**Zeroshell: VPN Host-to-Lan**


Il sistema operativo multifunzionale

creato da Fulvio.Ricciardi@zeroshell.net

www.zeroshell.net

Assicurare la comunicazione fra un host ed una rete

( Autore: 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

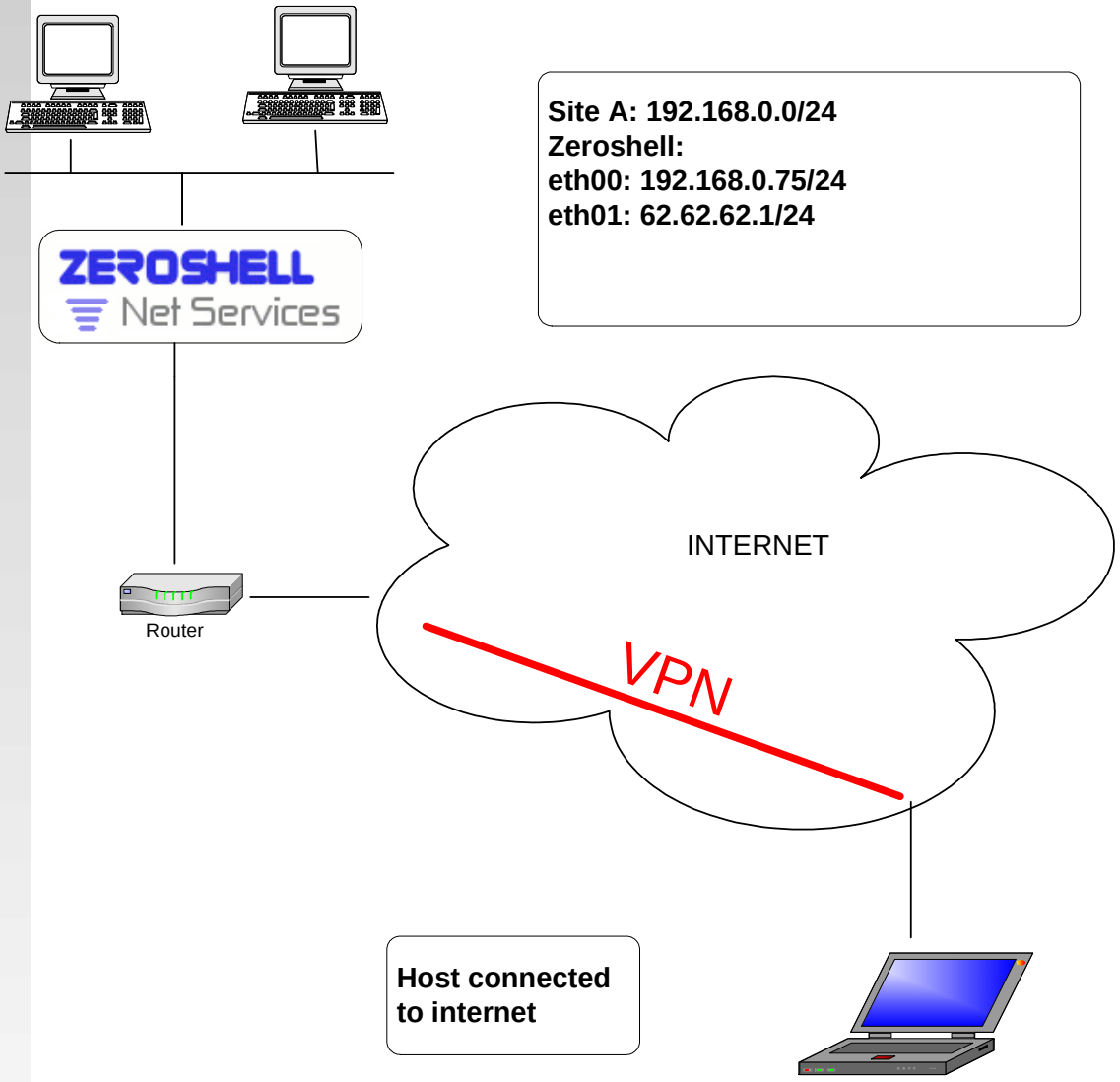
Host:

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

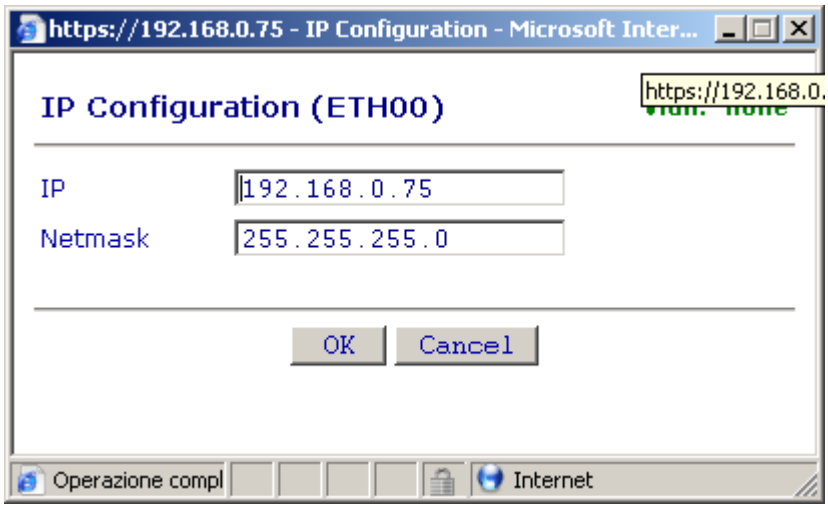


**Preparazione dei firewall**

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

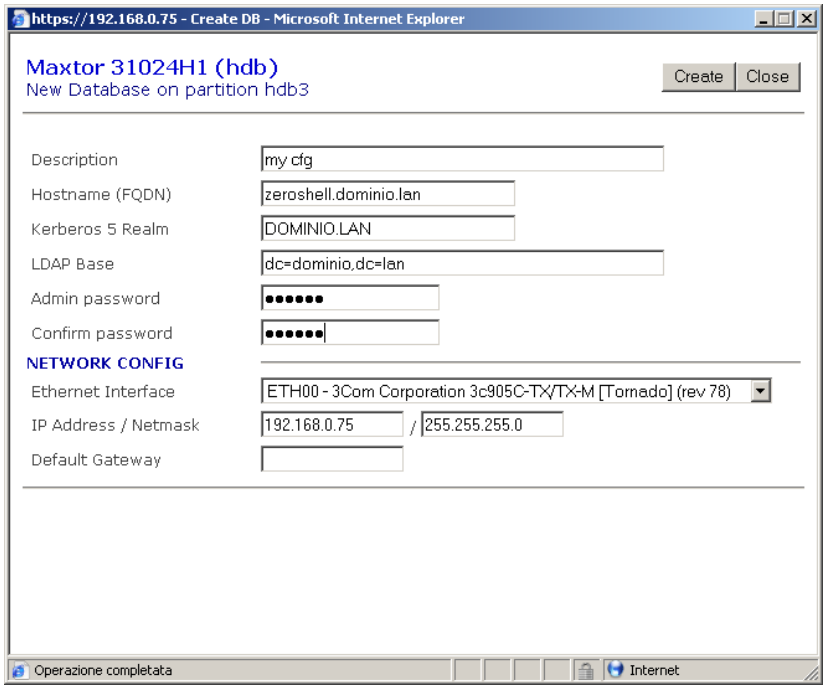
1 – primo accesso al firewall
2 – impostazione dell’indirizzo ip sulla scheda di rete interna:

SiteA:



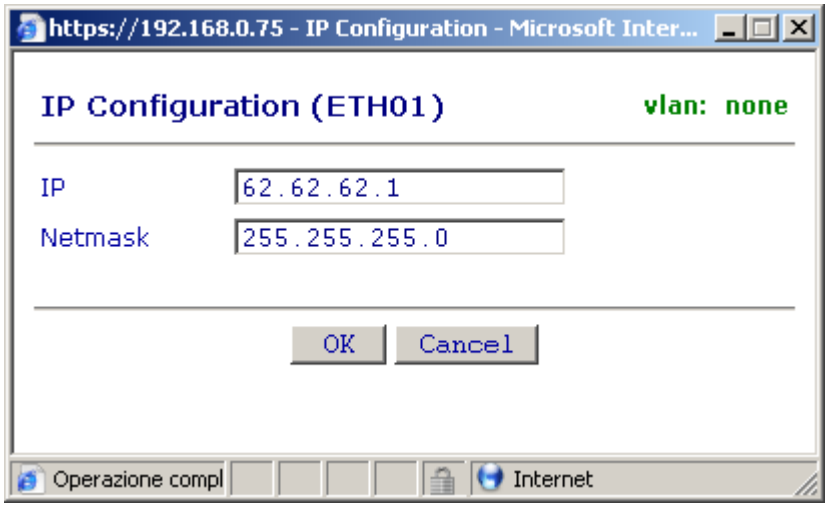

3 – Creare un databse di configurazione:

SiteA:

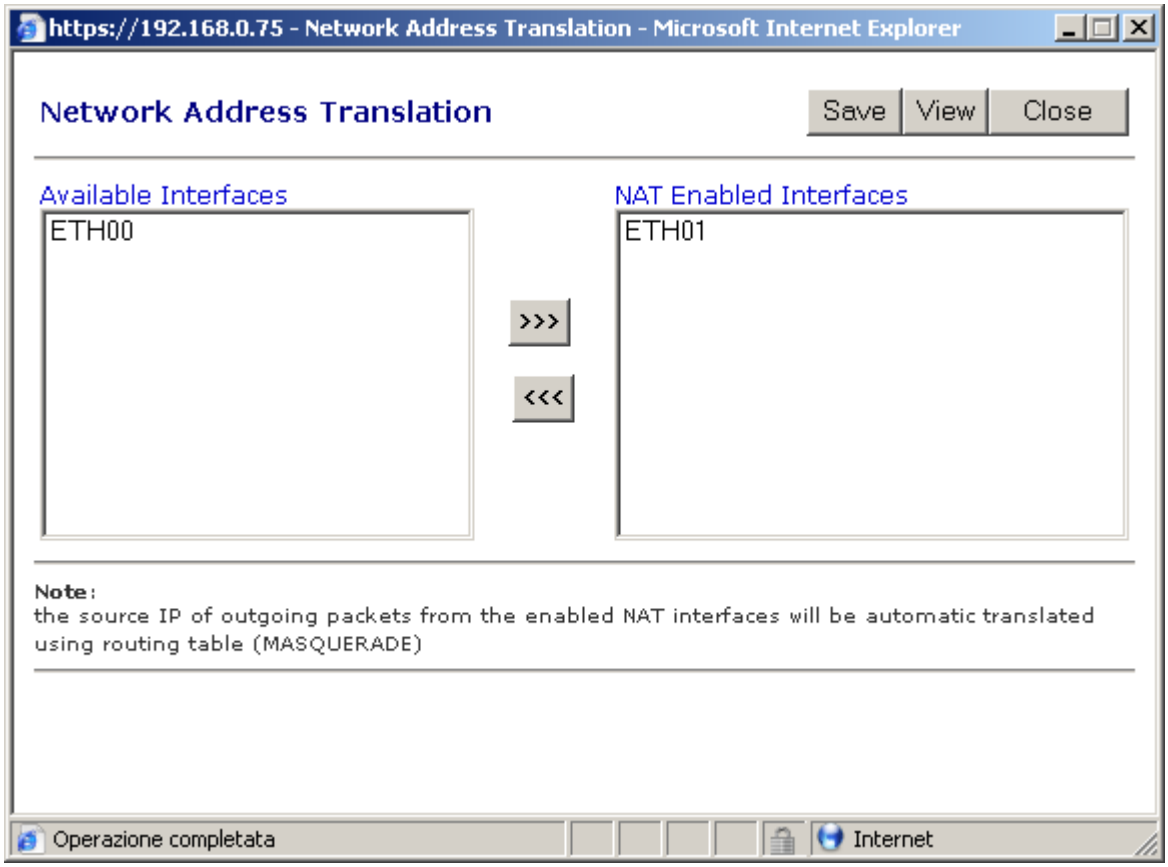


4 – Attivare sul firewall il database ed attendere il riavvio del sistema
5 – Impostare l' indirizzo ip sulla scheda di rete esterna:

SiteA:



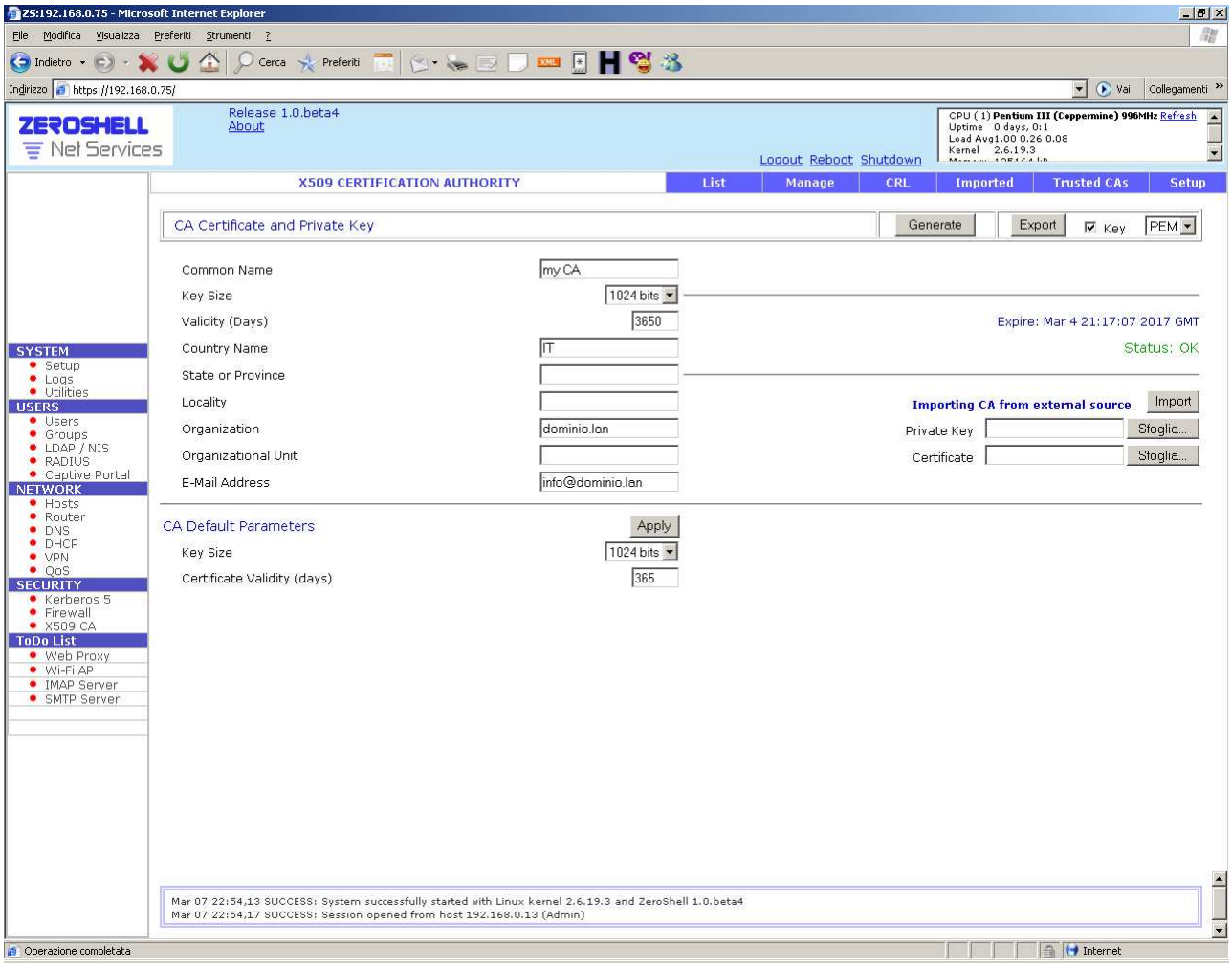

6 – Nel Router, alla voce NAT spostiamo la ETH01 in modo che vada a mascherare la nostra rete sulla ETH00:



**Preparazione del certificato del firewall:**

Creare il certificato del firewall:

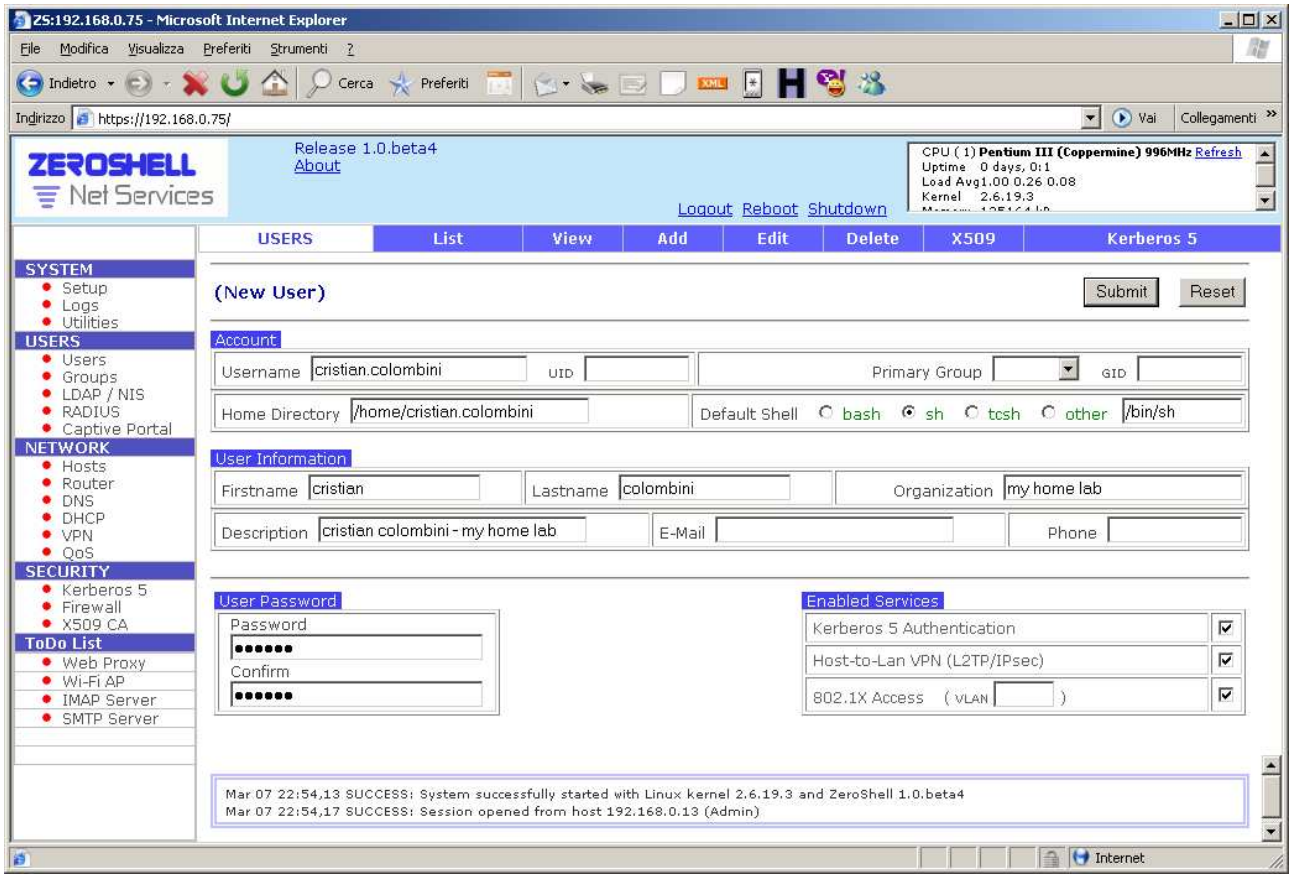
Nel menu “X509 CA”, portarsi alla voce “SETUP”:




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

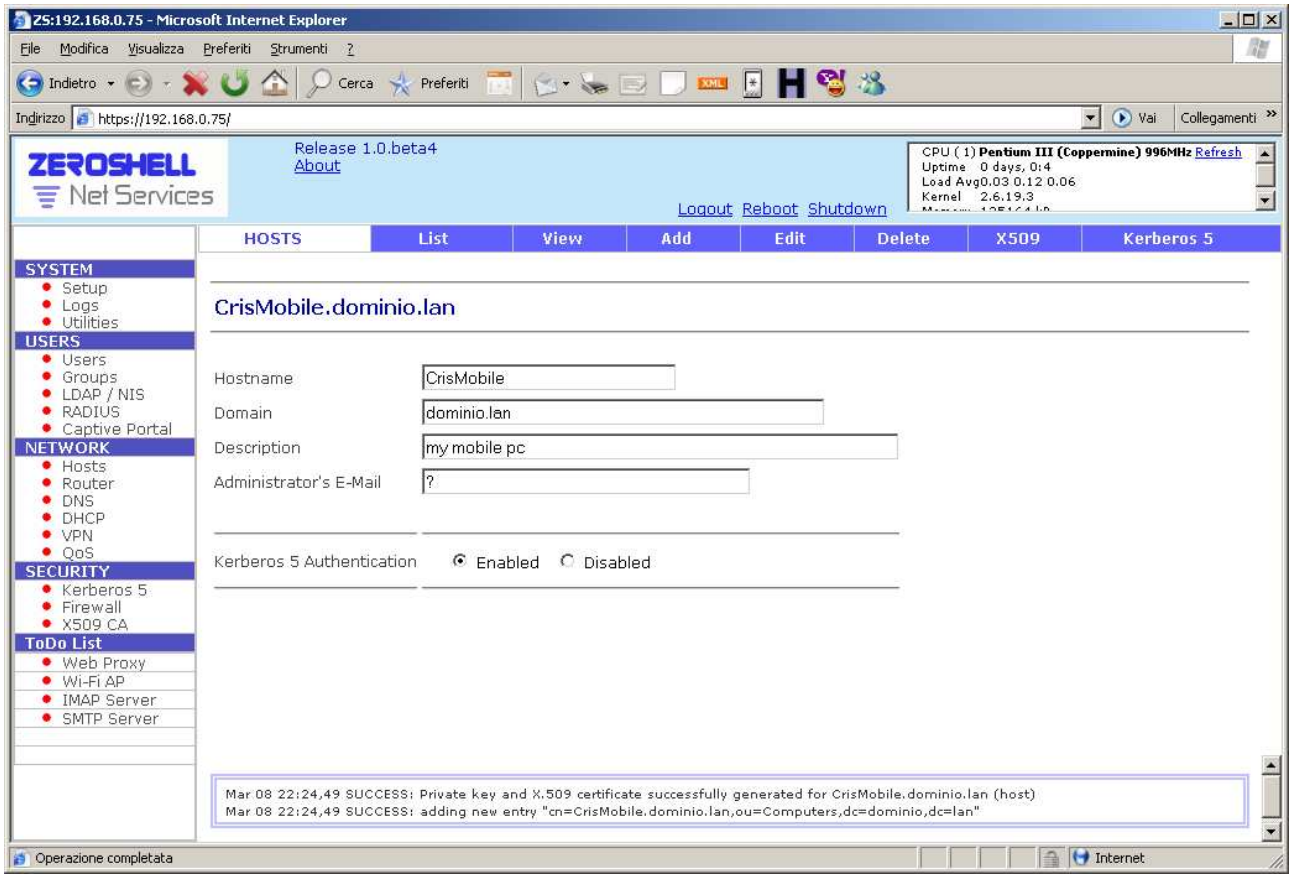
**Preparazione degli utenti e degli hosts:**

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



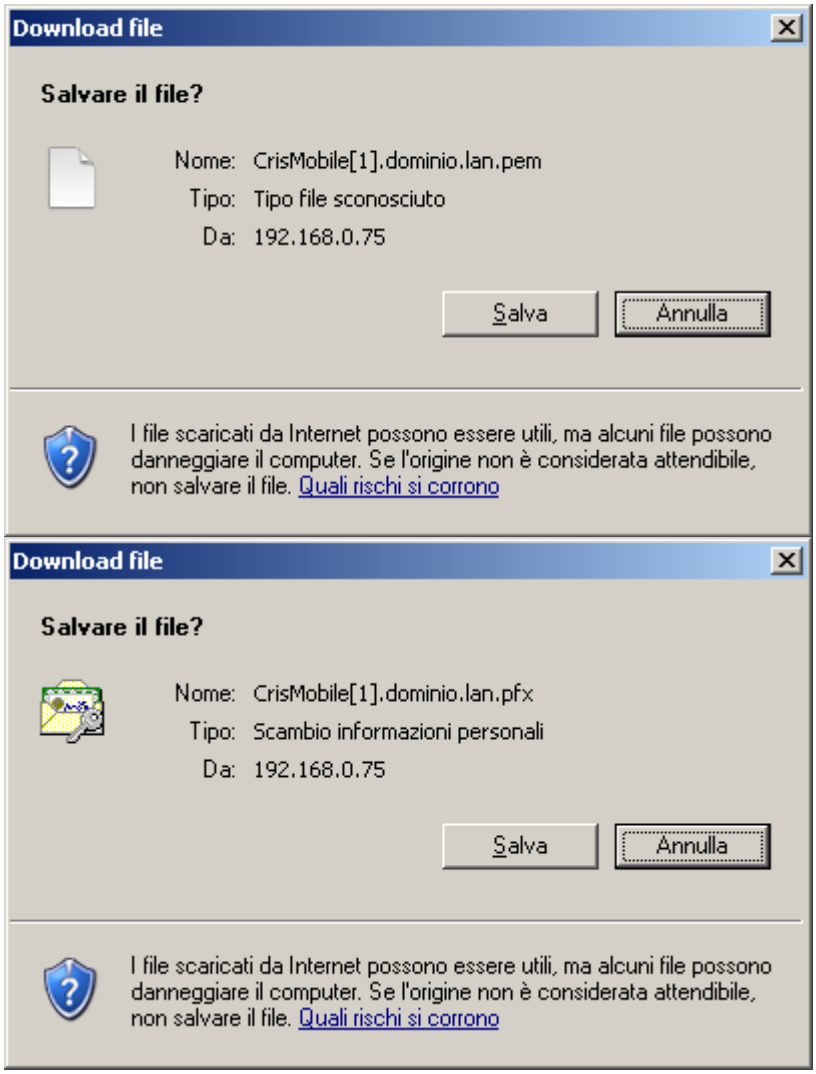

Riempire i campi tenendo presente che è sempre meglio usare una password strong ( per esempio: %RF45£”Se ) ..anche questo fa parte della sicurezza..no?
Accertarsi che sia flaggata la voce Host-to-Lan VPN (L2TP/Ipsec).

Recarsi al menu HOSTS e cliccare su ADD:


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.beta4
About
Logout Reboot Shutdown
CPU ( 1) Pentium III (Coppermine) 996MHz Refresh
Uptime 0 days, 0:4
Load Avg0.03 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
CrisMobile.dominio.lan
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

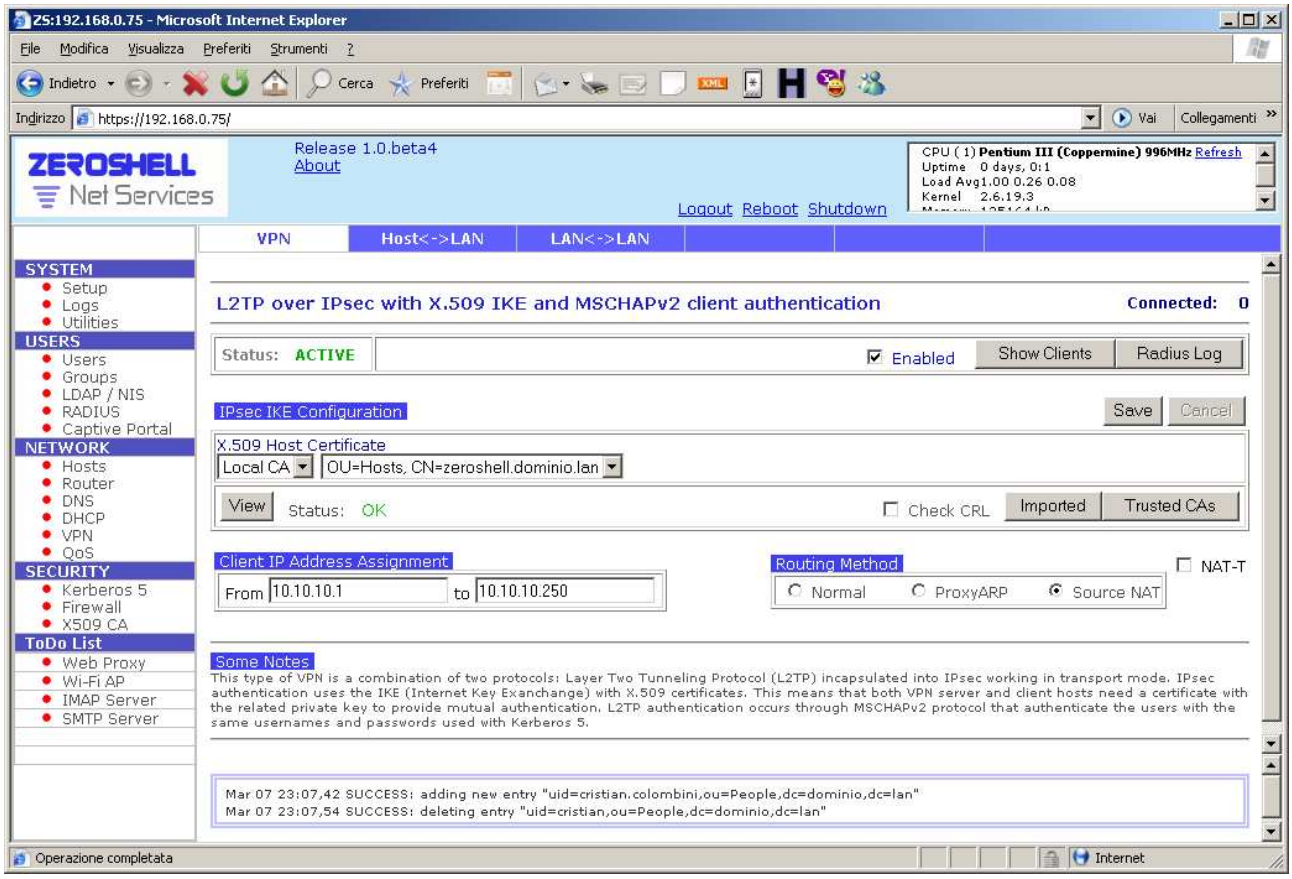
**Esportazione dei certificati per i clients**

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:



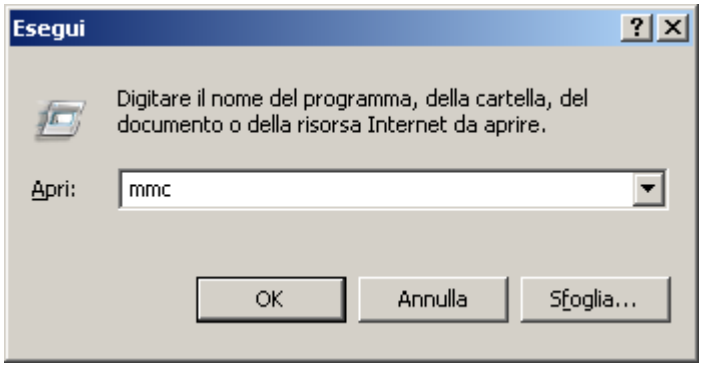

Verificare inoltre che gli ip assegnati appartengano ad una nuova rete non esistente nelle nostre ( nal mio caso gli hosts remoti che si connetteranno riceveranno gli ip dal 10.10.10.1 al 10.10.10.250).

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

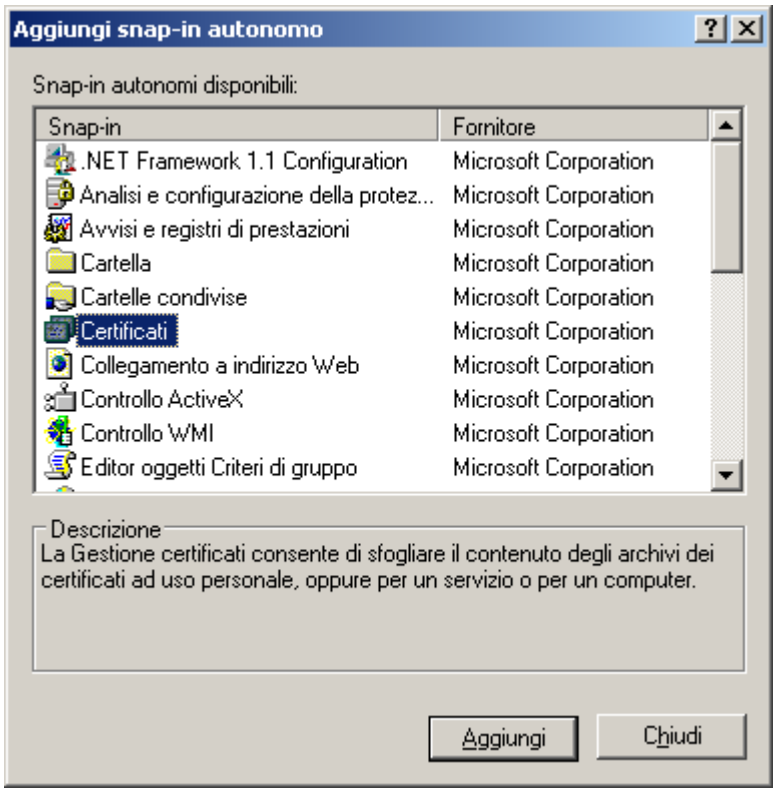
A questo punto possiamo configurare il client VPN sull'host. Nel mio caso si tratta di un sistema Ms Windows Xp Prof… ma il concetto vale per tutti i sistemi.

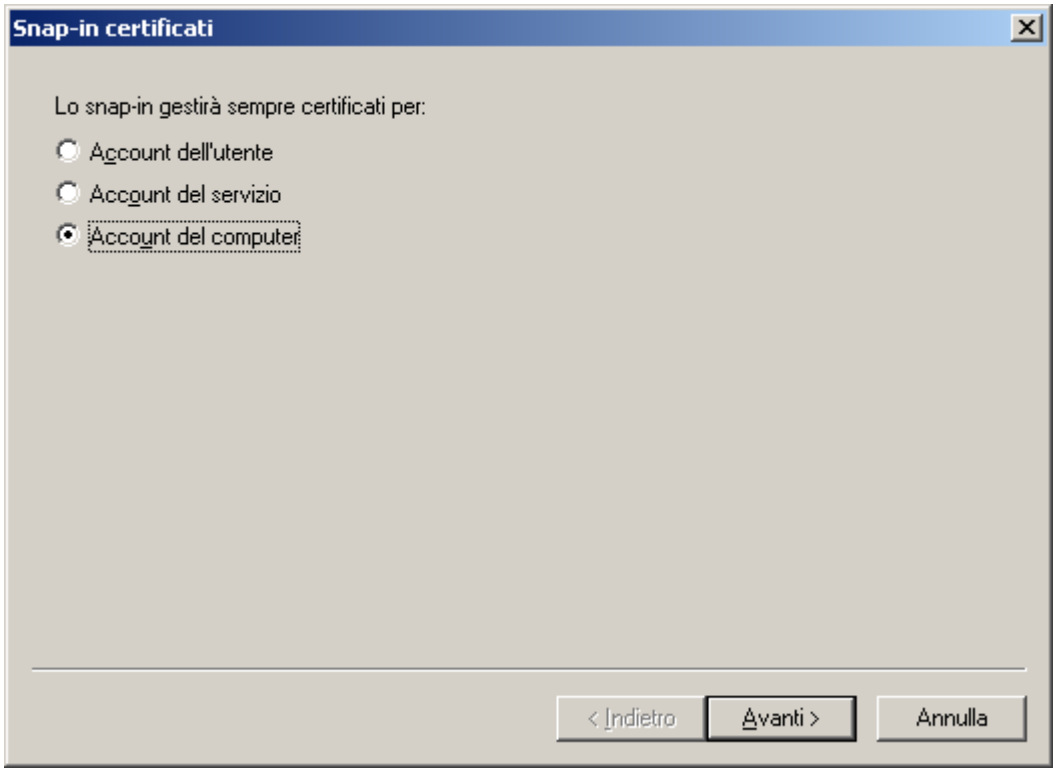
Importiamo il certificato che abbiamo salvato dal firewall:

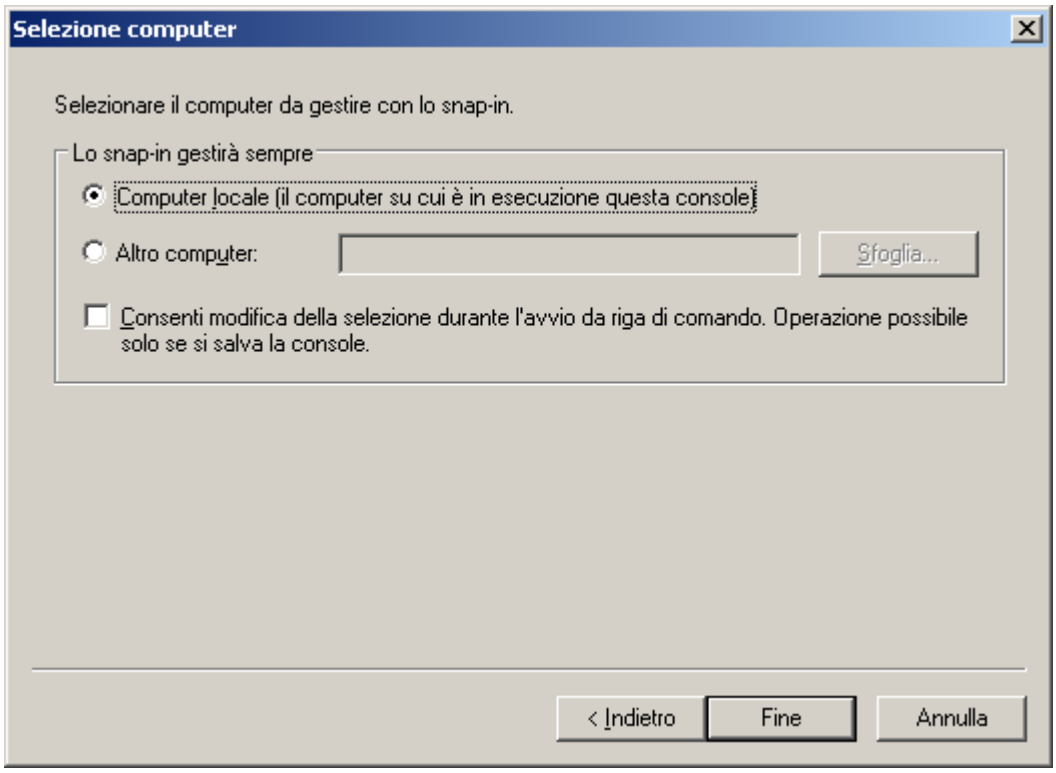
apriamo la console di microsoft con "mmc":




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

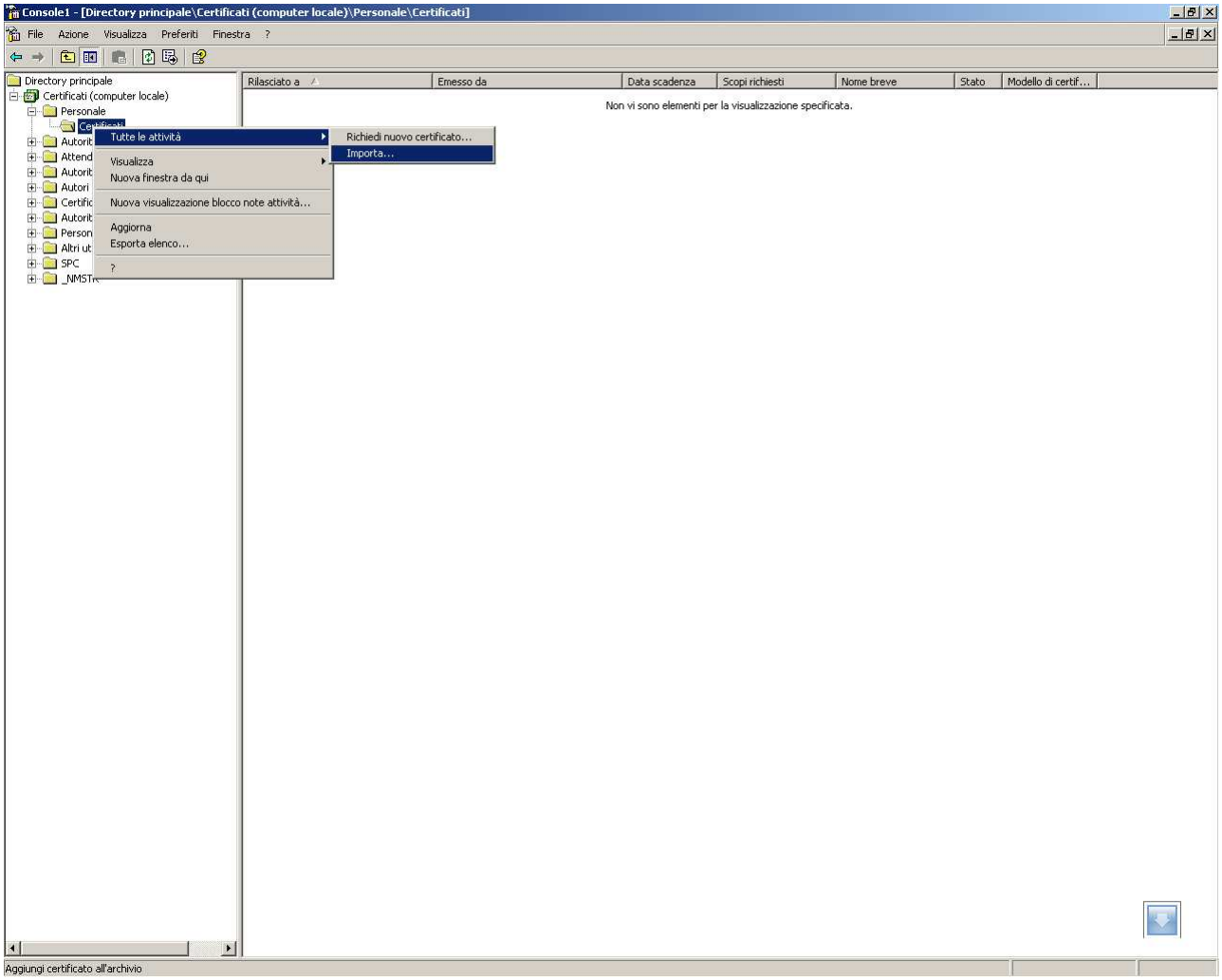




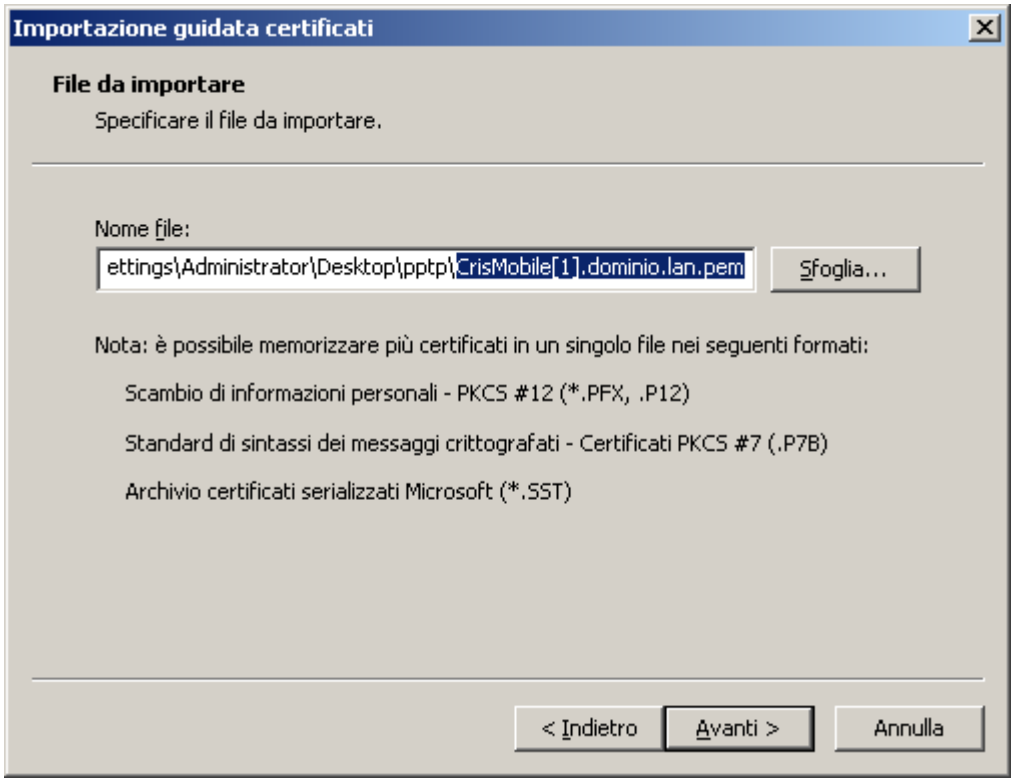



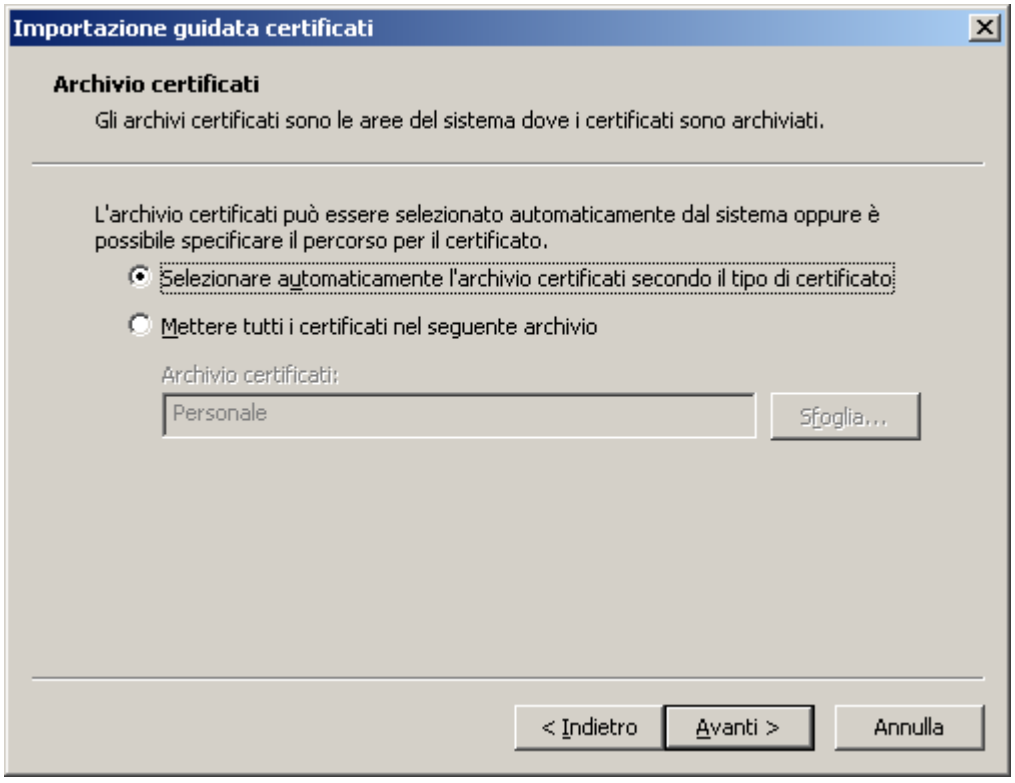

Fine – Chiudi.

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

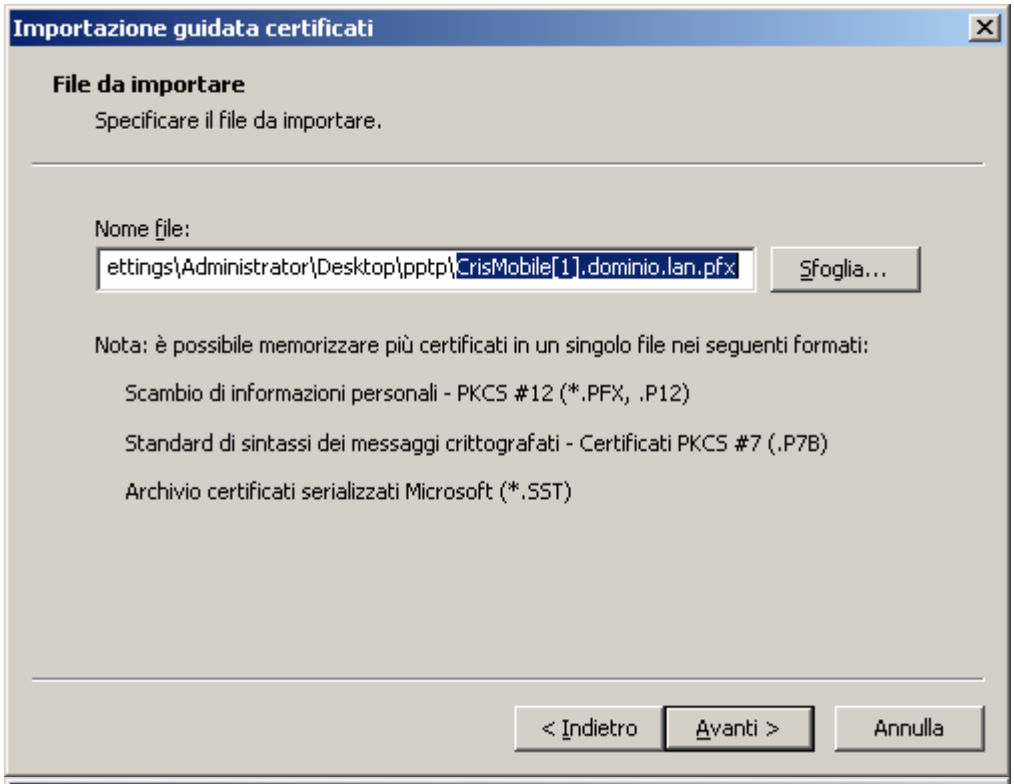

Console1 - [Directory principale\Certificati (computer locale)\Personale\Certificati]
File Azione Visualizza Preferiti Finestra ?
Directory principale
Certificati (computer locale)
Personale
Certificati
Tutte le attività
Visualizza
Nuova finestra da qui
Nuova visualizzazione blocco note attività...
Aggiorna
Esporta elenco...
?
Richiedi nuovo certificato...
Importa...
Rilasciato a
Emesso da
Data scadenza
Scopi richiesti
Nome breve
Stato
Modello di certif...
Non vi sono elementi per la visualizzazione specificata.
Aggiungi certificato all'archivio

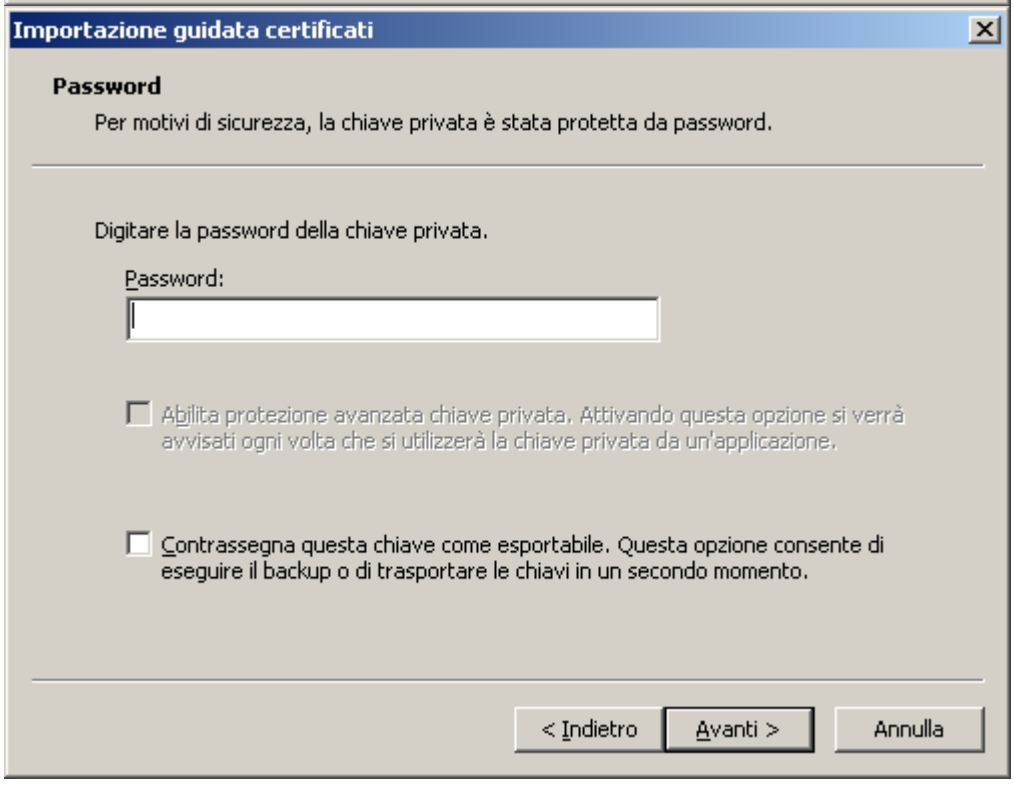

Importazione guidata certificati
Importazione guidata certificati
Questa procedura guidata permette di copiare certificati, elenchi di certificati attendibili ed elenchi di revoche di certificati dal disco all'archivio certificati.
Un certificato rilasciato da un'Autorità di certificazione conferma l'identità dell'utente e contiene informazioni utilizzate per proteggere i dati o per stabilire connessioni di rete protette. L'archivio certificati è l'area del sistema dove i certificati sono archiviati.
Per continuare, scegliere Avanti.
< Indietro
Avanti >
Annulla

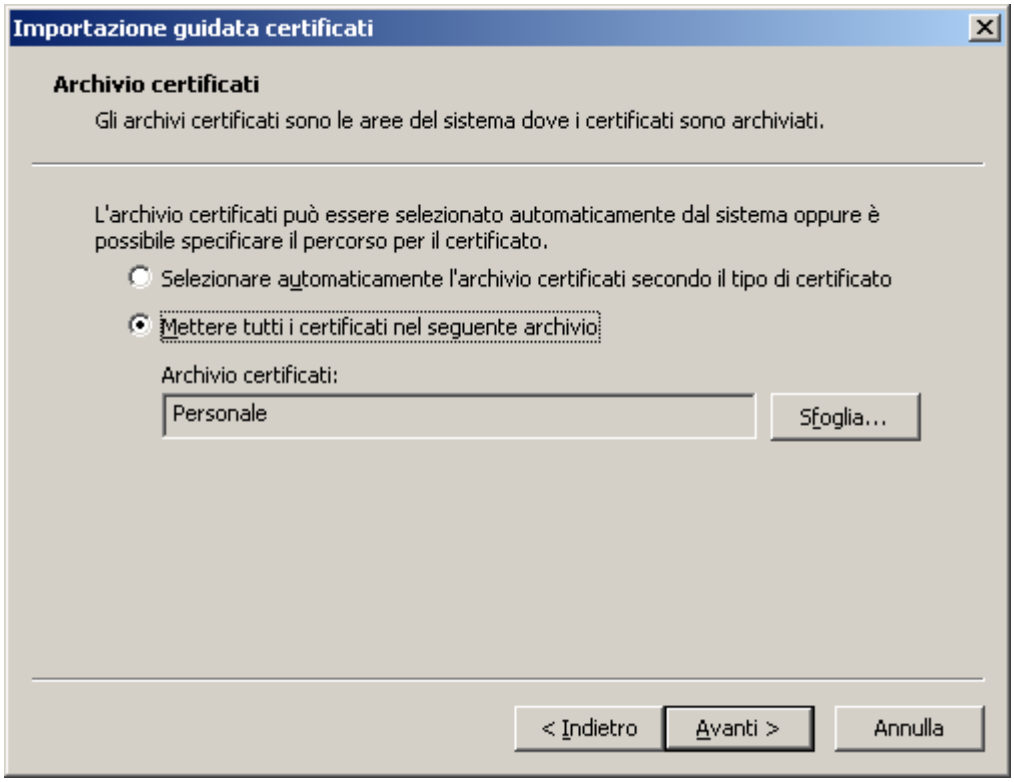


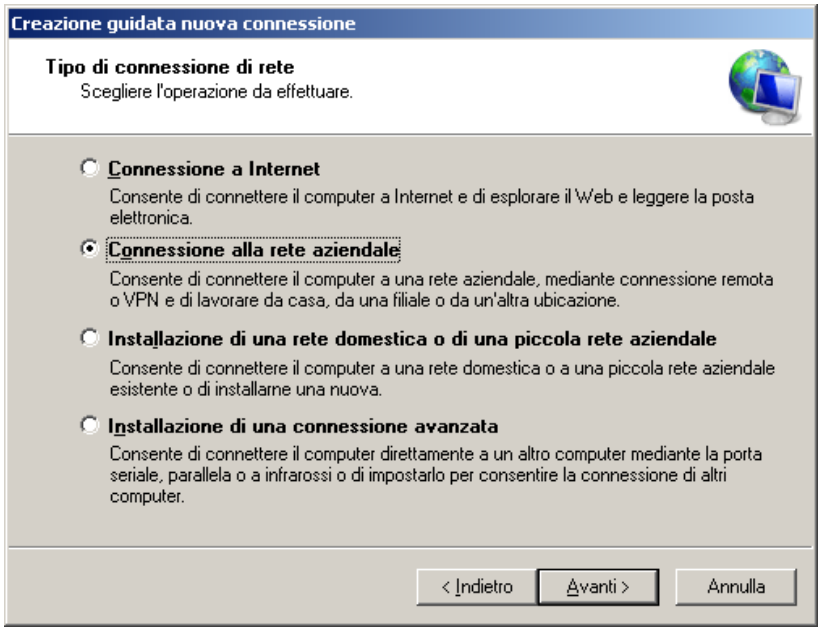

Facciamo lo stesso con il PKCS#12 (PFX):

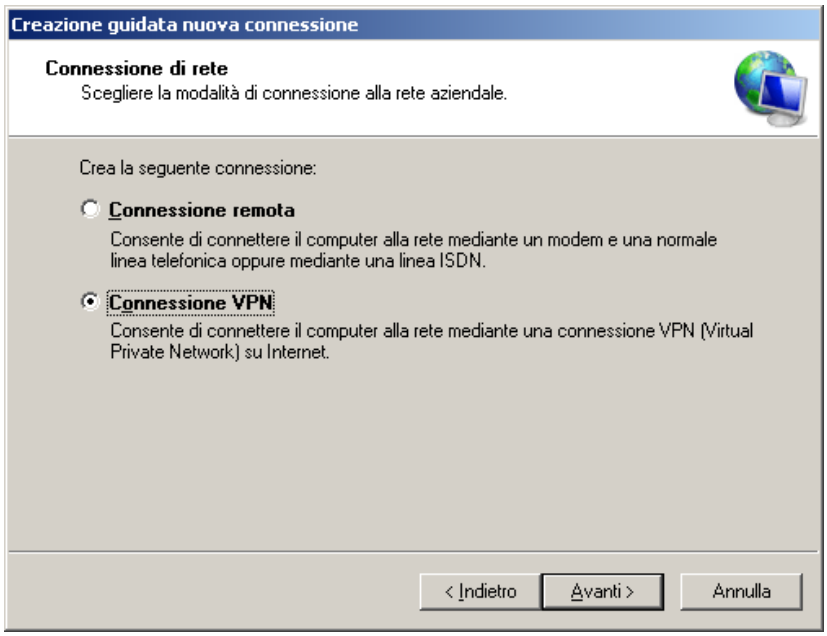

Importazione guidata certificati
File da importare
Specificare il file da importare.
Nome file:
ettings\Administrator\Desktop\pptp\CrisMobile[1].dominio.lan.pfx
Sfoglia...
Nota: è possibile memorizzare più certificati in un singolo file nei seguenti formati:
Scambio di informazioni personali - PKCS #12 (*.PFX, .P12)
Standard di sintassi dei messaggi crittografati - Certificati PKCS #7 (.P7B)
Archivio certificati serializzati Microsoft (*.SST)
< Indietro
Avanti >
Annulla

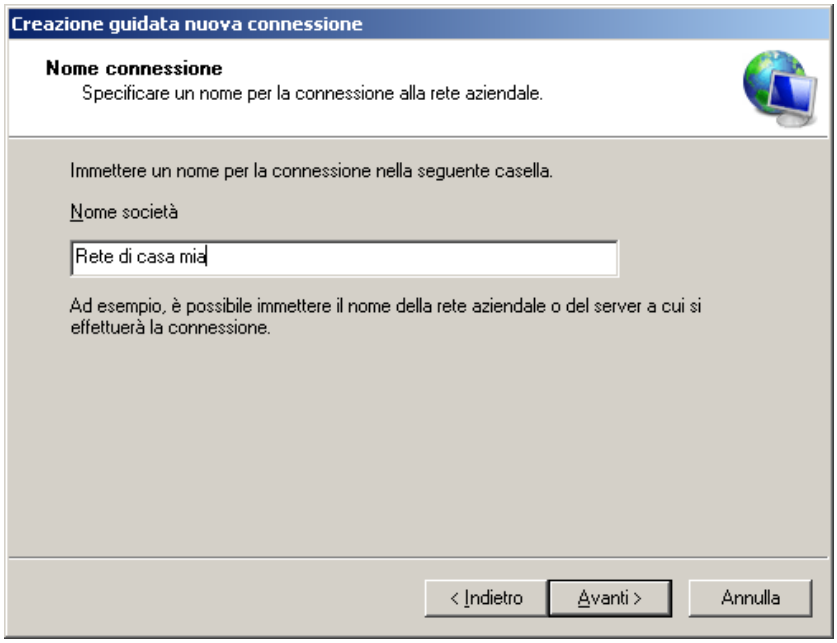

Importazione guidata certificati
Password
Per motivi di sicurezza, la chiave privata è stata protetta da password.
Digitare la password della chiave privata.
Password:
Abilita protezione avanzata chiave privata. Attivando questa opzione si verrà avvisati ogni volta che si utilizzerà la chiave privata 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
Sfoglia...
< Indietro
Avanti >
Annulla

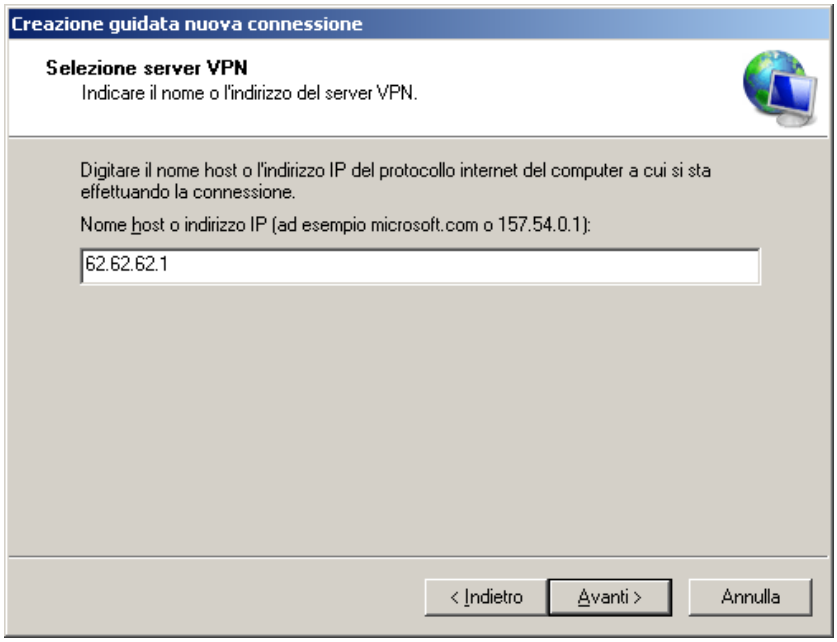
Procediamo creando una nuova connessione di rete nel pannello di controllo:



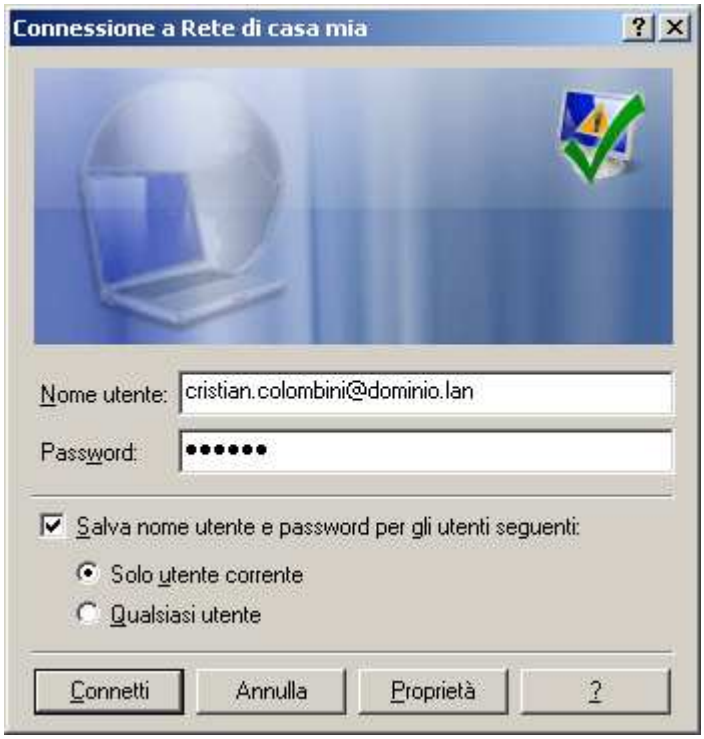





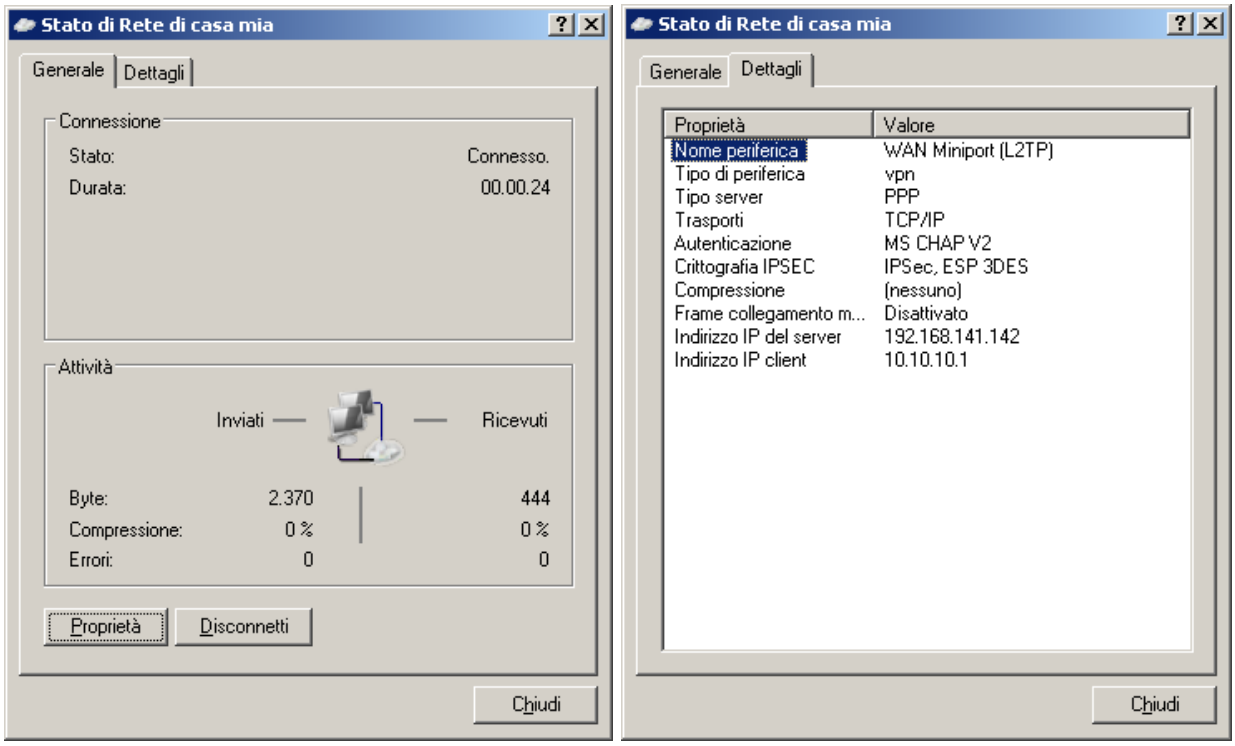

Nella seguente schermata possiamo inserire l'ip pubblico statico dell'interfaccia esterna di Zeroshell. Possiamo anche usare ( se non disponiamo di ip pubblici statici da assegnare al Firewall) le funzionalità di DynDns.org.




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.

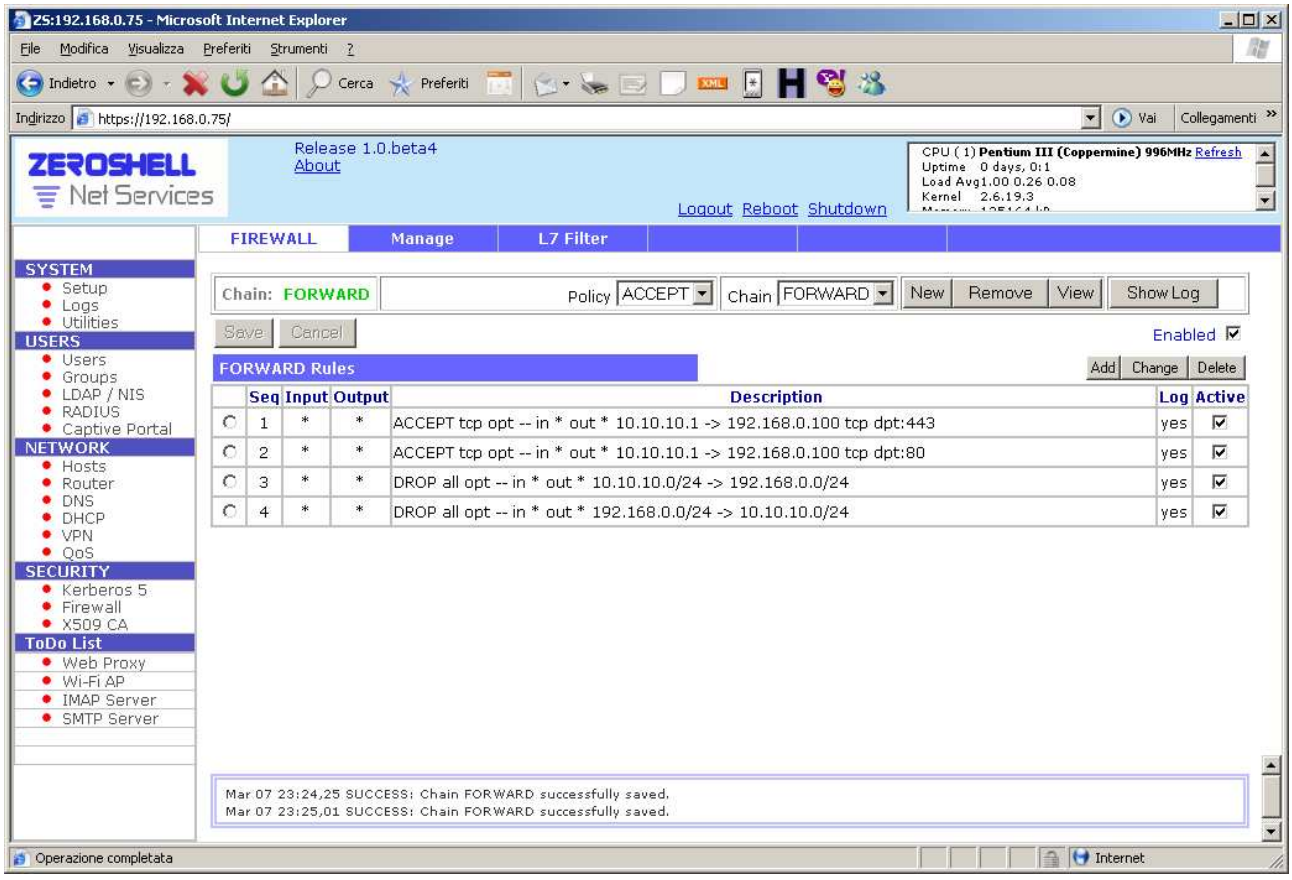
**23:17:56** Login OK: [cristian.colombini@dominio.lan] (from client localhost port 10)

**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:




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.