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

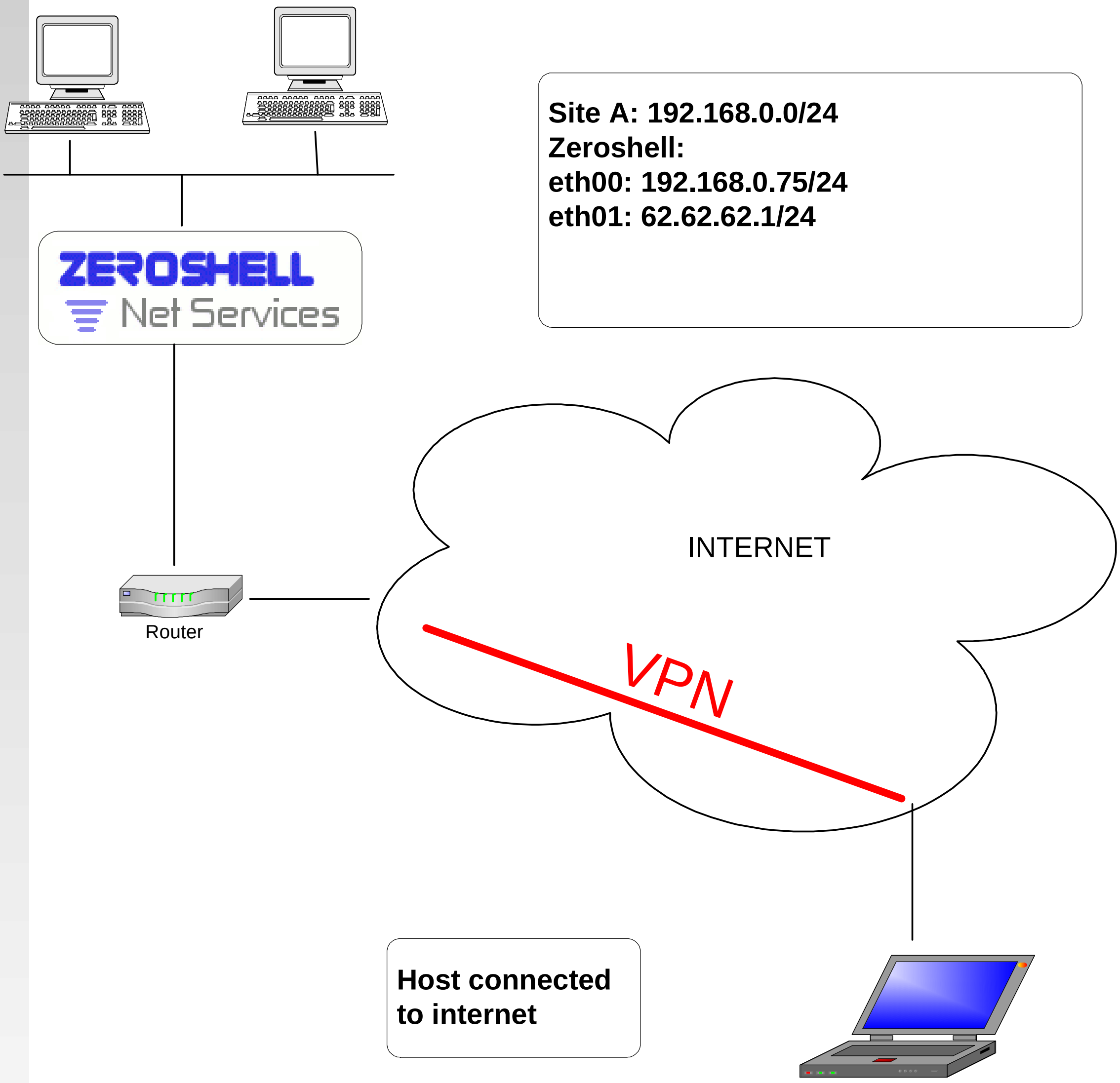
Host:

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



Site A: 192.168.0.0/24
Zeroshell:
eth00: 192.168.0.75/24
eth01: 62.62.62.1/24

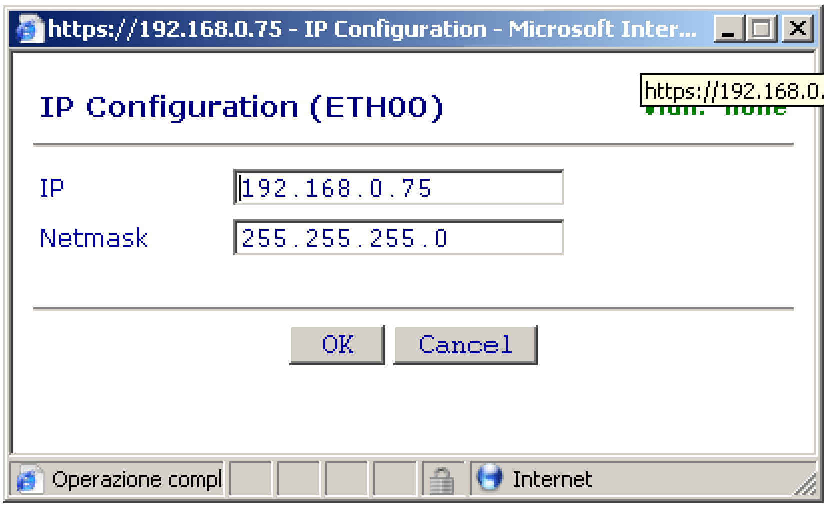
Host connected to internet

Preparing the firewall

Using th 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:


https://192.168.0.75 - IP Configuration - Microsoft Inter...
https://192.168.0.
OK
Cancel
Operazione compl
Internet

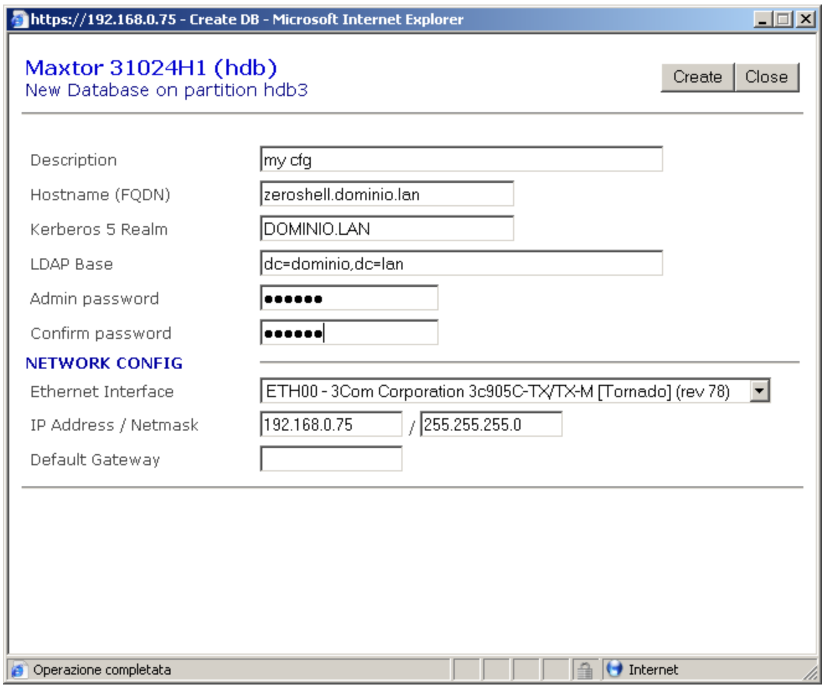
IP Configuration (ETH00)

IP 192.168.0.75

Netmask 255.255.255.0

3 – Create a configuration DB:

SiteA:


https://192.168.0.75 - Create DB - Microsoft Internet Explorer
Create
Close
Operazione completata
Internet

Maxtor 31024H1 (hdb)
New Database on partition hdb3

Description	my cfg
Hostname (FQDN)	zeroshell.dominio.lan
Kerberos 5 Realm	DOMINIO.LAN
LDAP Base	dc=dominio,dc=lan
Admin password	••••••
Confirm password	••••••

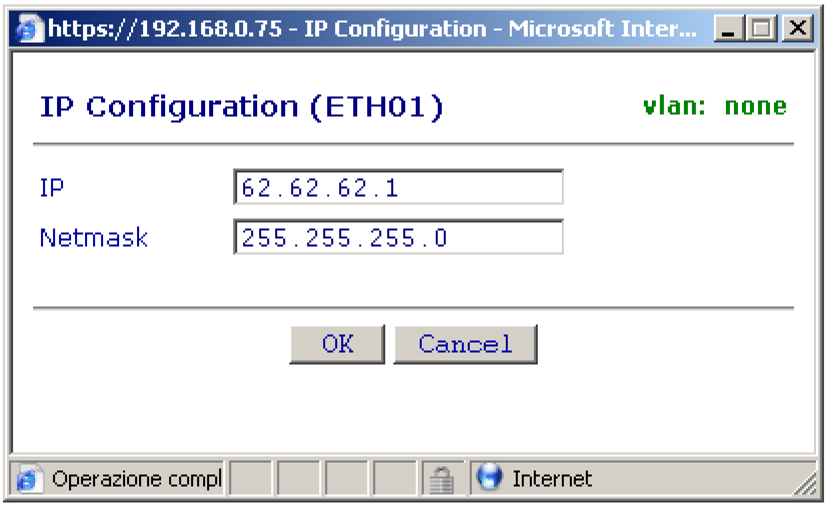
NETWORK CONFIG

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	

4 – Enabling the database configuration

5 – Set ip address on external interface:

SiteA:



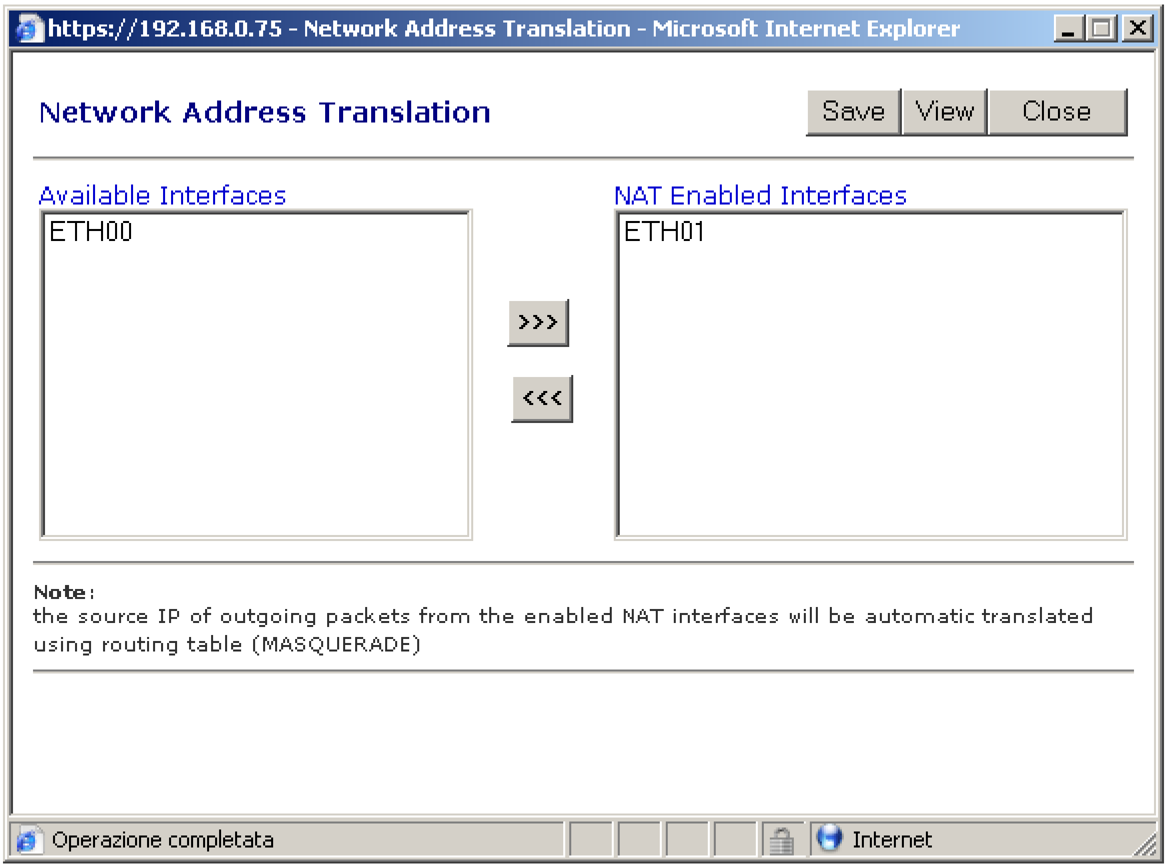
https://192.168.0.75 - IP Configuration - Microsoft Inter...

IP Configuration (ETH01) vlan: none

IP 62.62.62.1

Netmask 255.255.255.0

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



https://192.168.0.75 - Network Address Translation - Microsoft Internet Explorer

Network Address Translation

Available Interfaces: ETH00

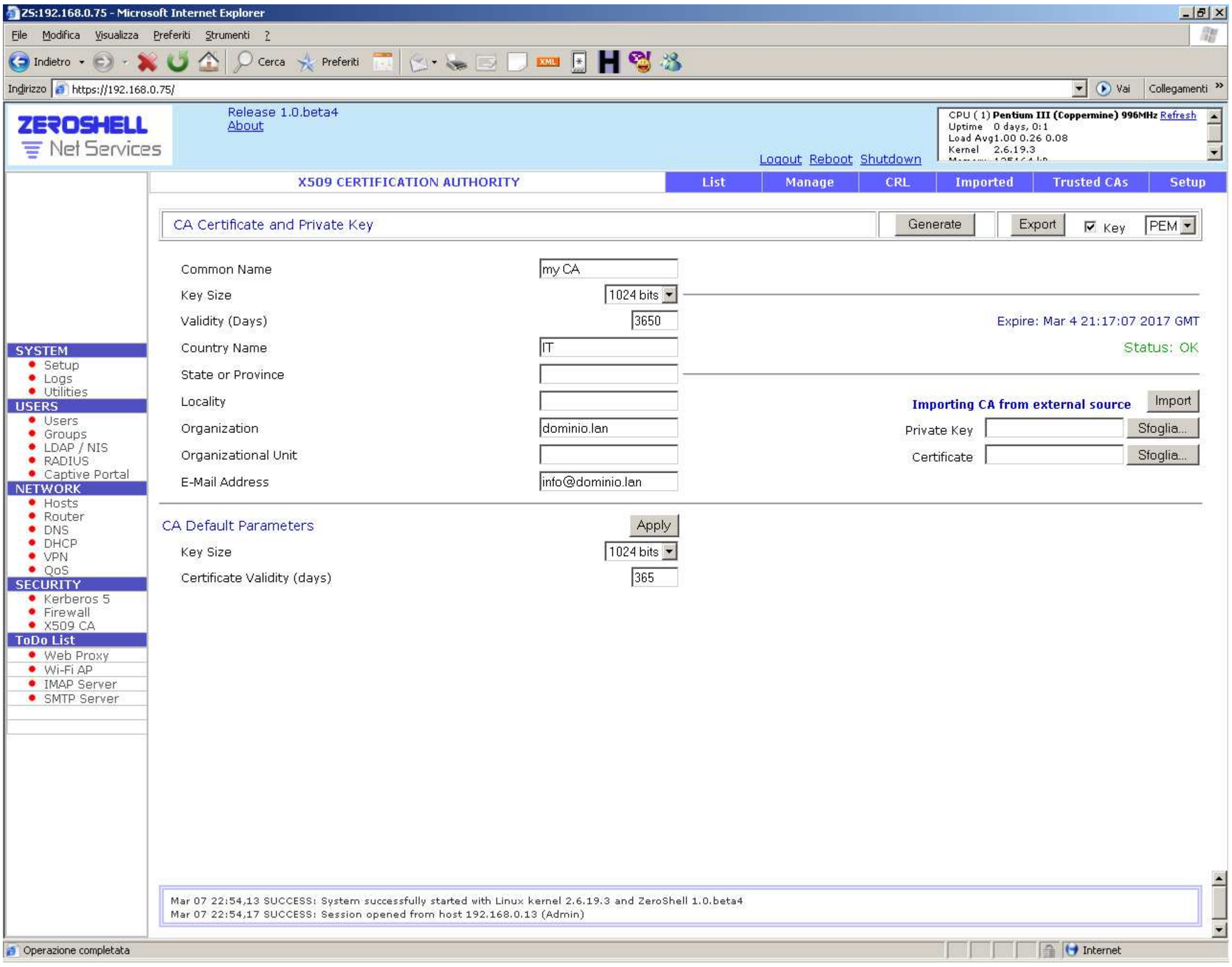
NAT Enabled Interfaces: ETH01

Note:
the source IP of outgoing packets from the enabled NAT interfaces will be automatic translated using routing table (MASQUERADE)

Preparing certificate:

Create the Firewall certificate:

In menu “X509 CA”, click “SETUP”:



CPU (1) **Pentium III (Coppermine) 996MHz** Refresh
Uptime 0 days, 0:1
Load Avg1.00 0.26 0.08
Kernel 2.6.19.3

CA Certificate and Private Key

☑ Key PEM

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

Expire: Mar 4 21:17:07 2017 GMT

Status: OK

Importing CA from external source

Private Key	
Certificate	

CA Default Parameters

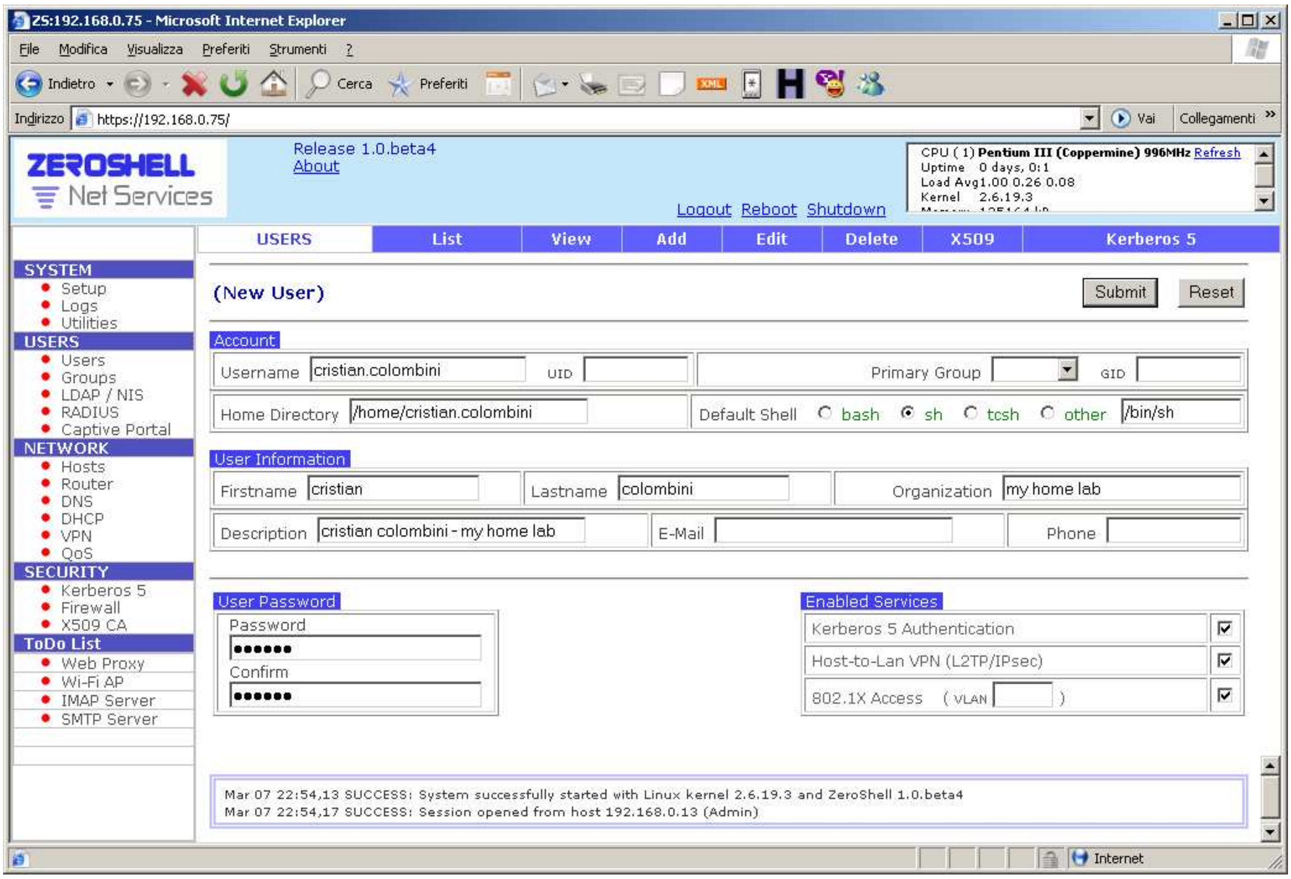
Key Size	1024 bits
Certificate Validity (days)	365

```
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 GENARATE the certificate.

Creating users and hosts:

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



(New User)

Account

Username: cristian.colombini
UID:
Primary Group:
GID:
Home Directory: /home/cristian.colombini
Default Shell: ○ bash ● sh ○ tcsh ○ other /bin/sh

User Information

Firstname: cristian
Lastname: colombini
Organization: my home lab
Description: cristian colombini - my home lab
E-Mail:
Phone:

User Password

Password: ••••••
Confirm: ••••••

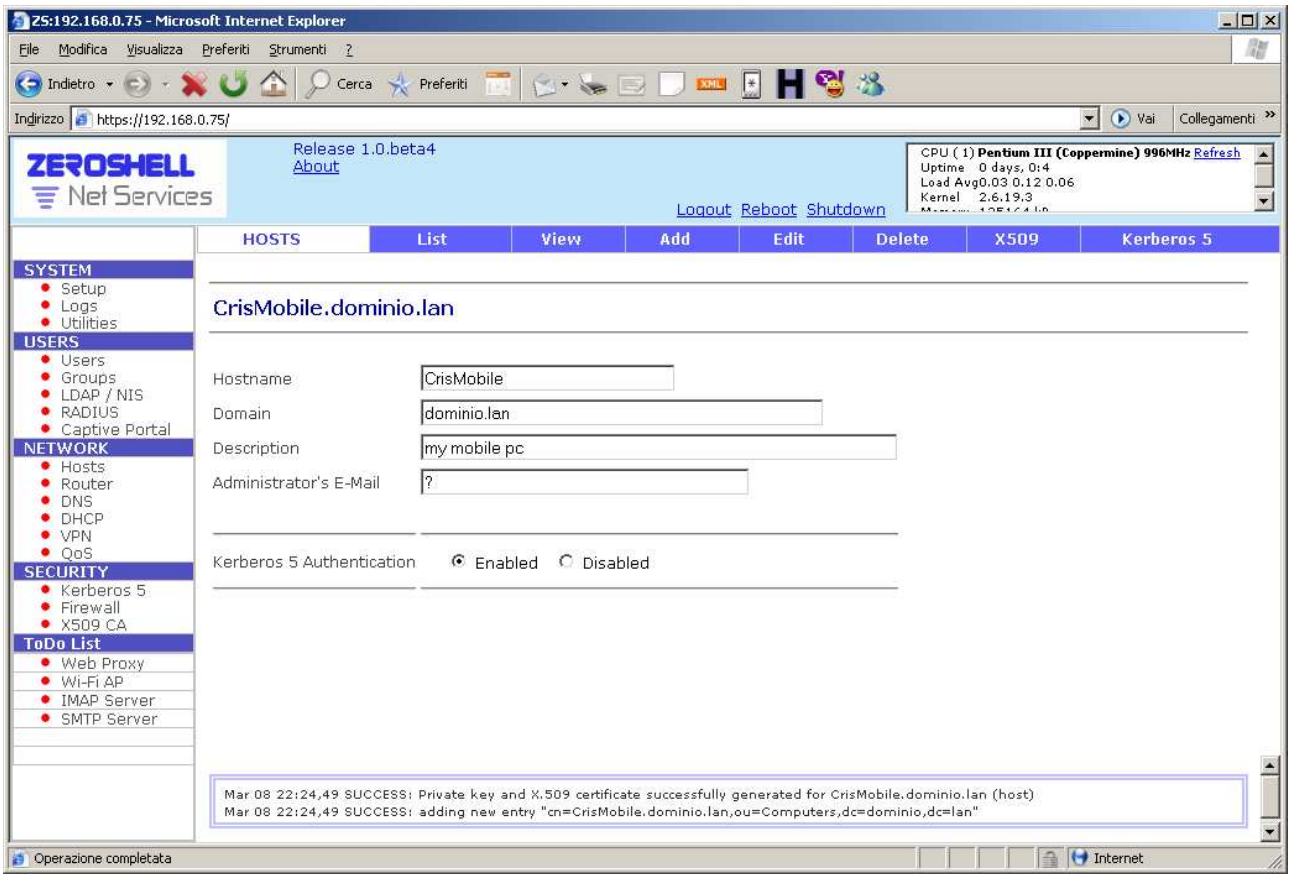
Enabled Services

Kerberos 5 Authentication ☑
Host-to-Lan VPN (L2TP/IPsec) ☑
802.1X Access (VLAN) ☑

```
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 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 estabilish a secure connection.

Now choose HOSTS e click ADD:



```
CPU ( 1) Pentium III (Coppermine) 996MHz Refresh
Uptime   0 days, 0:4
Load Avg0.03 0.12 0.06
Kernel   2.6.19.3
```

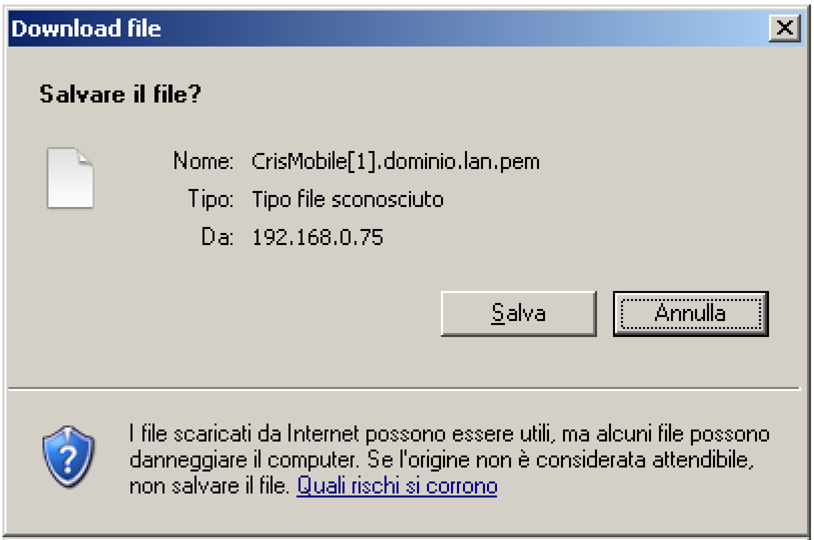
CrisMobile.dominio.lan

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"
```

Exporting the certificates for the remote host

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



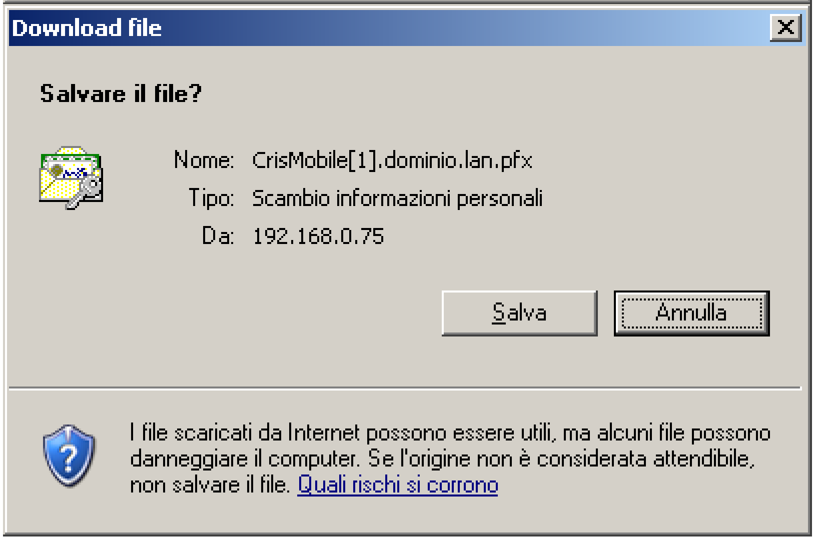
Salvare il file?

Nome: CrisMobile[1].dominio.lan.pem

Tipo: Tipo file sconosciuto

Da: 192.168.0.75

I file scaricati da Internet possono essere utili, ma alcuni file possono danneggiare il computer. Se l'origine non è considerata attendibile, non salvare il file. Quali rischi si corrono



Salvare il file?

Nome: CrisMobile[1].dominio.lan.pfx

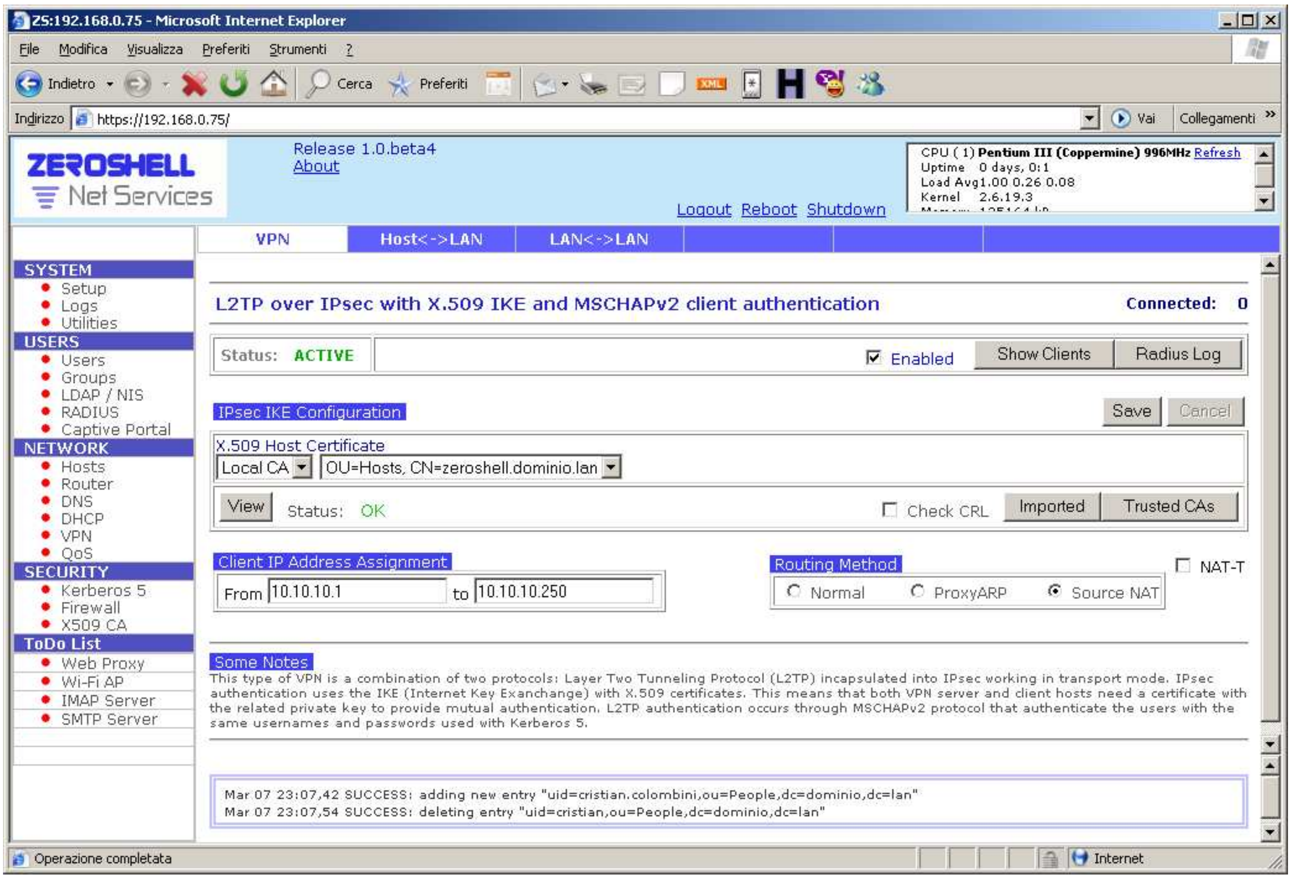
Tipo: Scambio informazioni personali

Da: 192.168.0.75

I file scaricati da Internet possono essere utili, ma alcuni file possono danneggiare il computer. Se l'origine non è considerata attendibile, non salvare il file. Quali rischi si corrono

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:



L2TP over IPsec with X.509 IKE and MSCHAPv2 client authentication — Connected: 0

Status: ACTIVE ☑ Enabled

IPsec IKE Configuration

X.509 Host Certificate: Local CA — OU=Hosts, CN=zeroshell.dominio.lan

Status: OK □ Check CRL

Client IP Address Assignment: From 10.10.10.1 to 10.10.10.250

Routing Method: ○ Normal ○ ProxyARP ● Source NAT □ NAT-T

Some Notes

This type of VPN is a combination of two protocols: Layer Two Tunneling Protocol (L2TP) incapsulated into IPsec working in transport mode. IPsec authentication uses the IKE (Internet Key Exanchange) with X.509 certificates. This means that both VPN server and client hosts need a certificate with the related private key to provide mutual authentication. L2TP authentication occurs through MSCHAPv2 protocol that authenticate the users with the same usernames and passwords used with Kerberos 5.

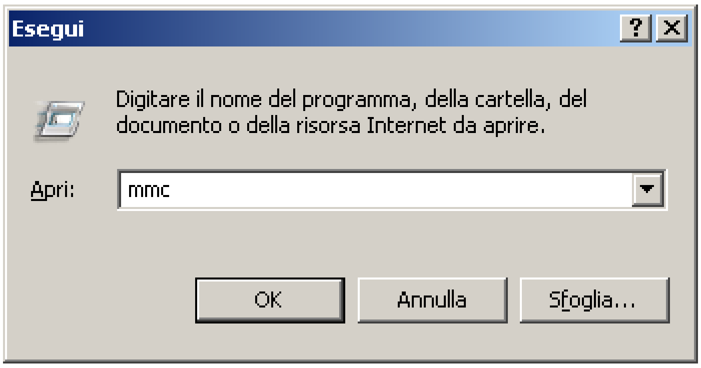
```
Mar 07 23:07,42 SUCCESS: adding new entry "uid=cristian.colombini,ou=People,dc=dominio,dc=lan"
Mar 07 23:07,54 SUCCESS: deleting entry "uid=cristian,ou=People,dc=dominio,dc=lan"
```

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. O f 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 caertifcate:

Open Ms Management Console in Run :

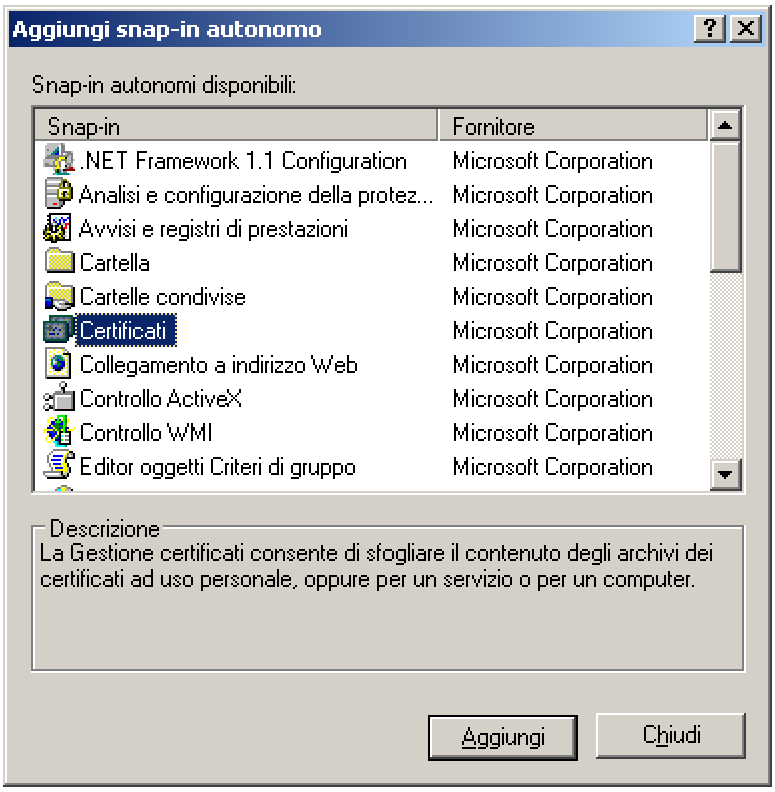


Esegui

Digitare il nome del programma, della cartella, del documento o della risorsa Internet da aprire.

Apri: mmc

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

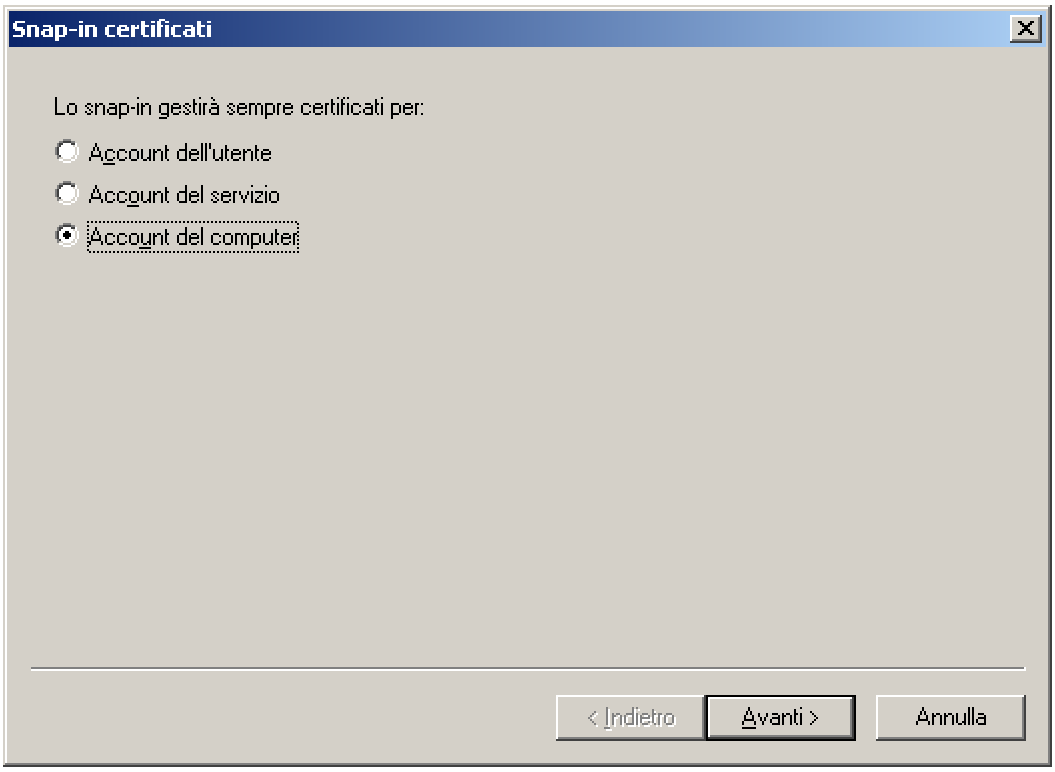


Aggiungi snap-in autonomo

Snap-in autonomi disponibili:

Snap-in	Fornitore
.NET Framework 1.1 Configuration	Microsoft Corporation
Analisi e configurazione della protez...	Microsoft Corporation
Avvisi e registri di prestazioni	Microsoft Corporation
Cartella	Microsoft Corporation
Cartelle condivise	Microsoft Corporation
Certificati	Microsoft Corporation
Collegamento a indirizzo Web	Microsoft Corporation
Controllo ActiveX	Microsoft Corporation
Controllo WMI	Microsoft Corporation
Editor oggetti Criteri di gruppo	Microsoft Corporation

Descrizione
La Gestione certificati consente di sfogliare il contenuto degli archivi dei certificati ad uso personale, oppure per un servizio o per un computer.



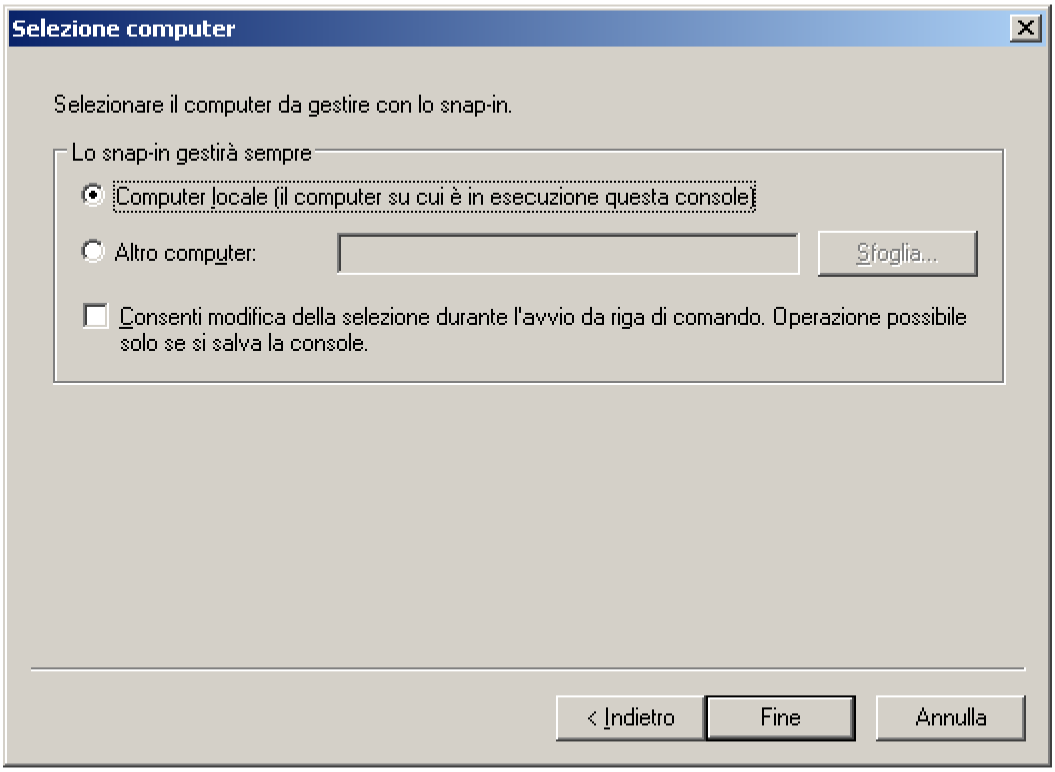
Snap-in certificati

Lo snap-in gestirà sempre certificati per:

○ Account dell'utente

○ Account del servizio

● Account del computer



Selezione computer

Selezionare il computer da gestire con lo snap-in.

Lo snap-in gestirà sempre

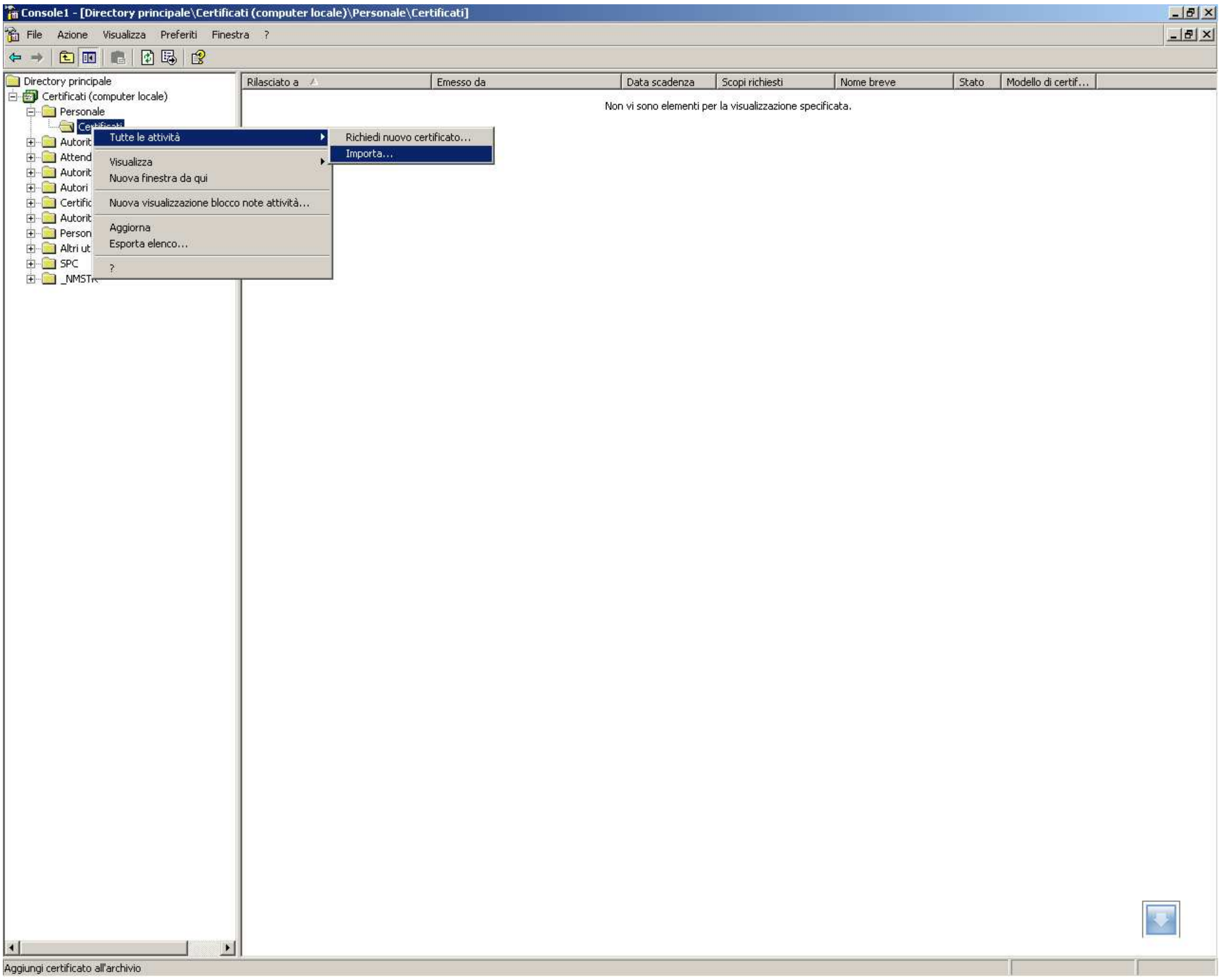
● Computer locale (il computer su cui è in esecuzione questa console)

○ Altro computer:

□ Consenti modifica della selezione durante l'avvio da riga di comando. Operazione possibile solo se si salva la console.

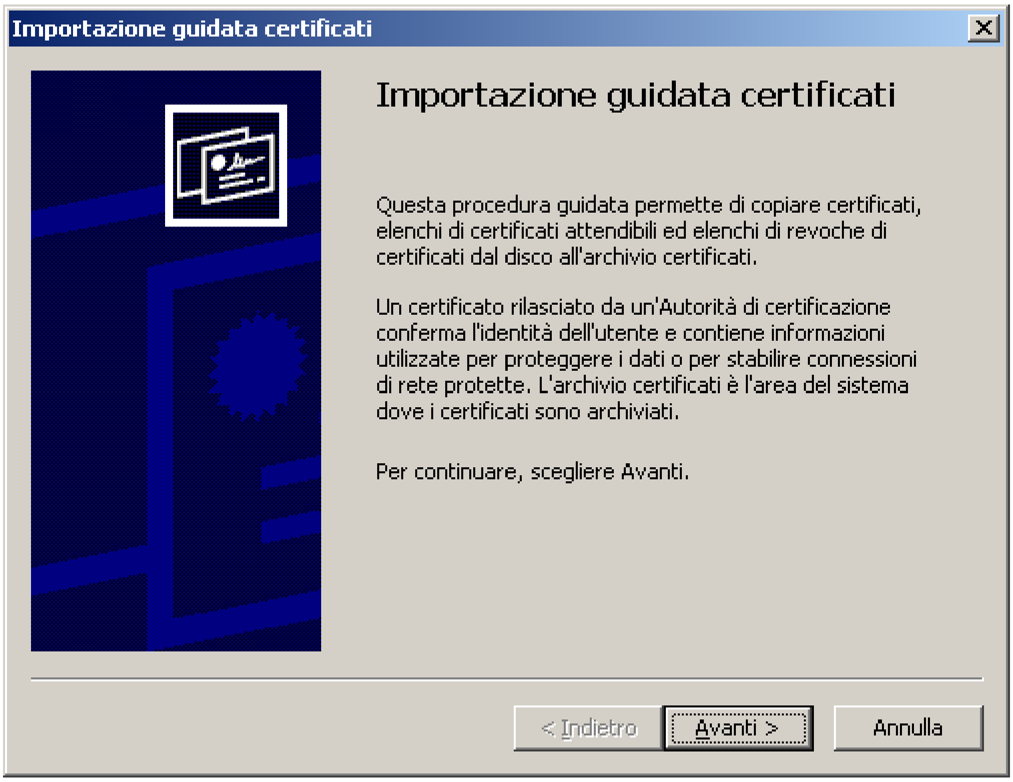
ok.

Richt click on PERSONAL – CERTIFICATES choose IMPORT:



Non vi sono elementi per la visualizzazione specificata.

Aggiungi certificato all'archivio

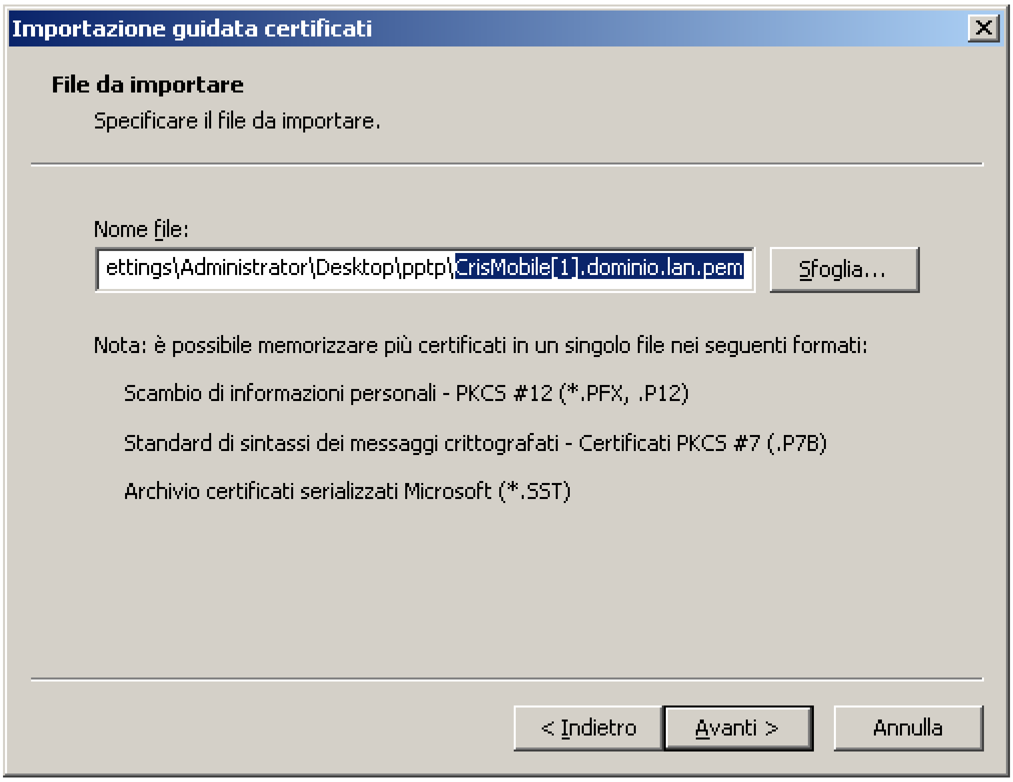


Importazione guidata certificati

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.



Importazione guidata certificati

File da importare

Specificare il file da importare.

Nome file:

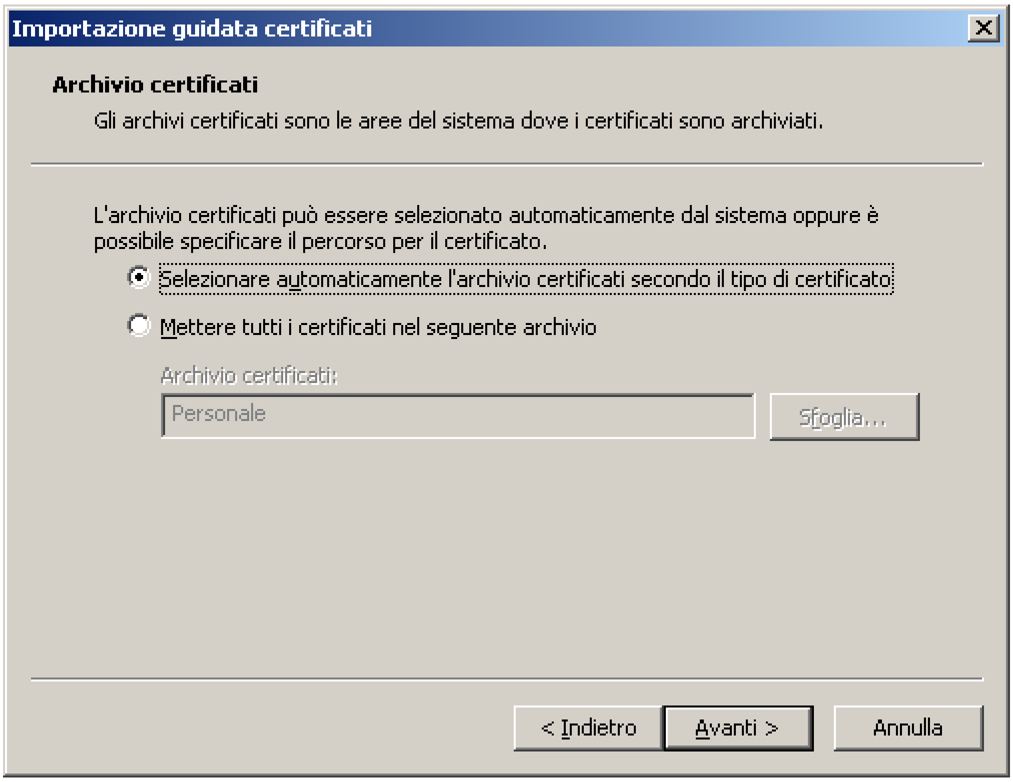
ettings\Administrator\Desktop\pptp\CrisMobile[1].dominio.lan.pem

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)



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.

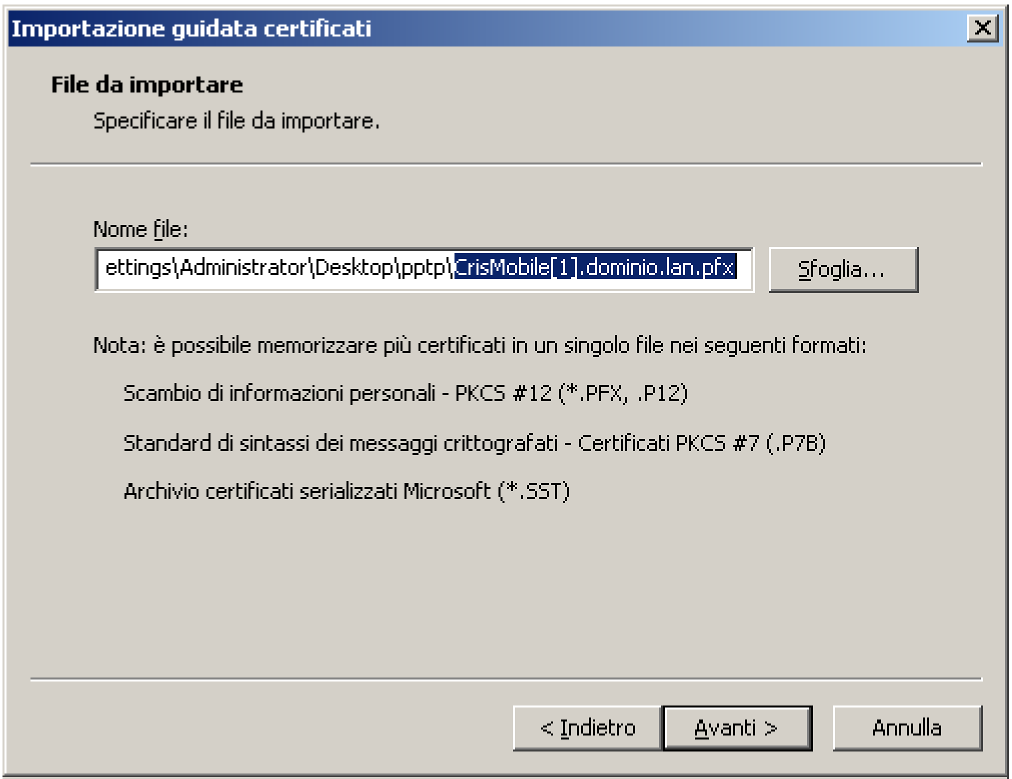
● Selezionare automaticamente l'archivio certificati secondo il tipo di certificato

○ Mettere tutti i certificati nel seguente archivio

Archivio certificati:

Personale

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



Importazione guidata certificati

File da importare

Specificare il file da importare.

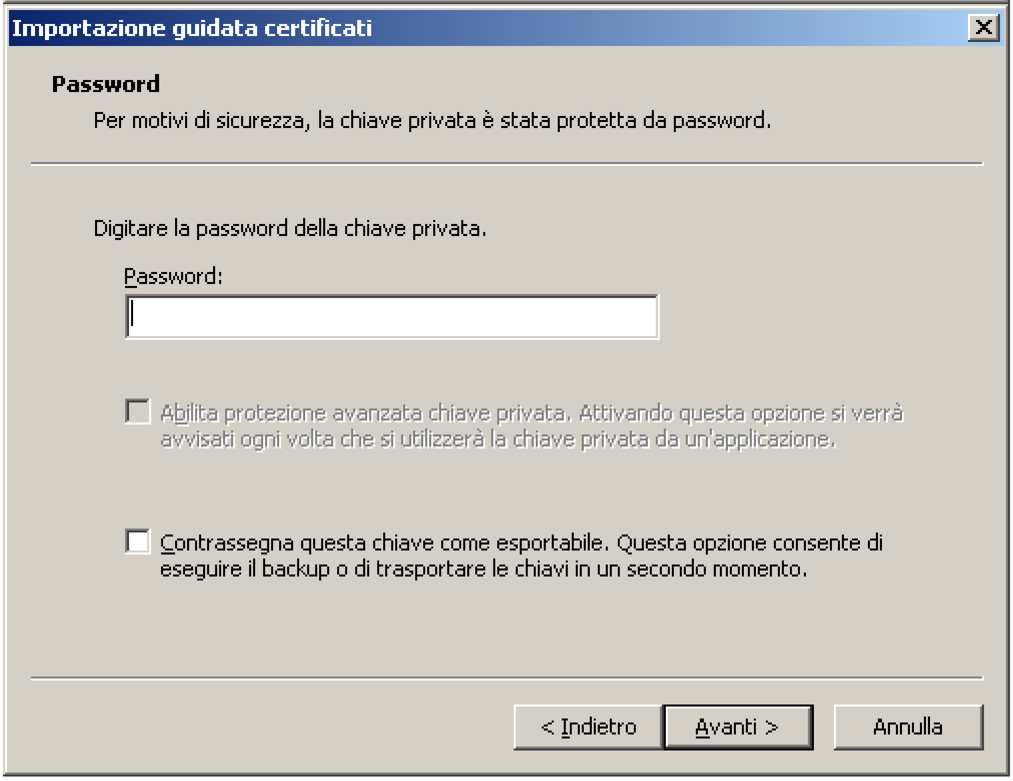
Nome file: ettings\Administrator\Desktop\pptp\CrisMobile[1].dominio.lan.pfx

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)



Importazione guidata certificati

Password

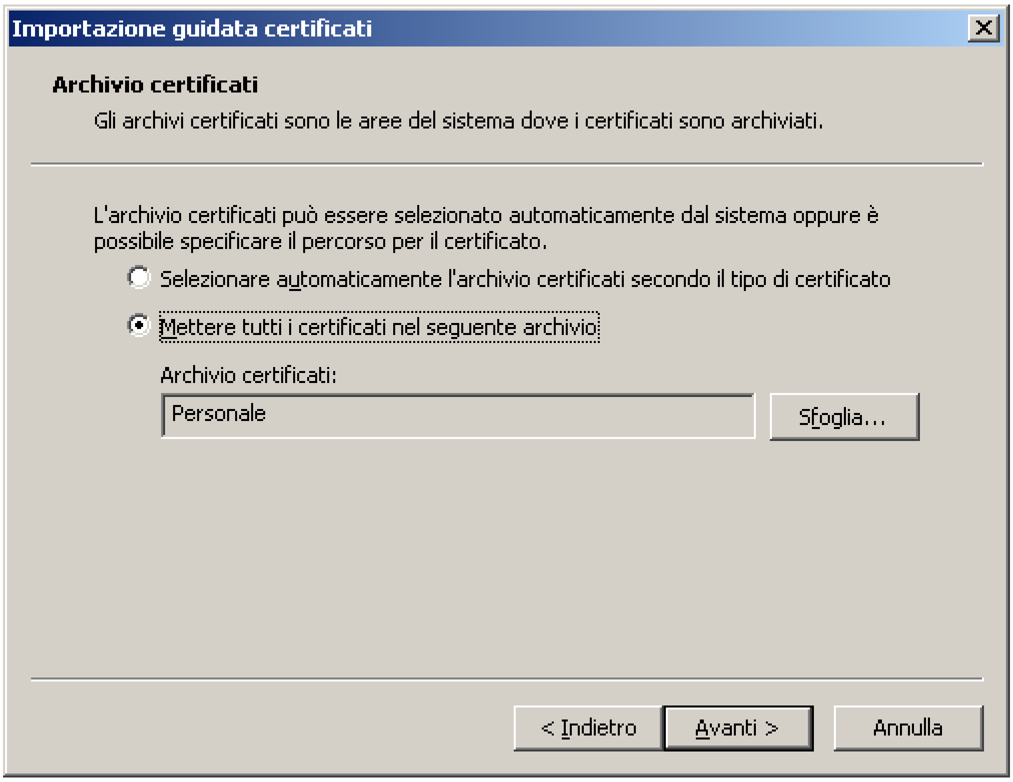
Per motivi di sicurezza, la chiave privata è stata protetta da password.

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.



Importazione guidata certificati

Archivio certificati

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

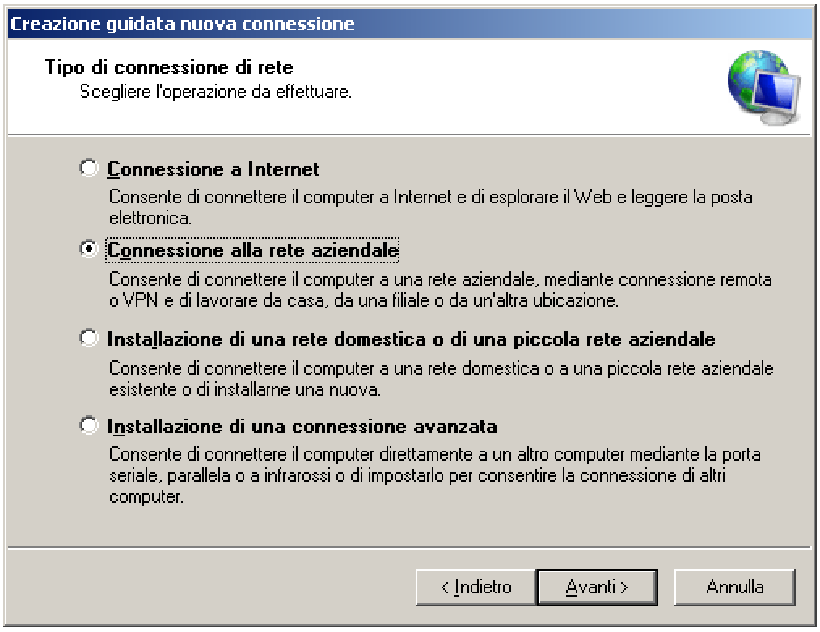
L'archivio certificati può essere selezionato automaticamente dal sistema oppure è possibile specificare il percorso per il certificato.

○ Selezionare automaticamente l'archivio certificati secondo il tipo di certificato

● Mettere tutti i certificati nel seguente archivio

Archivio certificati: Personale

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**

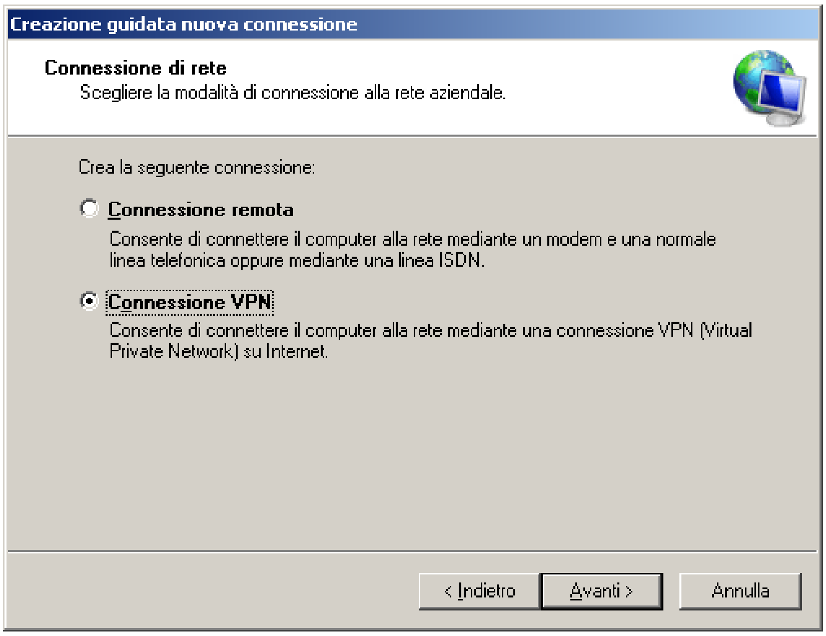
Consente di connettere il computer a una rete aziendale, mediante connessione remota o VPN e di lavorare da casa, da una filiale o da un'altra ubicazione.

○ **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.



Creazione guidata nuova connessione

Connessione di rete

Scegliere la modalità di connessione alla rete aziendale.

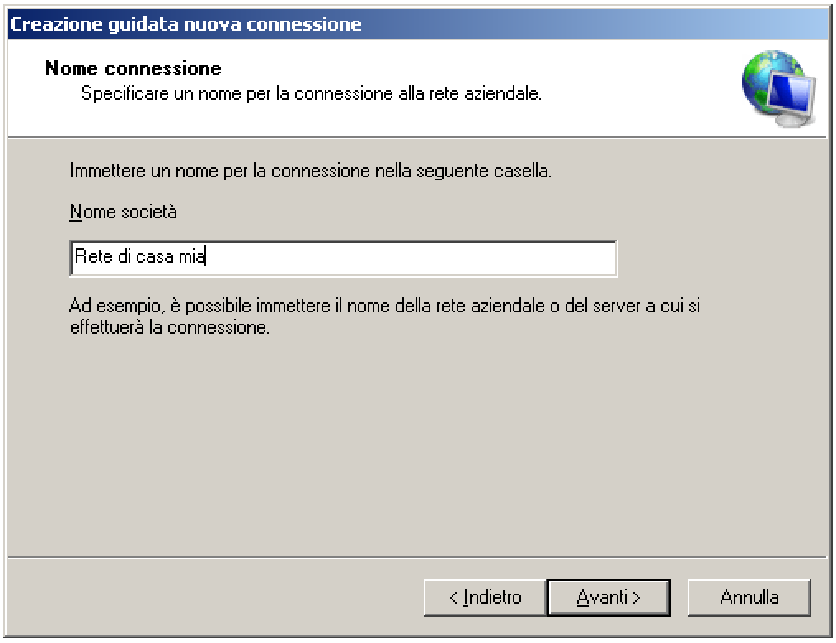
Crea la seguente connessione:

○ **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.



Creazione guidata nuova connessione

Nome connessione

Specificare un nome per la connessione alla rete aziendale.

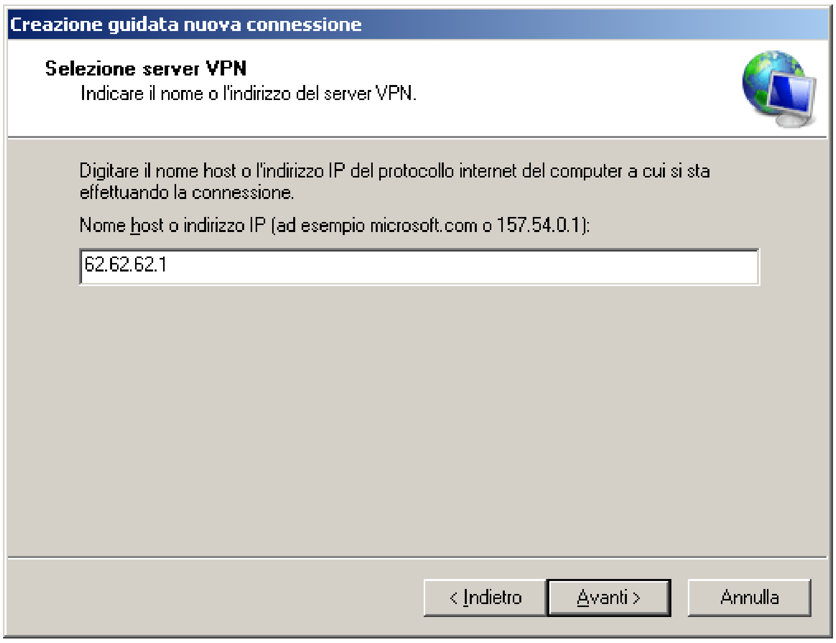
Immettere un nome per la connessione nella seguente casella.

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.

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.



Creazione guidata nuova connessione

Selezione server VPN

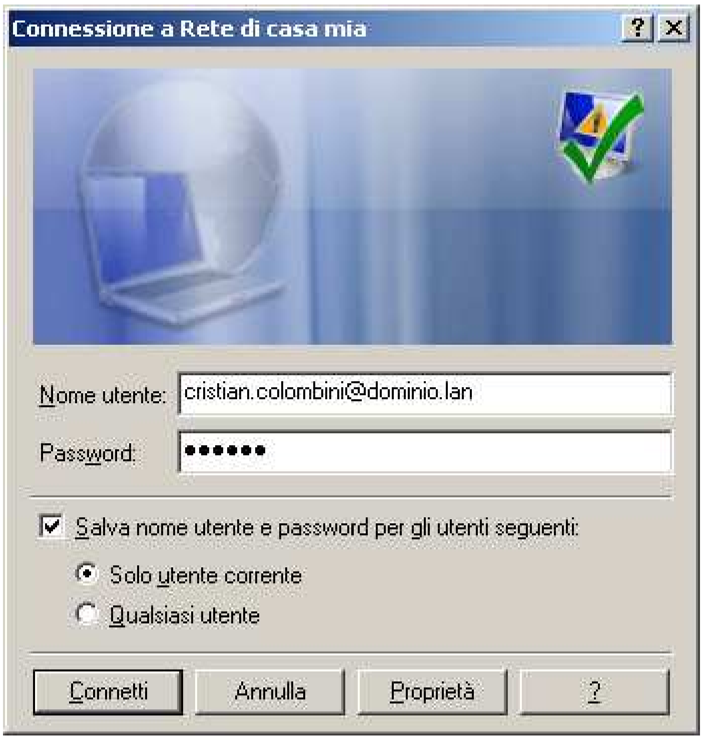
Indicare il nome o l'indirizzo del server VPN.

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

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



Connessione a Rete di casa mia

Nome utente: cristian.colombini@dominio.lan

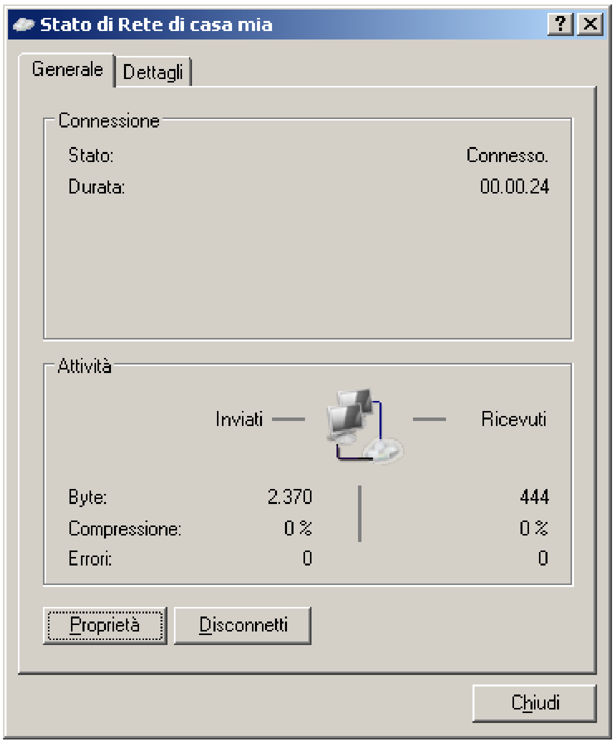
Password: ●●●●●●

☑ Salva nome utente e password per gli utenti seguenti:

● Solo utente corrente

○ Qualsiasi utente

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



Stato di Rete di casa mia

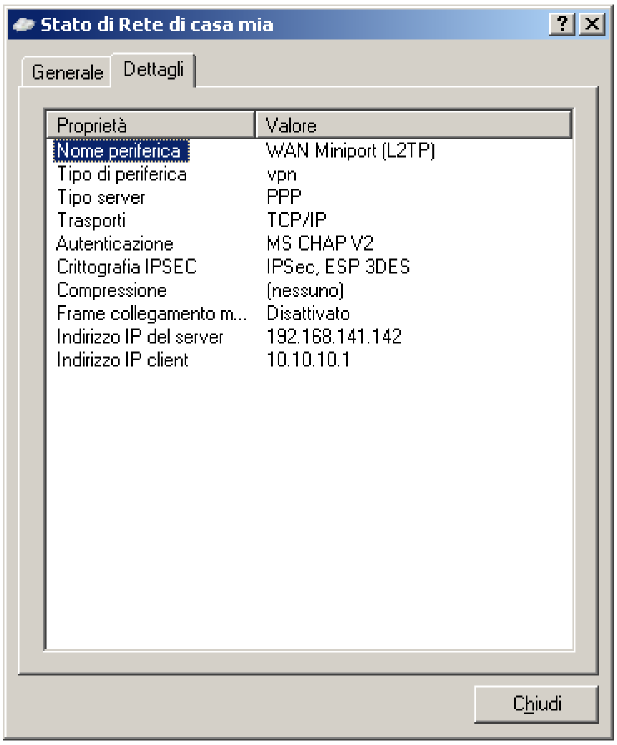
Generale | Dettagli

Connessione

Stato:	Connesso.
Durata:	00.00.24

Attività

	Inviati	Ricevuti
Byte:	2.370	444
Compressione:	0 %	0 %
Errori:	0	0



Stato di Rete di casa mia

Generale | Dettagli

Proprietà	Valore
Nome periferica	WAN Miniport (L2TP)
Tipo di periferica	vpn
Tipo server	PPP
Trasporti	TCP/IP
Autenticazione	MS CHAP V2
Crittografia IPSEC	IPSec, ESP 3DES
Compressione	(nessuno)
Frame collegamento m...	Disattivato
Indirizzo IP del server	192.168.141.142
Indirizzo IP client	10.10.10.1

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)
```

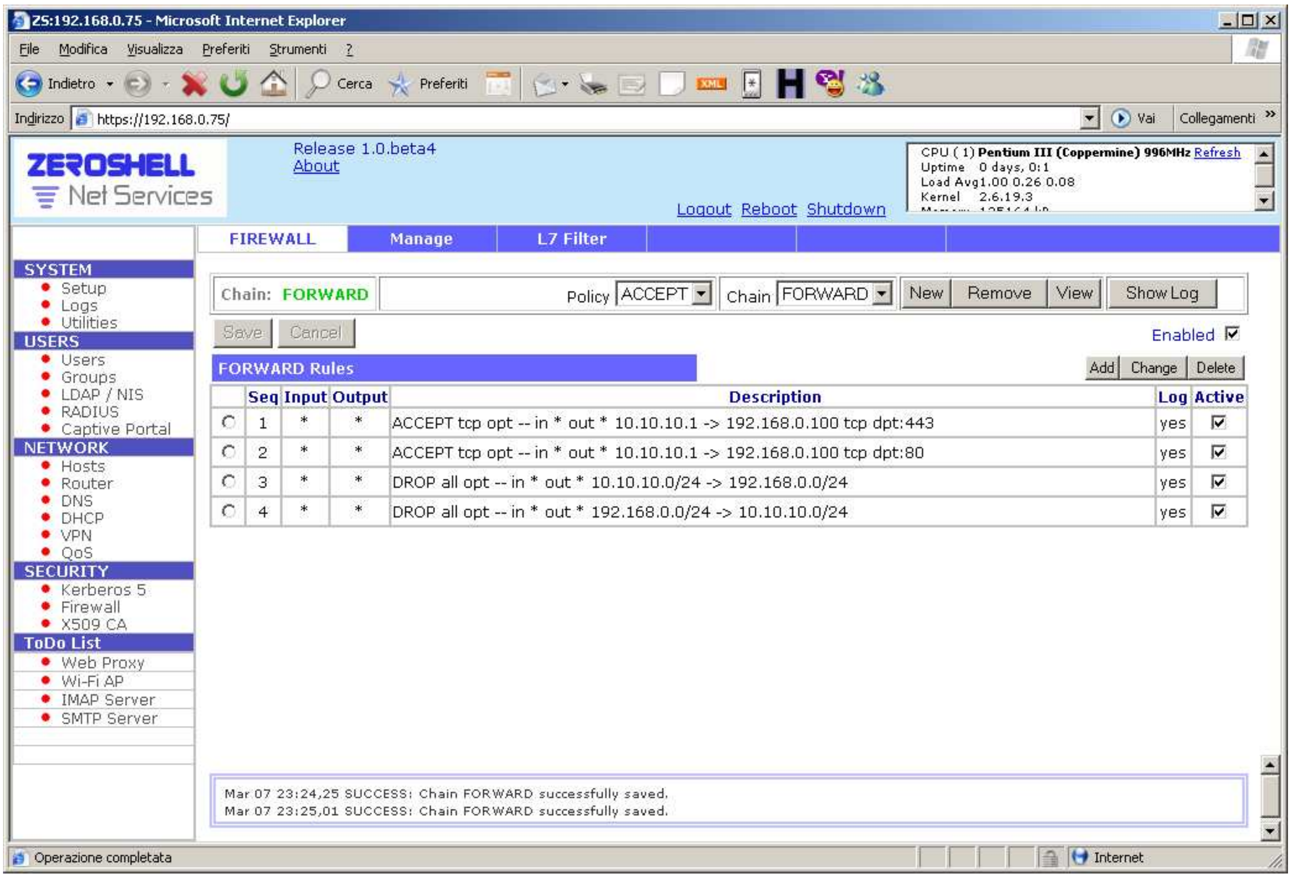
Look at the Radius server logs:

```
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 throug the VPN (see last 2 DROP lines):



Chain: FORWARD

Policy ACCEPT

Chain FORWARD

Enabled ☑

FORWARD Rules

	Seq	Input	Output	Description	Log	Active
○	1	*	*	ACCEPT tcp opt -- in * out * 10.10.10.1 -> 192.168.0.100 tcp dpt:443	yes	☑
○	2	*	*	ACCEPT tcp opt -- in * out * 10.10.10.1 -> 192.168.0.100 tcp dpt:80	yes	☑
○	3	*	*	DROP all opt -- in * out * 10.10.10.0/24 -> 192.168.0.0/24	yes	☑
○	4	*	*	DROP all opt -- in * out * 192.168.0.0/24 -> 10.10.10.0/24	yes	☑

```
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.