

MOBILE VPN between OpenVPN and Zeroshell



The multifunctional OS created by

Fulvio.Ricciardi@zeroshell.net

Mobile VPN in 2 minutes

(Author: cristiancolombini@libero.it)

This short guide will lead us to create mobile user vpn between our Zeroshell firewall and OpenVPN clients.

Usually we have to connect to our office through internet, to access our internal services as if we were working at our desk. The office network is protected by a Zeroshell firewall; its external interface must be reachable from internet everytime we need. So we need to have a public static ip address on external interface of Zeroshell or at least (if we have not a public static ip address) we need a service for Dynamic DNS (such as dyndns.org).

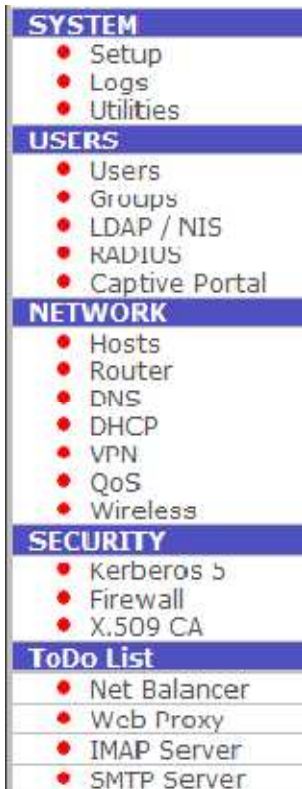
These are the steps to be followed:

1 – Activate Host to lan VPN (OpenVPN) on Zeroshell and create user

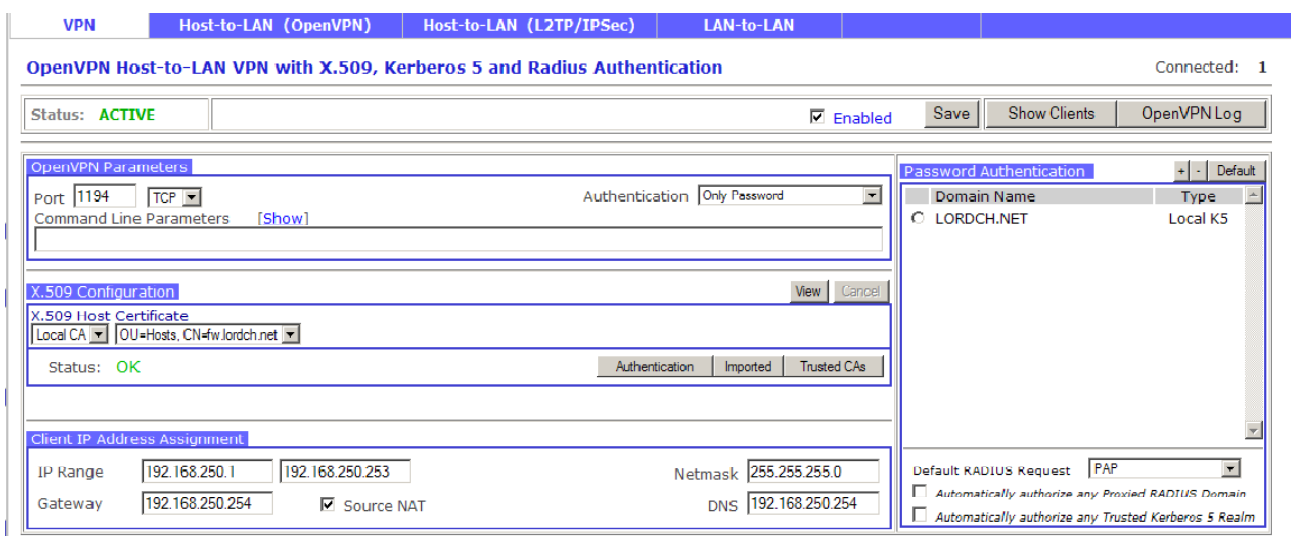
2 – Obtain OpenVPN software for Ms Windows Xp from OpenVPN official website; download Zeroshell preconfigured opvn file; save ca.pem from our firewall; configure our ms client

1 - Activate Host to lan VPN (OpenVPN) on Zeroshell and create user

Once we have done the first configuration of our firewall, we have to activate the Host to Lan VPN choosing VPN left menu:



Click ENABLE and SAVE:



You can now see that assigned ip address network to external clients that will connect through our VPN is 192.168.250.0/24 (253 hosts available). Please notice that OpenVPN parameters is Authentication = OnlyPassword (it must be so).

Click now left menu on User: here we can create mobile vpn users; please set strong password:

USERS	List	View	Add	Edit	Delete	X509	Kerberos 5
crislian colombini - lordch net (crislian) Submit Reset							
Account							
Username <input type="text" value="crislian"/>		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/crislian"/>				Default Shell <input type="radio" value="bash"/> bash <input checked="" type="radio" value="sh"/> sh <input type="radio" value="tcsh"/> tcsh <input type="radio" value="other"/> other <input type="text" value="/bin/sh"/>			
User Information							
Firstname <input type="text" value="crislian"/>		Lastname <input type="text" value="colombini"/>		Organization <input type="text" value="lordch net"/>			
Description <input type="text" value="crislian colombini - lordch net"/>			E-Mail <input type="text" value="crisliancolombini@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"/>			

We can now configure the client pc.

2 – Obtain OpenVPN software for Ms Windows Xp from OpenVPN official website; download Zeroshell preconfigured opvn file; save ca.pem from our firewall; configure our ms client

Download from official website the OPENVPN Software: <http://openvpn.se/download.html> .
Install it on your ms windows pc.

From Zeroshell official website download the preconfigured OpenVPN file:
<http://www.zeroshell.net/download/zeroshell.ovpn>. Save it in configuration folder of OpenVPN:



From our Zeroshell firewall download the CA certificate CA.pem:

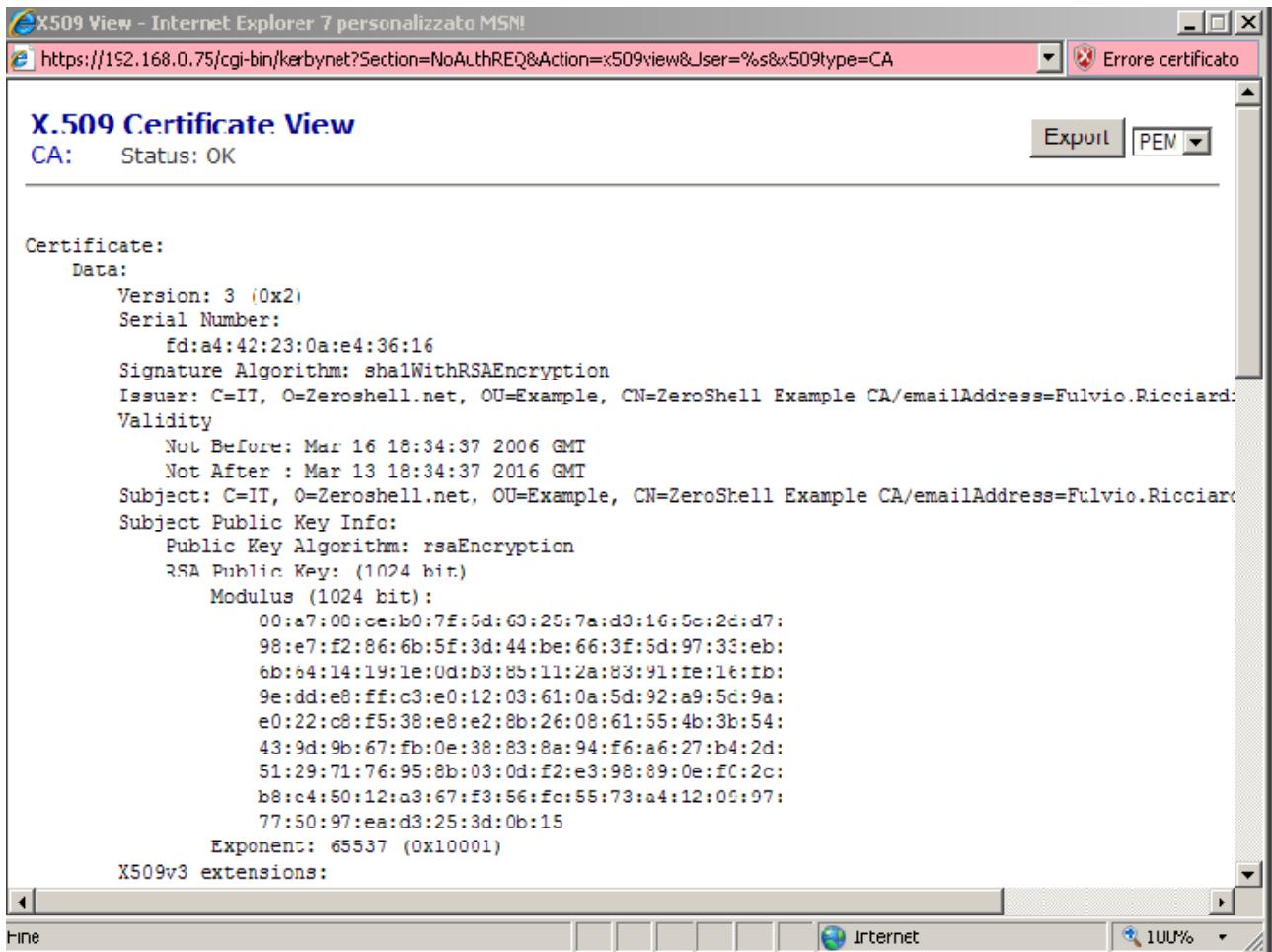


X.509 certificates
[CA](#) [Users](#) [Hosts](#) [CRL](#)

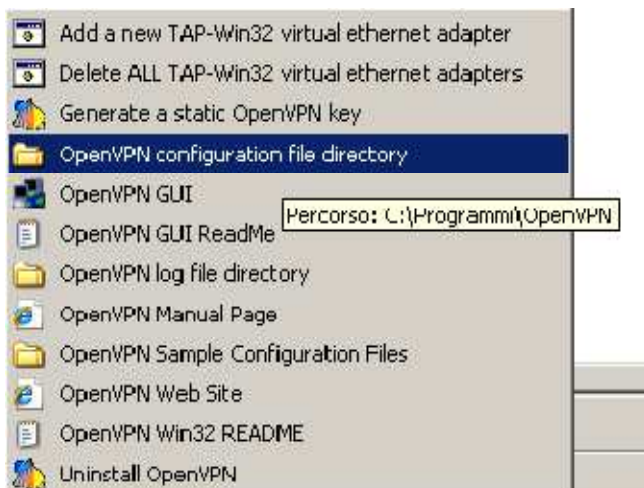
Username

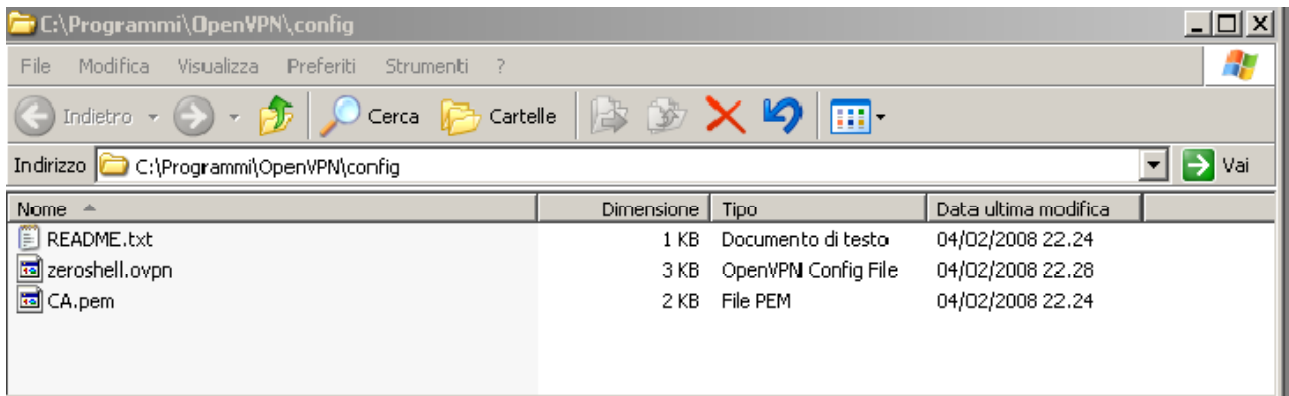
Password

And export it:

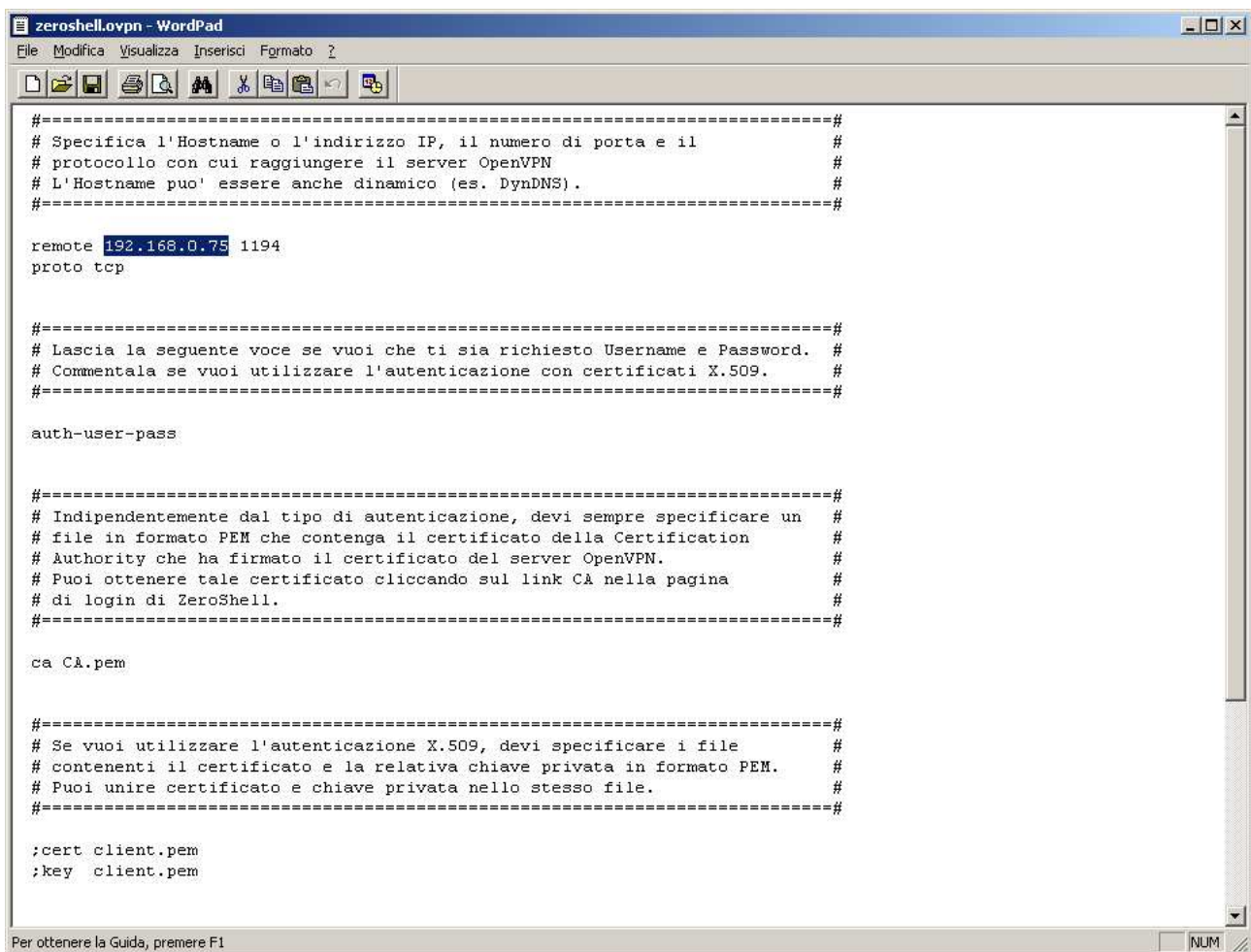


Copy also this file in the configuration folder of OpenVpn:




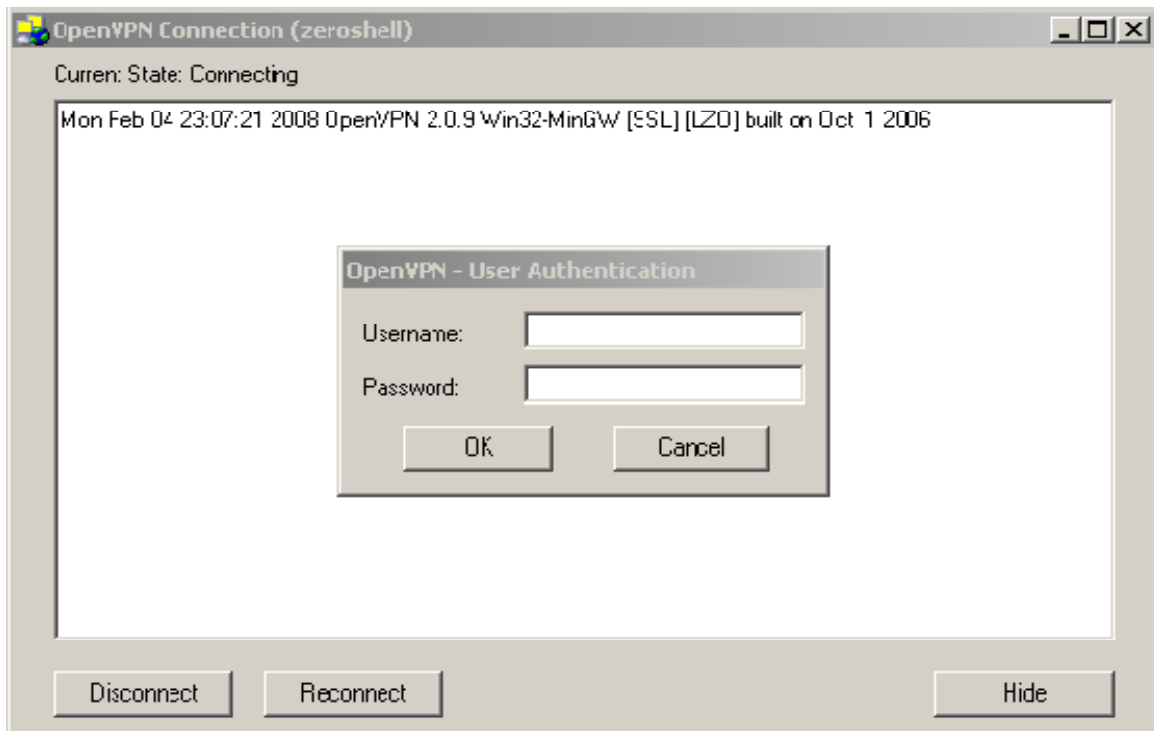


Using ms wordpad you can now edit and modify the zeroshell.ovpn file. Set the public ip address of your external interface firewall or dns name (if you use DynDNS.org):

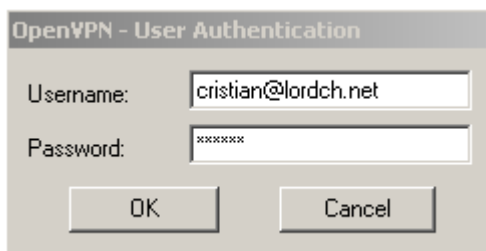


(In my example I have the laboratory test ip: 192.168.0.75 on my external interface). Save it.

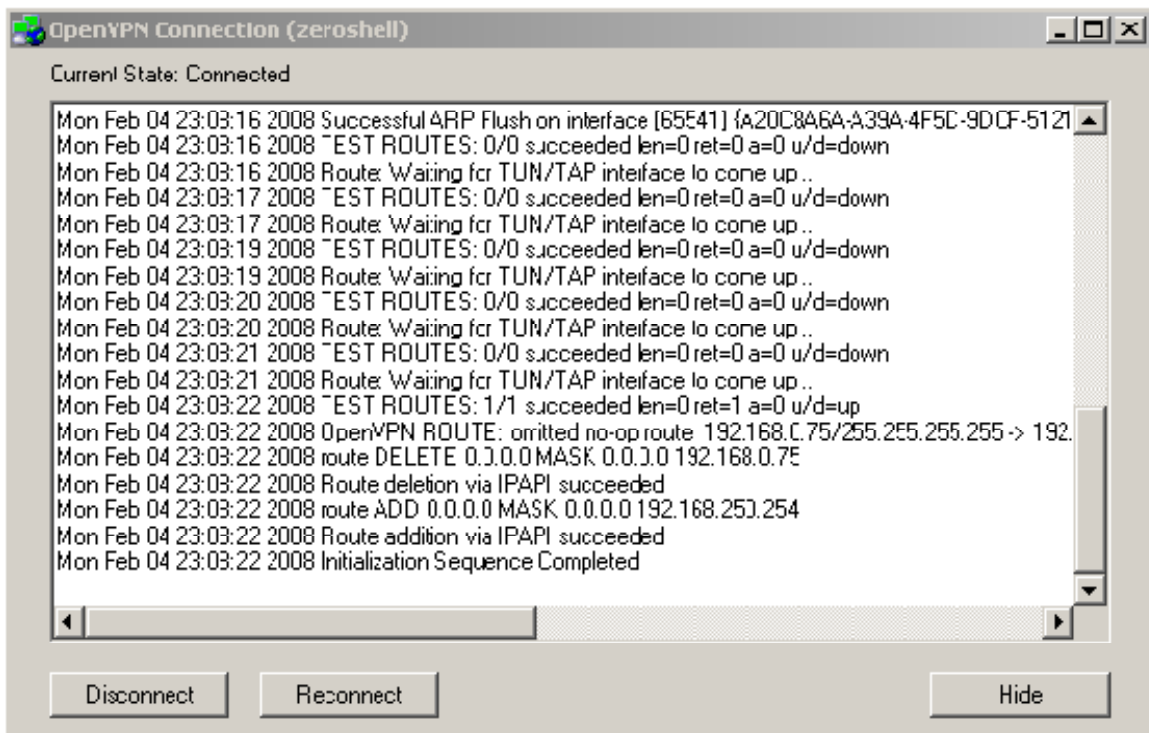
Open now your vpn connection from your client, right click the OpenVPN icon  near your windows clock and choose CONNECT. Type the user and its password:



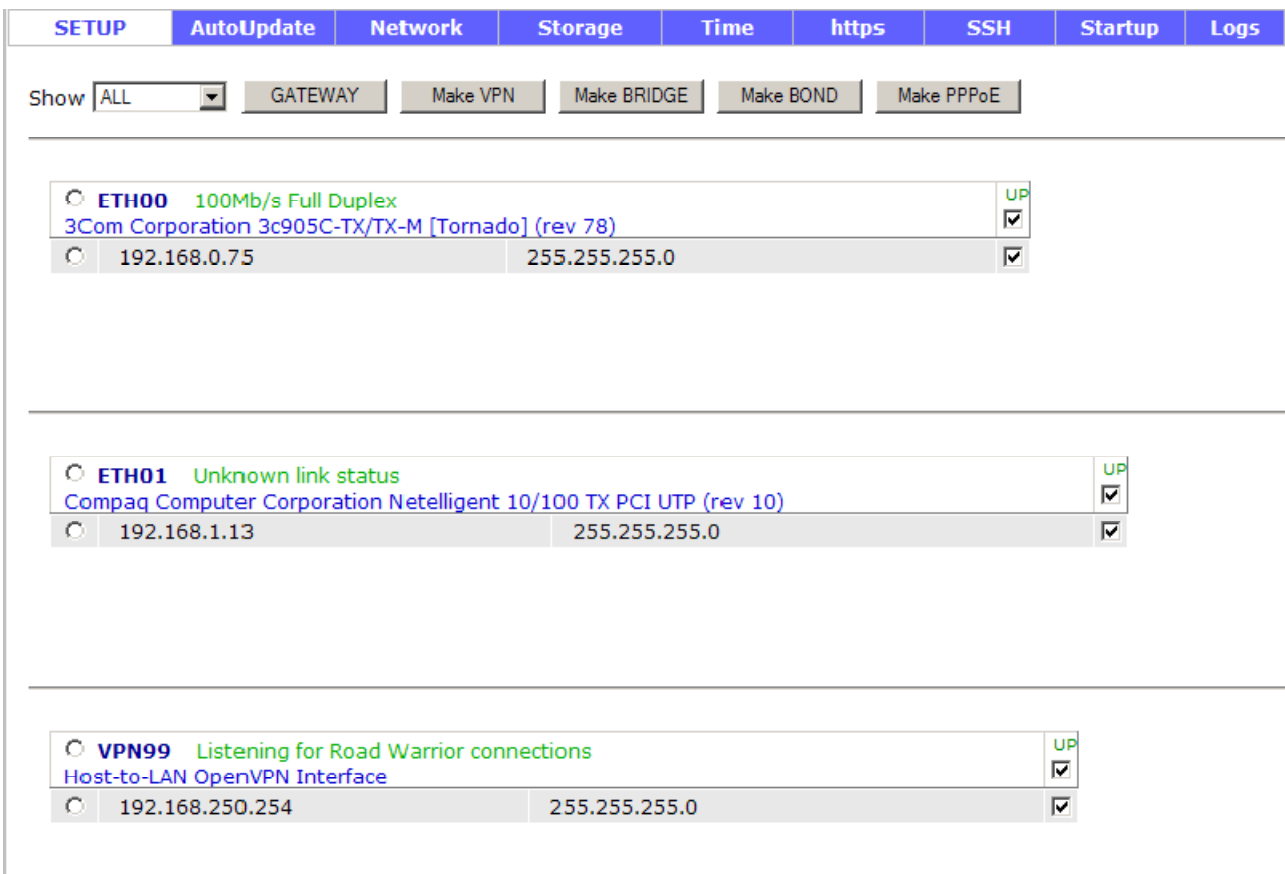
Pay attention typing also the domain following the @ symbol:



We are now going to see that the connection is established and that the default route (route add 0.0.0.0 MASK: 0.0.0.0) has its own gateway: the virtual interface on our Zeroshell firewall (192.168.250.254 VPN99):



Check that the virtual interface VPN99 on the firewall is active:



Check the logs of mobile VPN:

VPN Host-to-LAN (OpenVPN) Host-to-LAN (L2TP/IPSec) LAN-to-LAN

OpenVPN Host-to-LAN VPN with X.509, Kerberos 5 and Radius Authentication Connected: 1

Status: **ACTIVE** Enabled Save Show Clients OpenVPN Log

OpenVPN Parameters

Port: 1194 TCP

Command Line Parameters: [Sh]

X.509 Configuration

X.509 Host Certificate

Local CA: [Local CA] OU=Hosts, CN=fw.lordch.net

Status: **OK**

Client IP Address Assignment

IP Range: 192.168.250.1

Gateway: 192.168.250.251

Log Viewer - Internet Explorer 7 personalizzato MSN

Log Viewer Host Section Filter

2008 Feb 04 fw (Local) VPN99_HZL

[Configure](#)

Refresh Close

```

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

```

Internet 100%