

MOBILE VPN con OpenVPN e Zeroshell



Il sistema operativo multifunzionale
creato da Fulvio.Ricciardi@zeroshell.net
www.zeroshell.net

Mobile Vpn in 2 minuti
(Autore: cristiancolombini@libero.it)

Questa breve guida ci consentirà di creare in 2 minuti delle mobile user VPN verso il nostro firewall Zeroshell.

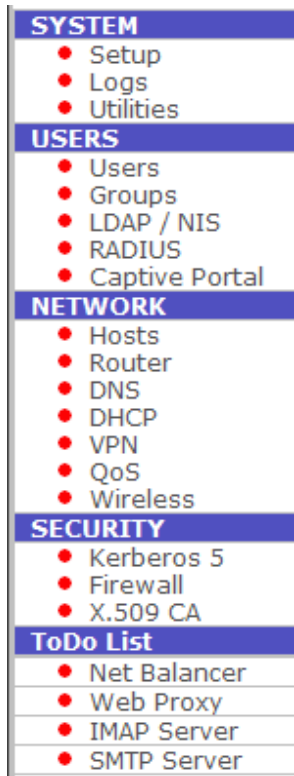
Lo scenario che generalmente si presenta è quello di una sede centrale con dei servizi interni protetti da un firewall (Zeroshell) e di agenti mobili che da internet devono entrare in modo sicuro nella rete e lavorarci come se fossero seduti alle loro scrivanie. Il firewall dovrà essere reperibile in ogni momento su internet; dovrà quindi avere indirizzo ip pubblico statico sulla propria interfaccia esterna oppure dinamico ma registrato con un servizio per Dynamic DNS (esempio: dyndns.org).

I passi da seguire:

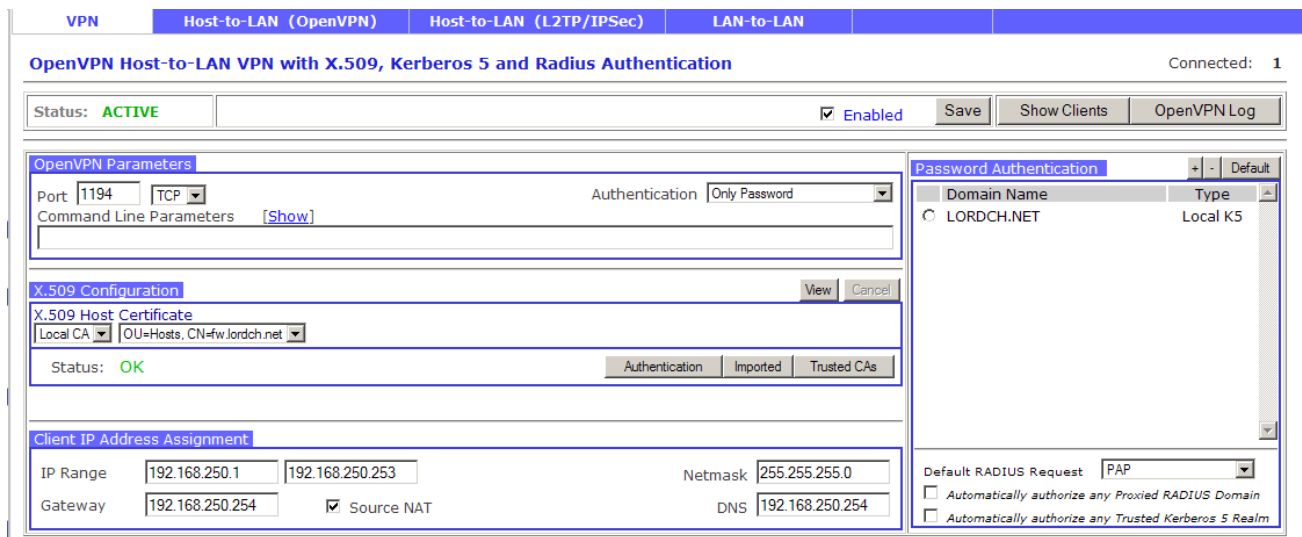
- 1 – Attivare la Host to LAN VPN (OPENVPN) su Zeroshell e creare gli utenti
- 2 – Scaricare il client OpenVPN per il nostro pc con Windows Xp; scaricare dal sito di Zeroshell un file di configurazione base per OpenVPN preconfigurato per il nostro caso; salvare dal nostro Zeroshell il certificato CA.pem

1 - Attivare la Host to LAN VPN (OPENVPN) su Zeroshell e creare gli utenti

Dopo aver preparato il nostro firewall Zeroshell, procedere con la attivazione delle VPN Host to LAN nel menu laterale VPN:



Scegliere poi ENABLE e save:



Una volta fatto ciò, notare che il range di indirizzi da assegnare ai client esterni che si collegano può essere modificato (nel nostro caso il range consta di ben 253 indirizzi ip ed appartiene alla rete

192.168.250.0/24). Si noti anche che OpenVPN parameters è settato su Authentication = Only Password. Tale valore deve restare invariato.

Passiamo ora al menu User dove faremo attenzione a creare gli utenti per l'accesso VPN in modo che contengano delle password forti (contenenti caratteri numerici , alfanumerici e simboli):

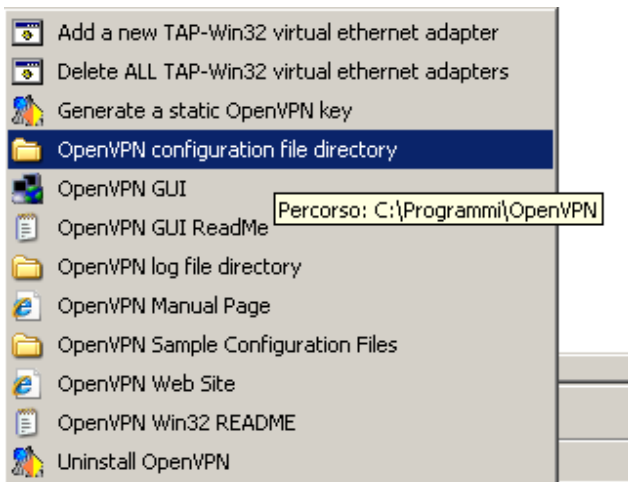
USERS	List	View	Add	Edit	Delete	X509	Kerberos 5
cristian colombini - lordch net (cristian) Submit Reset							
Account							
Username <input type="text" value="cristian"/>		UID <input type="text" value="1"/>		Primary Group <input type="text" value="nobody"/>		GID <input type="text" value="65534"/>	
Home Directory <input type="text" value="/home/cristian"/>				Default Shell <input type="radio"/> bash <input checked="" type="radio"/> sh <input type="radio"/> tcsh <input type="radio"/> other <input type="text" value="/bin/sh"/>			
User Information							
Firstname <input type="text" value="cristian"/>		Lastname <input type="text" value="colombini"/>		Organization <input type="text" value="lordch net"/>			
Description <input type="text" value="cristian colombini - lordch net"/>			E-Mail <input type="text" value="cristiancolombini@libero.it"/>		Phone <input type="text" value="?"/>		
User Password				Enabled Services			
Password <input type="password"/>				Kerberos 5 Authentication <input checked="" type="checkbox"/>			
Confirm <input type="password"/>				Host-to-Lan VPN (L2TP/IPsec) <input checked="" type="checkbox"/>			
				802.1X Access (VLAN <input type="text"/>) <input checked="" type="checkbox"/>			

Una volta creato l'utente possiamo procedere con la configurazione del client che si dovrà collegare.

2 – Scaricare il client OpenVPN per il nostro pc con Windows Xp; scaricare dal sito di Zeroshell un file di configurazione base per OpenVPN preconfigurato per il nostro caso; salvare dal nostro Zeroshell il certificato CA.pem

Dal sito ufficiale <http://openvpn.se/download.html> prelevare l'ultima versione disponibile per MS Windows e procedere con l'installazione standard sul client.

Dal sito ufficiale di Zeroshell procurarsi il file di configurazione base di OpenVPN: <http://www.zeroshell.net/download/zeroshell.ovpn>. Salvarlo nella cartella di configurazione di OpenVPN:



Dal nostro firewall Zeroshell scaricare il certificato CA.pem cliccando su CA :



X.509 certificates
[CA](#) [Users](#) [Hosts](#) [CRL](#)

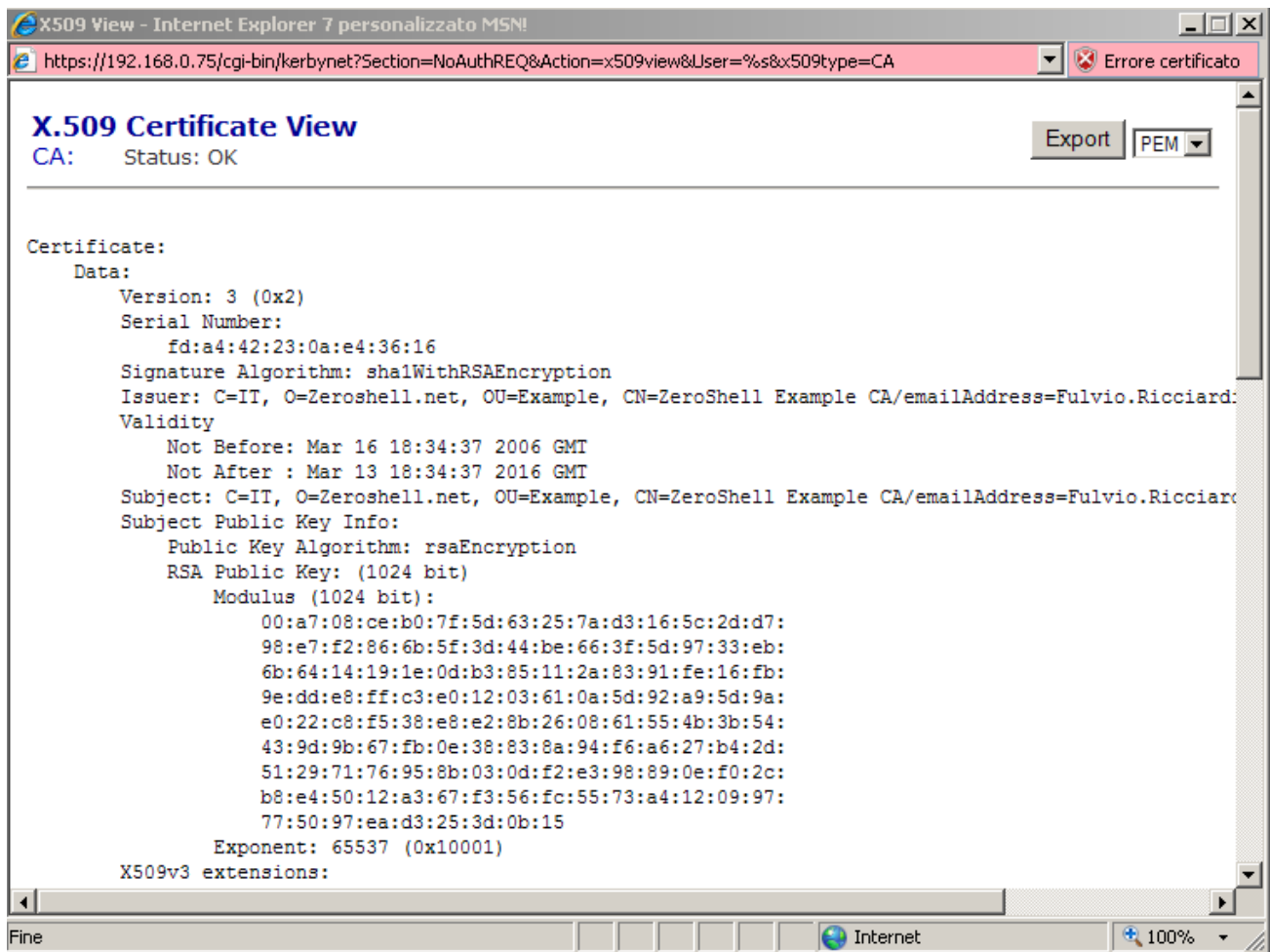
Username

Password

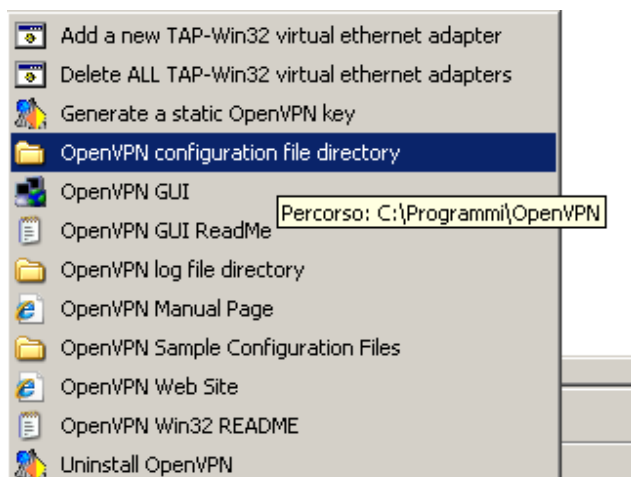
Login

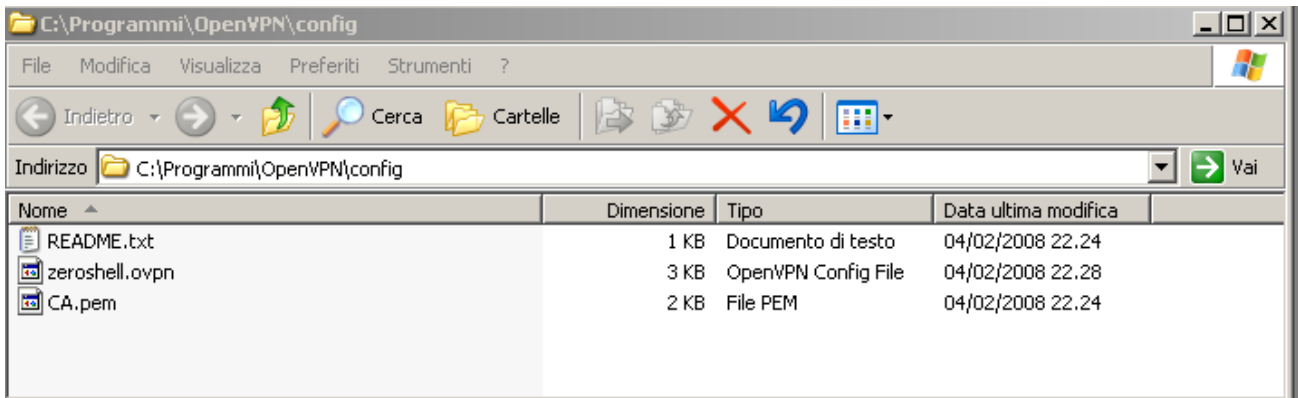
Password

ed esportarlo come segue:

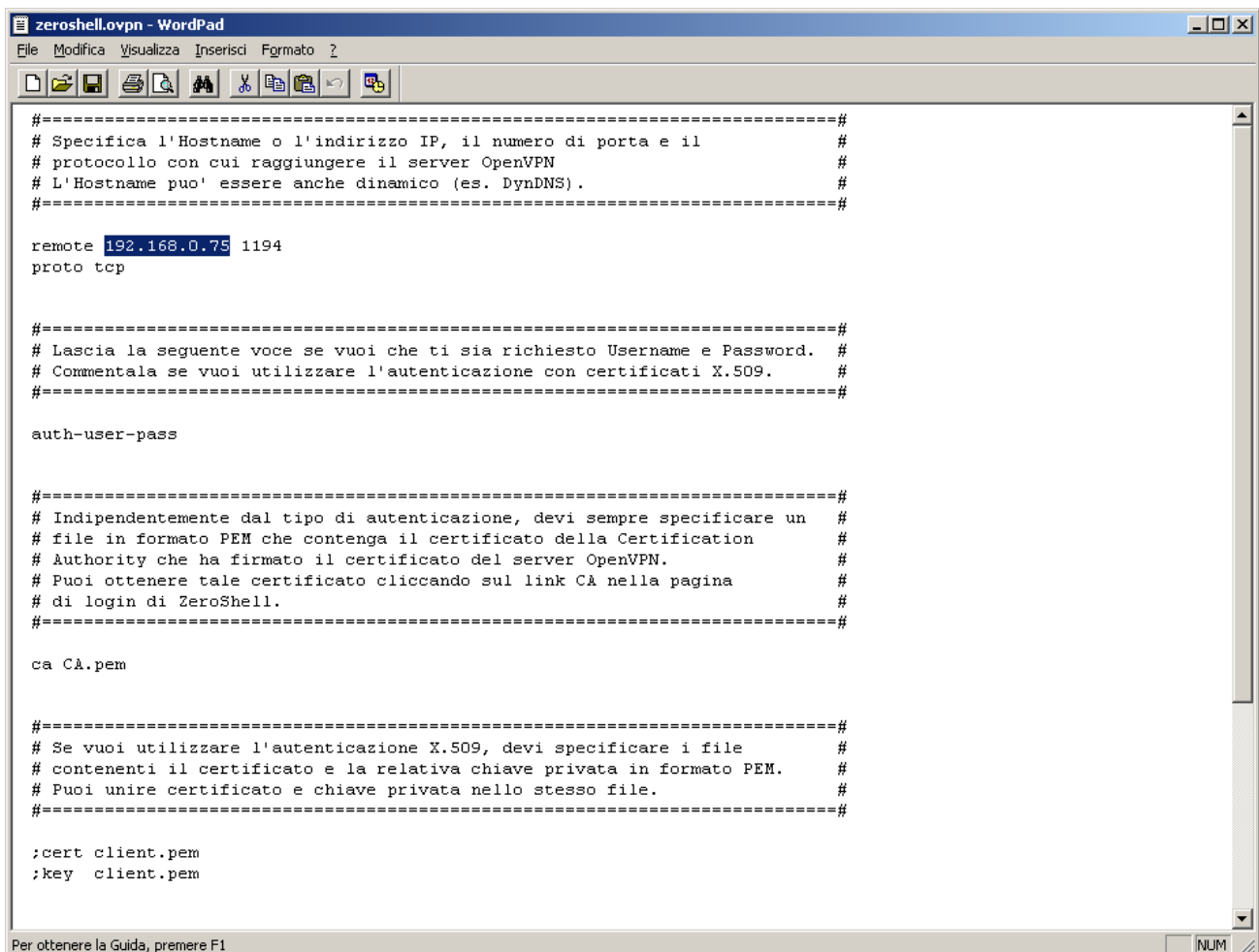


Inserire anche questo file nella cartella di configurazione di OpenVPN:






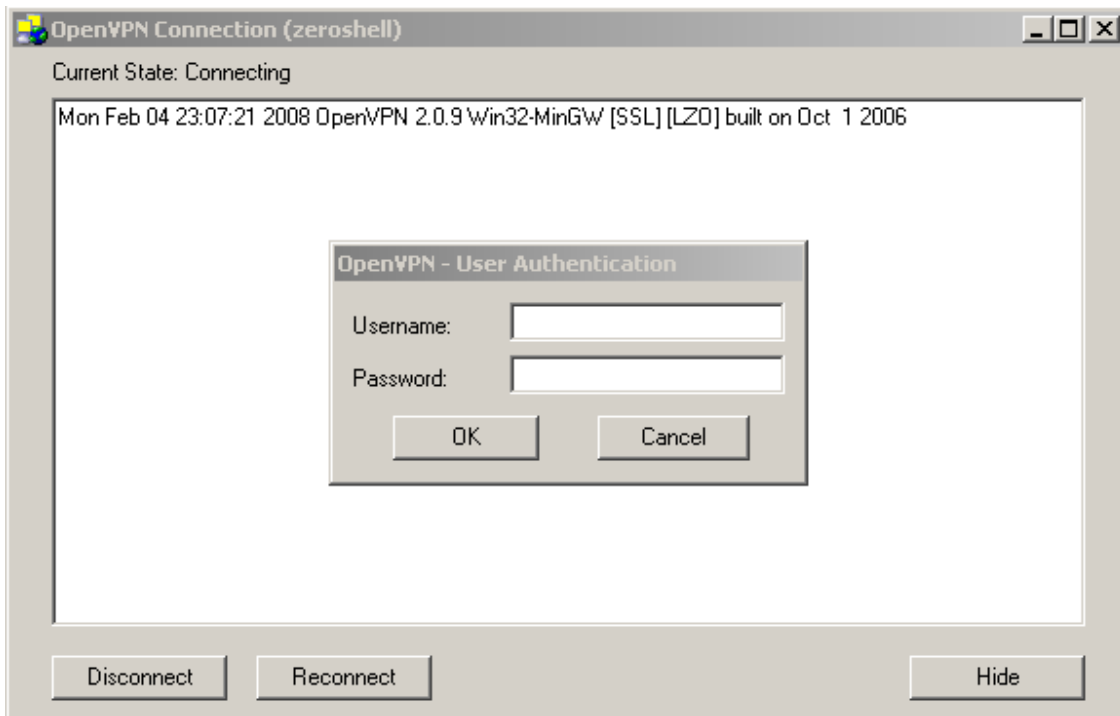
A questo punto modificare con wordpad di windows il file zeroshell.ovpn nella parte relativa all'indirizzo ip del firewall Zeroshell. Inserirvi l'ip pubblico statico o il nome DNS (per esempio nel caso di utilizzo di dyndns) assegnato all'interfaccia esterna del firewall:



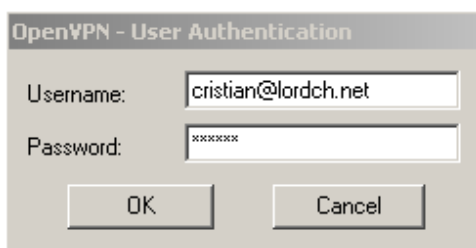
(Nel mio esempio di laboratorio è 192.168.0.75). Salvare il file.

Stabilire ora la connessione VPN fra il client ed il firewall. Fare clic col tasto destro sull'icona vicino all'orologio:  e scegliere CONNECT.

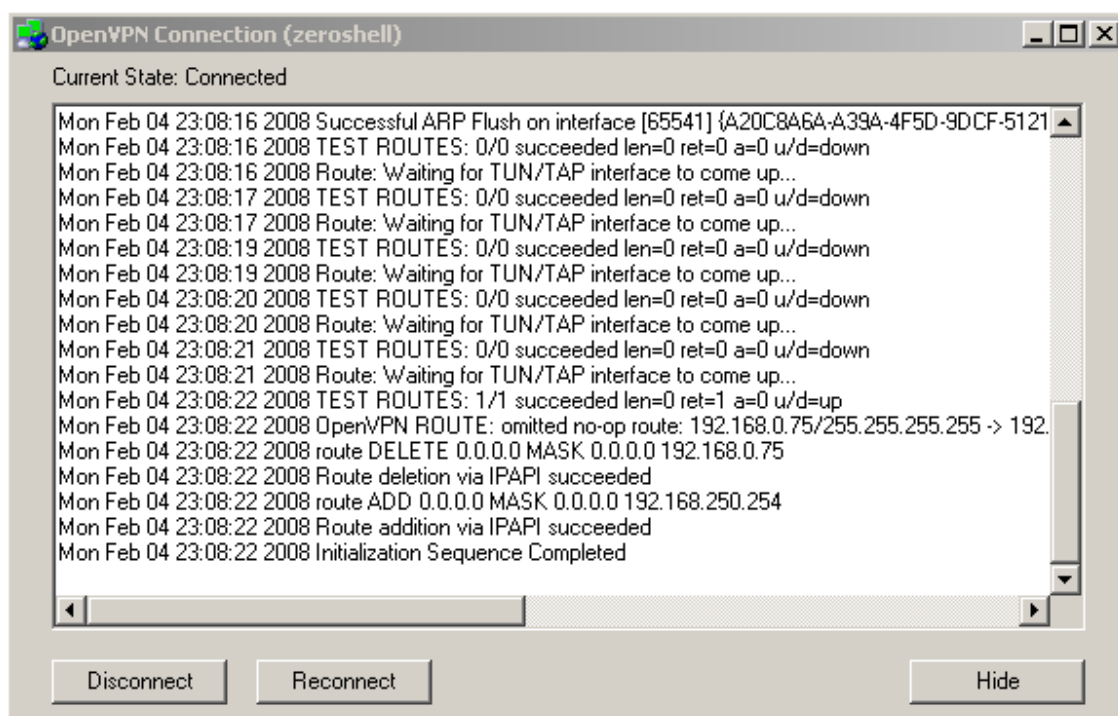
Ci verranno chieste l'utenza e la password dell'utente creato che si deve collegare:



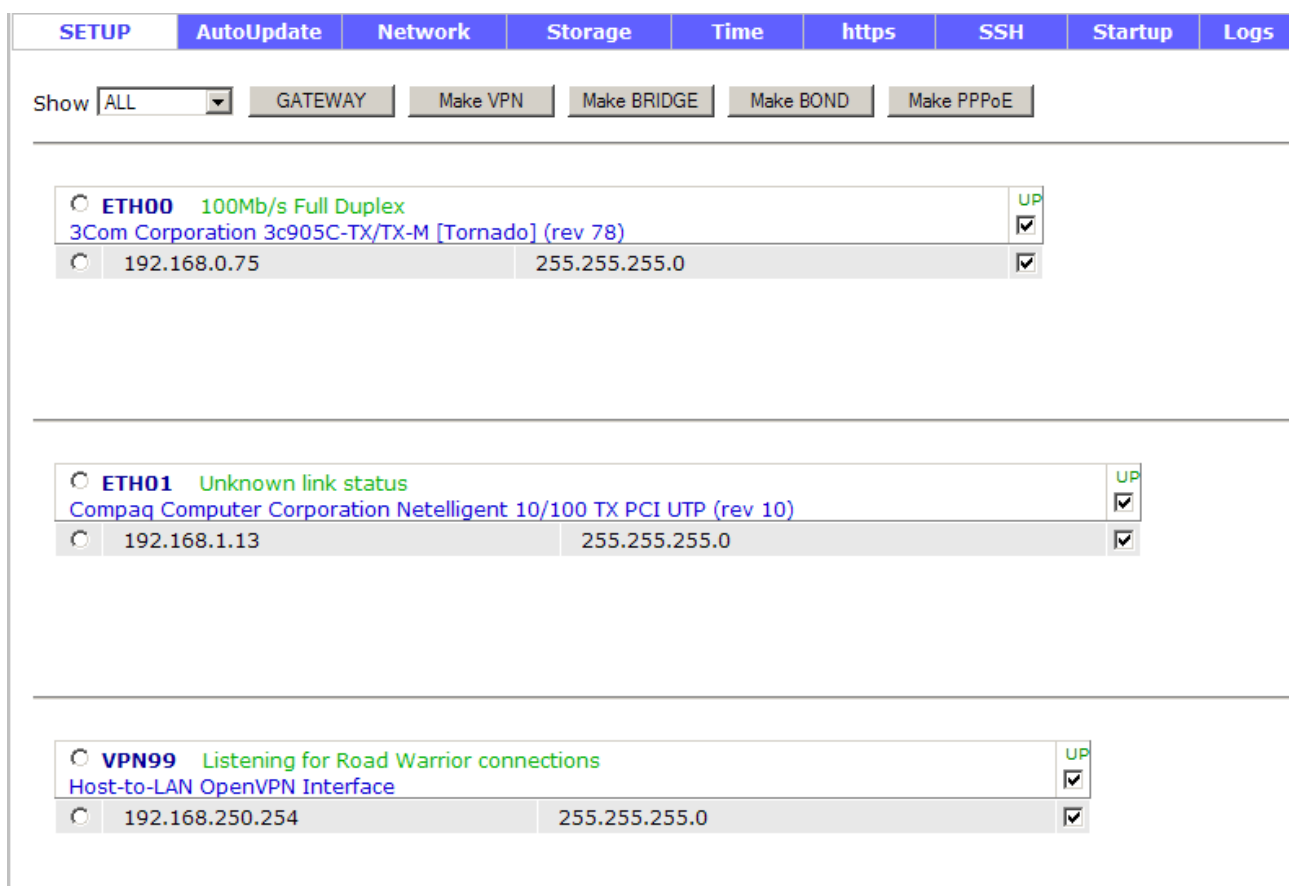
Compilare attentamente i campi includendo il nome del dominio dopo la @:



Vedremo che la connessione verrà stabilita e che la default route (route add 0.0.0.0 MASK: 0.0.0.0) del client sarà indirizzata sull'interfaccia virtuale dell'VPN di Zeroshell (nel nostro caso all'IP 192.168.250.254 VPN99):



Sul firewall si attiverà l'interfaccia virtuale VPN99:



Verifichiamo i logs di connessione della mobile vpn sul firewall:

The screenshot displays a web-based VPN configuration interface. At the top, there are tabs for 'VPN', 'Host-to-LAN (OpenVPN)', 'Host-to-LAN (L2TP/IPSec)', and 'LAN-to-LAN'. The 'Host-to-LAN (OpenVPN)' tab is selected, showing the configuration for 'OpenVPN Host-to-LAN VPN with X.509, Kerberos 5 and Radius Authentication'. The status is 'ACTIVE' and the VPN is 'Enabled'. On the left, there are sections for 'OpenVPN Parameters' (Port: 1194, Protocol: TCP), 'X.509 Configuration' (Local CA, OU=Hosts, CN=fw.lordch.net, Status: OK), and 'Client IP Address Assignment' (IP Range: 192.168.250.1, Gateway: 192.168.250.254). The main area is a 'LOG VIEWER' window showing a list of log entries for the 'fw (Local)' host and 'VPN99_H2L' section. The logs show the process of establishing and resetting connections for user 'cristian@lordch.net'.

LOG VIEWER

Time	Host	Section	Filter
22:55:00	fw (Local)	VPN99_H2L	
22:55:00			TCPv4_SERVER link local: [undef]
22:55:00			TCPv4_SERVER link remote: 192.168.0.13:2911
22:55:00			192.168.0.13:2911 [cristian@LORDCH.NET] Trying Kerberos 5 (Local KDC) authentication
22:55:00			192.168.0.13:2911 [cristian@LORDCH.NET] Successfully authenticated
22:55:00			192.168.0.13:2911 [cristian@lordch.net] Peer Connection Initiated with 192.168.0.13:2911
22:55:00			192.168.0.13:2911 [cristian@lordch.net] Virtual IP automatically assigned: 192.168.250.1
22:58:16			cristian@lordch.net/192.168.0.13:2911 Connection reset, restarting [-1]
22:58:16			192.168.0.13:2911 [cristian@lordch.net] Client disconnected
22:58:45			Re-using SSL/TLS context
22:58:45			LZO compression initialized
22:58:45			TCP connection established with 192.168.0.13:2951
22:58:45			TCPv4_SERVER link local: [undef]
22:58:45			TCPv4_SERVER link remote: 192.168.0.13:2951
22:58:45			192.168.0.13:2951 [cristian@LORDCH.NET] Trying Kerberos 5 (Local KDC) authentication
22:58:45			192.168.0.13:2951 [cristian@LORDCH.NET] Successfully authenticated
22:58:45			192.168.0.13:2951 [cristian@lordch.net] Peer Connection Initiated with 192.168.0.13:2951
22:58:45			192.168.0.13:2951 [cristian@lordch.net] Virtual IP automatically assigned: 192.168.250.1
22:59:26			cristian@lordch.net/192.168.0.13:2951 Connection reset, restarting [-1]
22:59:26			192.168.0.13:2951 [cristian@lordch.net] Client disconnected
23:00:30			Re-using SSL/TLS context
23:00:30			LZO compression initialized
23:00:30			TCP connection established with 192.168.0.13:2984
23:00:30			TCPv4_SERVER link local: [undef]
23:00:30			TCPv4_SERVER link remote: 192.168.0.13:2984
23:00:30			192.168.0.13:2984 [cristian@LORDCH.NET] Trying Kerberos 5 (Local KDC) authentication
23:00:30			192.168.0.13:2984 [cristian@LORDCH.NET] Successfully authenticated
23:00:30			192.168.0.13:2984 [cristian@lordch.net] Peer Connection Initiated with 192.168.0.13:2984
23:00:30			192.168.0.13:2984 [cristian@lordch.net] Virtual IP automatically assigned: 192.168.250.1