudi.

Col tasto destro su Personal – Certificati scegliere IMPORTA come di seguito:





Facciamo lo stesso con il PKCS#12 (PFX):

**Importazione guidata certificati** [X]

**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** [X]

**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

Procediamo creando una nuova connessione di rete nel pannello di controllo:

**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

**Creazione guidata nuova connessione**

**Nome connessione**  
Specificare un nome per la connessione alla rete aziendale.

Immettere un nome per la connessione nella seguente casella.

Nome società

Rete di casa mia

Ad esempio, è possibile immettere il nome della rete aziendale o del server a cui si effettuerà la connessione.

< Indietro   Avanti >   Annulla

Nella seguente schermata possiamo inserire l'ip pubblico statico dell'interfaccia esterna di Zeroshell. Possiamo anche usare ( se non disponiamo di ip pubblici statici da assegnare al Firewall) le funzionalità di DynDns.org.

**Creazione guidata nuova connessione**

**Selezione server VPN**  
Indicare il nome o l'indirizzo del server VPN.

Digitare il nome host o l'indirizzo IP del protocollo internet del computer a cui si sta effettuando la connessione.

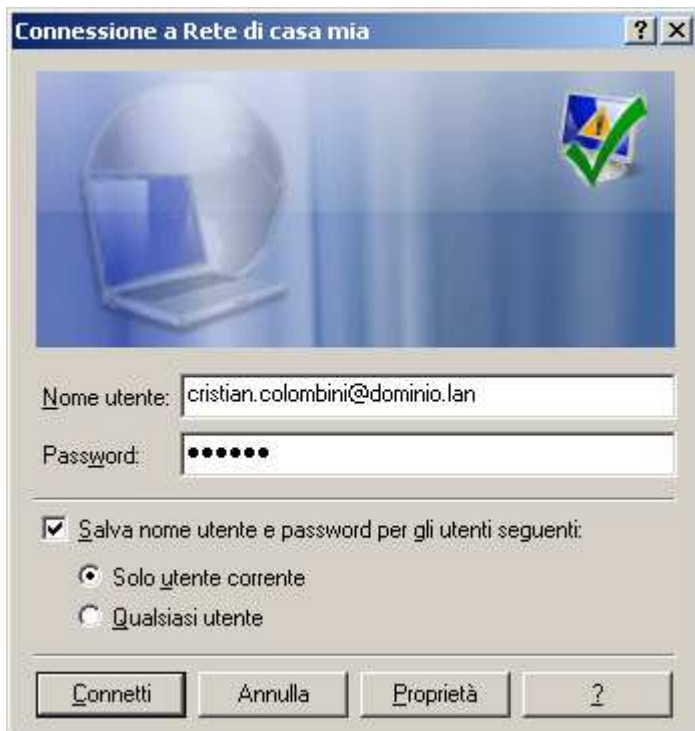
Nome host o indirizzo IP (ad esempio microsoft.com o 157.54.0.1):

62.62.62.1

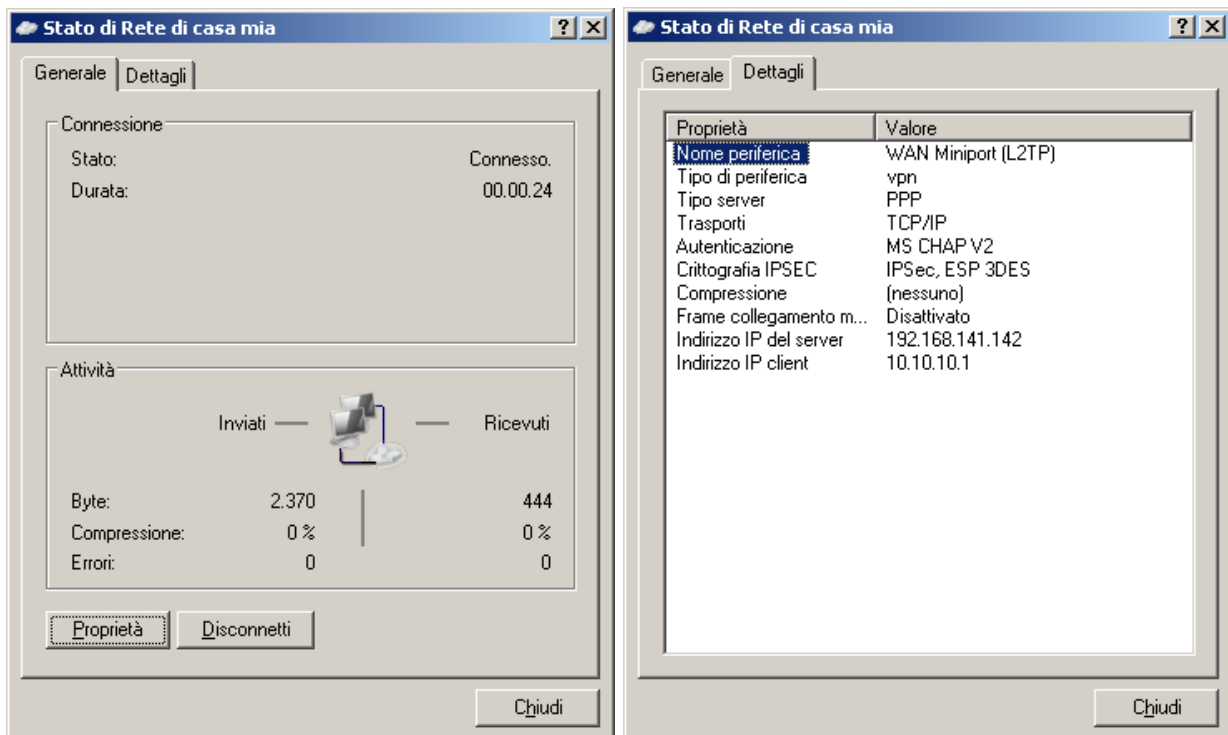
< Indietro   Avanti >   Annulla

Fine

Compiliamo i seguenti campi rispettando maiuscole e minuscole:



Fare attenzione al nome utente che è seguito ovviamente dal dominio al quale appartiene ( il dominio configurato su Zeroshell). Connetti:



Vediamo l'ip che ci è stato assegnato: 10.10.10.1. Bene.

Controlliamo sul firewall nel menu VPN nel bottone Show Clients chi si è collegato:

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)

### E nel bottone Radius Log come lavora il server Radius:

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)

## Filtri di sicurezza sul tunnel

A questo punto qualsiasi comunicazione può passare dall'host alla sede e viceversa. Per motivi sempre legati alla sicurezza possiamo stabilire delle regole molto rigide per chi entra nella nostra rete in questo modo; possiamo bloccare qualsiasi comunicazione esclusa la connessione ad un server web interno per esempio:

consultazione di un server web 192.168.0.100 ( TCP 80 e TCP 443)

Ecco come nel menu FIREWALL dobbiamo intervenire:

Release 1.0.beta4  
CPU ( 1) Pentium III (Coppermine) 996MHz Refresh  
Uptime: 0 days, 0:1  
Load Avg: 1.00 0.26 0.08  
Kernel: 2.6.19.3  
Memory: 405164 kb

Chain: FORWARD Policy: ACCEPT Chain: FORWARD New Remove View Show Log  
Save Cancel Enabled

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"/>

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

Operazione completata

Come si vede ho creato delle regole che vengono lette dall'alto verso il basso. In fondo ho messo la regola che blocca qualsiasi tipo di comunicazione dalla rete 192.168.0.0/24 alla 10.10.10.0/24. Tutto quello che sta sopra sono le richieste che invece dovranno passare.