

VPN LAN-to-LAN con Zeroshell

Introduzione

In questo articolo spiegherò come realizzare una VPN che unisca due reti locali distinte (anche fisicamente distanti centinaia di km tra loro) adoperando Zeroshell. Sono già state pubblicate numerose guide che spiegano come realizzare proprio questo (Zeroshell rende molto facile la creazione di una VPN LAN-to-LAN), ma tutte presuppongono l'uso di due router Zeroshell. A me serviva che la macchina remota fosse separata e con una sola scheda di rete per ragioni che diventeranno ovvie quando spiegherò lo scopo di questa VPN e la situazione di rete. :-)

Scopo della VPN

Questa VPN nasce per permettere a me ed agli altri membri della famiglia di accedere al NAS (non esposto ad Internet per ragioni di sicurezza, dato che SMB non è cifrato) anche dalla nostra barca a vela, che è dotata di un router 4G TP-Link Archer.

Ovviamente le reti sono fisicamente distinte (una si trova per giunta in mezzo al mare!) e hanno una struttura completamente diversa. In questa tabella ho elencato le principali differenze:

| Parametro | LAN 1 | LAN 2 |
|--------------|---------------|----------------------|
| IP Pubblico | statico | dinamico con CGN* |
| Connessione | WiMAX | 4G LTE |
| Subnet | 172.16.0.0/16 | 192.168.1.0/24 |
| Access-point | vari dedicati | integrato nel router |
| Switch | dedicati | integrato nel router |

*CGN = *carrier-grade NAT (il NAT di Fastweb per intenderci)*

Il motivo per cui non è possibile utilizzare un'altra macchina Zeroshell funzionante da router o bridge è dato dall'impossibilità di riutilizzare l'access point e lo switch integrato al router TP-Link, che comporterebbe quindi l'uso di uno switch e un access point dedicati causando quindi un maggior consumo elettrico (ricordiamo che il tutto è alimentato dal banco batterie di bordo e deve funzionare anche quando il motore è spento), un maggior peso e un maggior ingombro. Tutte caratteristiche che sarebbero state odiate dal proprietario dell'imbarcazione! ;-)

Soluzione adottata

Ho avuto l'idea per la soluzione del problema pensando a questo semplice fatto: nella VPN ci devono passare solo i dati destinati all'altra LAN che ha una subnet diversa rispetto alla LAN della barca.

Per cui, *dovrebbe in teoria* essere possibile impostare una regola nelle tabelle di routing del modem TP-Link in modo da segnalare ai PC che il gateway a cui devono fare riferimento per la subnet 172.16.0.0/16 è l'OrangePI su cui è installato Zeroshell e non il gateway dell'operatore 4G LTE.

Un po' di smanettamenti dopo quest'idea ha funzionato! :-)

Configurazione della VPN

Requisiti

- Un Router Zeroshell nella LAN principale (LAN 1).
- Una minima conoscenza di come funziona una rete informatica (cos'è un gateway, una subnet etc.)
- Un'infarinatura generale sulle operazioni di base di Zeroshell: creazione di un profilo, configurazione utenti etc.
- Un indirizzo IP statico oppure un servizio di DNS dinamico tipo [Duckdns](#) per la LAN 1.
- L'interfaccia di Zeroshell della LAN 1 deve essere accessibile dalla LAN 2 (esempio: direttamente, tramite port-forwarding, tramite VPN PPTP, tramite un PC lasciato acceso con Teamviewer aperto...). Se si usa il port forwarding o l'accesso diretto bisogna ricordarsi di autorizzare l'accesso da WAN tramite la finestra WEB nella pagina Setup!

Installazione

In primo luogo è necessario rimediare un PC su cui installare Zeroshell nella seconda LAN: per ragioni di spazio ed energia ho scelto un [OrangePI Zero](#) (la versione da 256 MB di RAM va benissimo) ma potrebbe anche essere usato un Raspberry Pi, un Alix, un [thin client](#) un PC portatile o fisso. I requisiti hardware sono molto modesti, a meno che non si voglia attivare la compressione e/o avere un traffico sostenuto.

Installare quindi Zeroshell sul PC selezionato seguendo le istruzioni presenti sul [sito di Zeroshell](#) e creare un profilo nuovo. Scegliere un indirizzo IP per la macchina, io ho scelto *192.168.1.3*.

Collegarsi in remoto a Zeroshell della LAN 1 (di seguito lo chiamerò ZS 1, mentre quello della LAN 2 lo chiamerò ZS 2) e recarsi nella pagina VPN.

The screenshot shows the Zeroshell Net Services web interface. At the top, there's a status bar with system information: Release 3.0.1, 9.38 Kbit/s (Connections: 146 Load: 18%), CPU (1) AMD G-T440 Processor 1197MHz, Kernel 4.4.96-25-64, Memory 952568 kB (30% used), and Uptime 7 days: 4:14. The main navigation menu includes SYSTEM, USERS, NETWORK, and SECURITY. The current page is titled "OpenVPN Virtual Private Network LAN to LAN" and shows a table of VPN interfaces:

| VPN | Host-to-LAN (OpenVPN) | Host-to-LAN (L2TP/IPSec) | Host-to-LAN (PPTP) | LAN-to-LAN (OpenVPN) |
|-------|--|--------------------------|--------------------|----------------------|
| VPN99 | Listening for Road Warrior connections | | | UP |
| | Host-to-LAN OpenVPN Interface | | | |
| | 192.168.250.254 | 255.255.255.0 | | |

Below the table, there's a section for "OpenVPN Software" with a description and a list of advantages:

- By creating an Ethernet (Layer 2) connection between the two LANs, in addition to routing, bridging of the networks is made possible guaranteeing the passage of any layer 3 protocol (IP, IPX, Apple Talk);
- The 802.1Q VLAN protocol is supported. This means that if a network is broken into Virtual LANs, the latter can also be transported on the peer network with a single VPN tunnel;
- Bonding of two or more VPNs is supported in load balancing or fault tolerance configuration. This means, for example, that if there are two or more ADSL connections, a VPN can be created for each connection and they can be combined increasing the bandwidth or reliability;
- Thanks to the LZD real-time compression algorithm, data is compressed in an adaptive manner. In other words, compression only occurs when the data on the VPN really can be compressed;
- The use of TLS tunnels on TCP or UDP ports makes it possible to transit the router where the NAT is enabled without problems.

At the bottom, there are two success messages:

```
Dec 28 23:48:21 SUCCESS: The Key is valid: Repository Subscription successfully activated
Dec 29 13:50:18 SUCCESS: Session opened from host [redacted] Admin]
```

Fare clic su LAN-to-LAN (OpenVPN) e New VPN. Si aprirà una finestra:

The screenshot shows the "VPN Config - Mozilla Firefox" window. The URL is [https://\[redacted\]/cgi-bin/kerbynet?Section=VPN&Stk=4b6548417f80e7395291a371c22b322f5d0ce26](https://[redacted]/cgi-bin/kerbynet?Section=VPN&Stk=4b6548417f80e7395291a371c22b322f5d0ce26). The page title is "LAN-to-LAN Virtual Private Network Configuration" and the interface is for "Interface: VPN00".

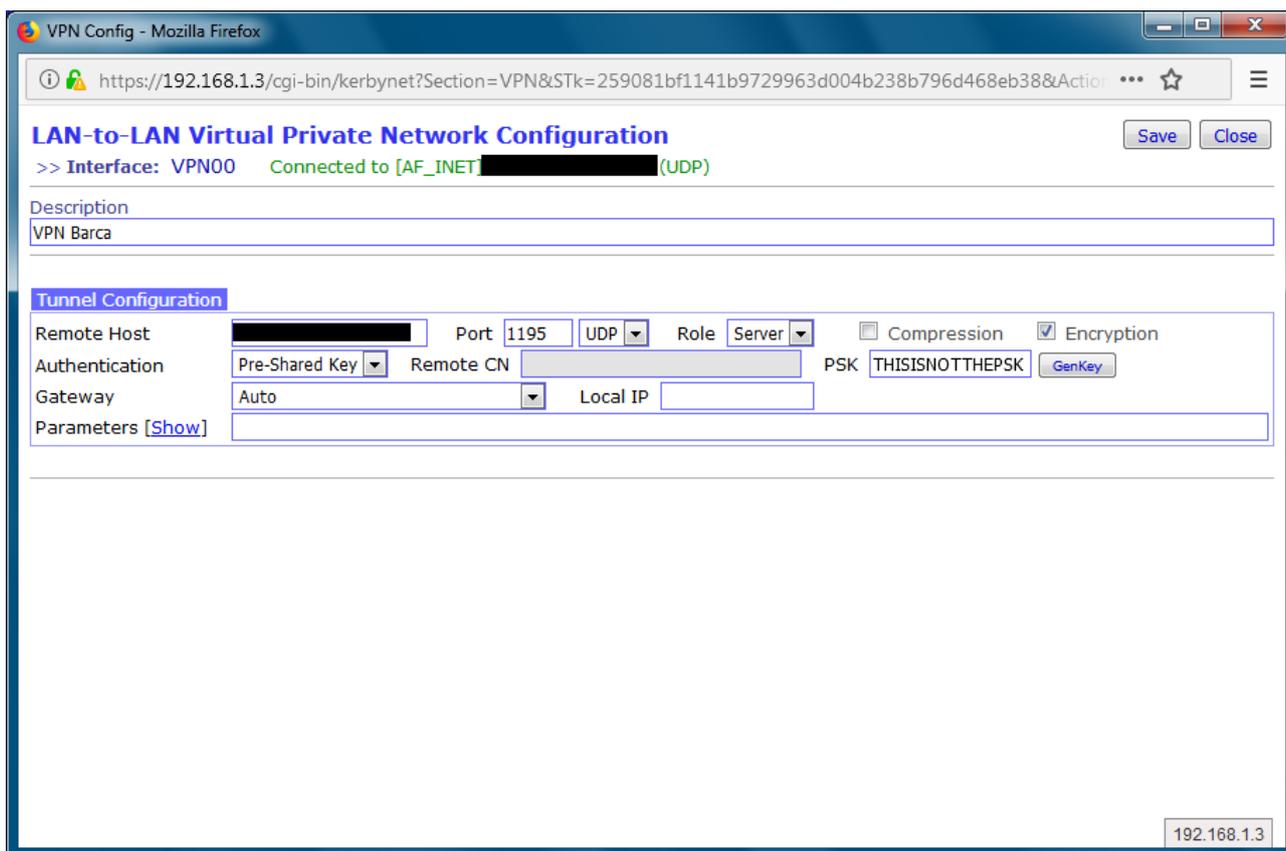
The "Tunnel Configuration" section includes the following fields:

- Remote Host: [redacted]
- Port: 1195
- UDP
- Role: Client
- Compression:
- Encryption:
- Authentication: Pre-Shared Key
- Remote CN: [redacted]
- PSK: THISISNOTTHEPSK
- Gateway: Auto
- Local IP: [redacted]

There are "Save" and "Close" buttons at the top right of the configuration area.

Impostare la descrizione della VPN (a piacere) ed il ruolo dell'host remoto che deve essere impostato a client. Inoltre è necessario impostare l'autenticazione a Pre-shared key e inserire una chiave di cifratura nella casella PSK. Lasciare tutti gli altri parametri invariati. Se si desidera è possibile abilitare la compressione, io l'ho lasciata disabilitata in quanto con la potenza ridotta dell'OrangePI Zero si otteneva una perdita di prestazioni.

Ora, collegarsi a ZS 2 e ripetere il passo 1 e 2 fino ad aprire la stessa finestra di prima:



Impostare i parametri come prima. In Remote Host inserire l'indirizzo IP o nome host di ZS 1 ed impostare il ruolo a server. Assicurarsi inoltre che la chiave PSK e le impostazioni di crittografia e compressione siano identiche su tutti e due i ZS.

Una volta salvate le impostazioni, abilitare la VPN utilizzando la casellina Up su entrambi i ZS. Se tutto va bene, dovrebbe comparire una scritta verde Connected.

Adesso è necessario impostare un indirizzo IP alle due interfacce virtuali. E' importante che l'indirizzo non corrisponda a nessuna delle subnet già utilizzate nella due LAN. Per questo, io ho scelto la subnet 10.50.0.1/8. Rechiamoci in Setup -> Networking e clicchiamo su Add IP accanto all'interfaccia virtuale. L'operazione è identica all'aggiunta di un IP ad un'interfaccia fisica e va effettuata sia su ZS 1 che su ZS 2 (ovviamente gli indirizzi IP dovranno essere diversi!).

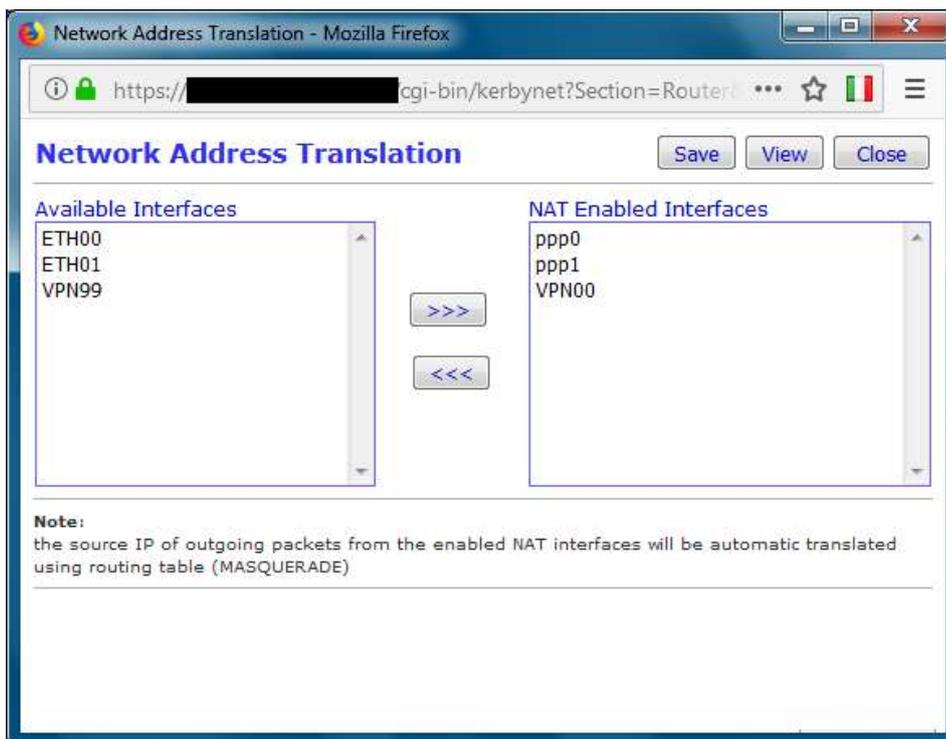
La pagina Networking dovrebbe apparire così:

The screenshot shows the Zeroshell Net Services web interface. At the top, it displays system information: Release 3.0.1A - RPT 3.57 Kbit/s (Connections: 19 Load: 27%), CPU (4) ARMv7 Processor rev 4 (v7l) 1200MHz, Kernel 4.4.30-ARM-ZS, Memory 925 MB (9% used), and Uptime 0 days, 1:27. The main navigation menu includes SYSTEM, USERS, NETWORK, and SECURITY. The NETWORK section is expanded, showing VPN configuration. Two VPNs are listed: VPN00 (Connected to [AF_INET] [redacted] (UDP) UP) and VPN99 (Connections from Road Warrior clients disabled, Host-to-LAN OpenVPN Interface UP). The VPN00 configuration shows a dynamic IP of 9.0.0.0 and a MAC address [redacted]. The VPN99 configuration shows a dynamic IP of 192.168.250.254 and a MAC address [redacted]. Below the VPN list, there is a section for OpenVPN Software, which explains that Zeroshell uses OpenVPN to encapsulate Ethernet datagrams in TLS tunnels. A log entry at the bottom indicates a successful change to a static route: 'Dec 29 15:39:07 SUCCESS: Static route 172.16.0.0/255.255.0.0 via 10.50.0.1 metric 2 successfully changed.'

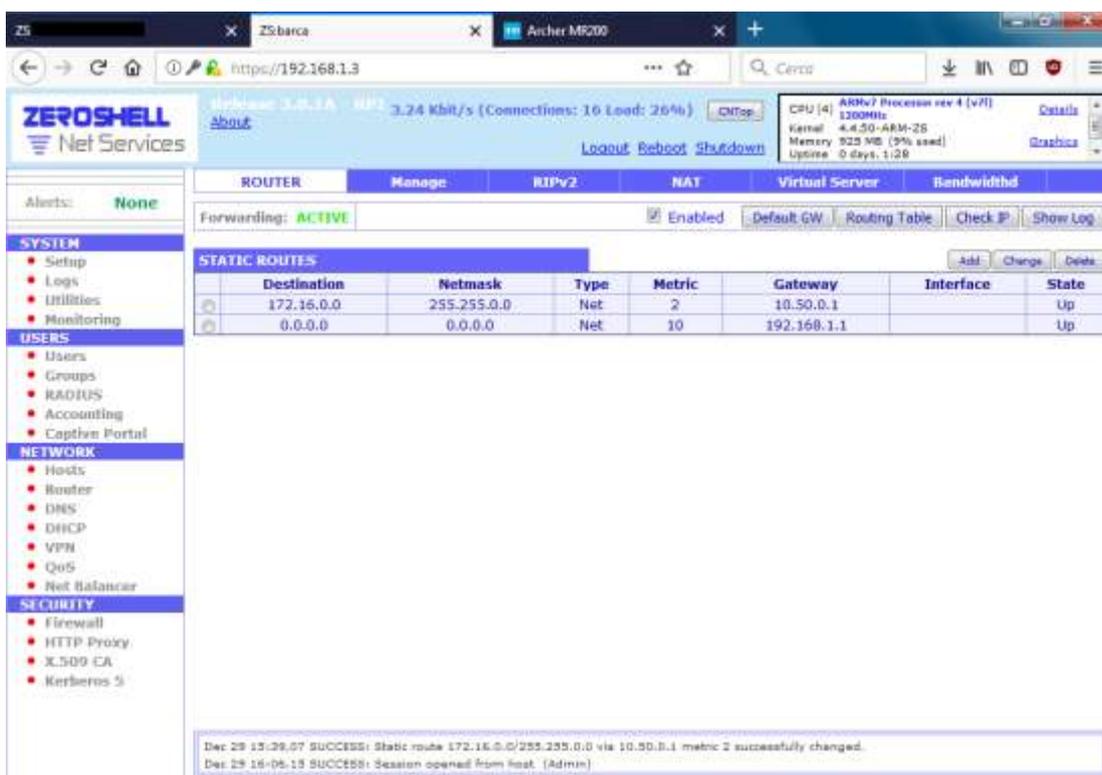
Il prossimo passo è quello di abilitare il NAT. Su ZS 2, recarsi sulla pagina Router -> NAT e abilitare l'interfaccia VPN00 alla NAT come nello screenshot:

The screenshot shows the 'Network Address Translation' configuration page in the Zeroshell interface. The page title is 'Network Address Translation - Mozilla Firefox'. The URL is 'https://192.168.1.3/cgi-bin/kerbynet?Section=Router&STk=ec'. The page has 'Save', 'View', and 'Close' buttons. There are two main sections: 'Available Interfaces' and 'NAT Enabled Interfaces'. The 'Available Interfaces' list contains 'ETH00' and 'VPN99'. The 'NAT Enabled Interfaces' list contains 'VPN00'. Between the two lists are two buttons: '>>>' and '<<<'. A 'Note' at the bottom states: 'the source IP of outgoing packets from the enabled NAT interfaces will be automatic translated using routing table (MASQUERADE)'. The IP address '192.168.1.3' is visible in the bottom right corner.

Effettuare la stessa operazione su ZS 1:

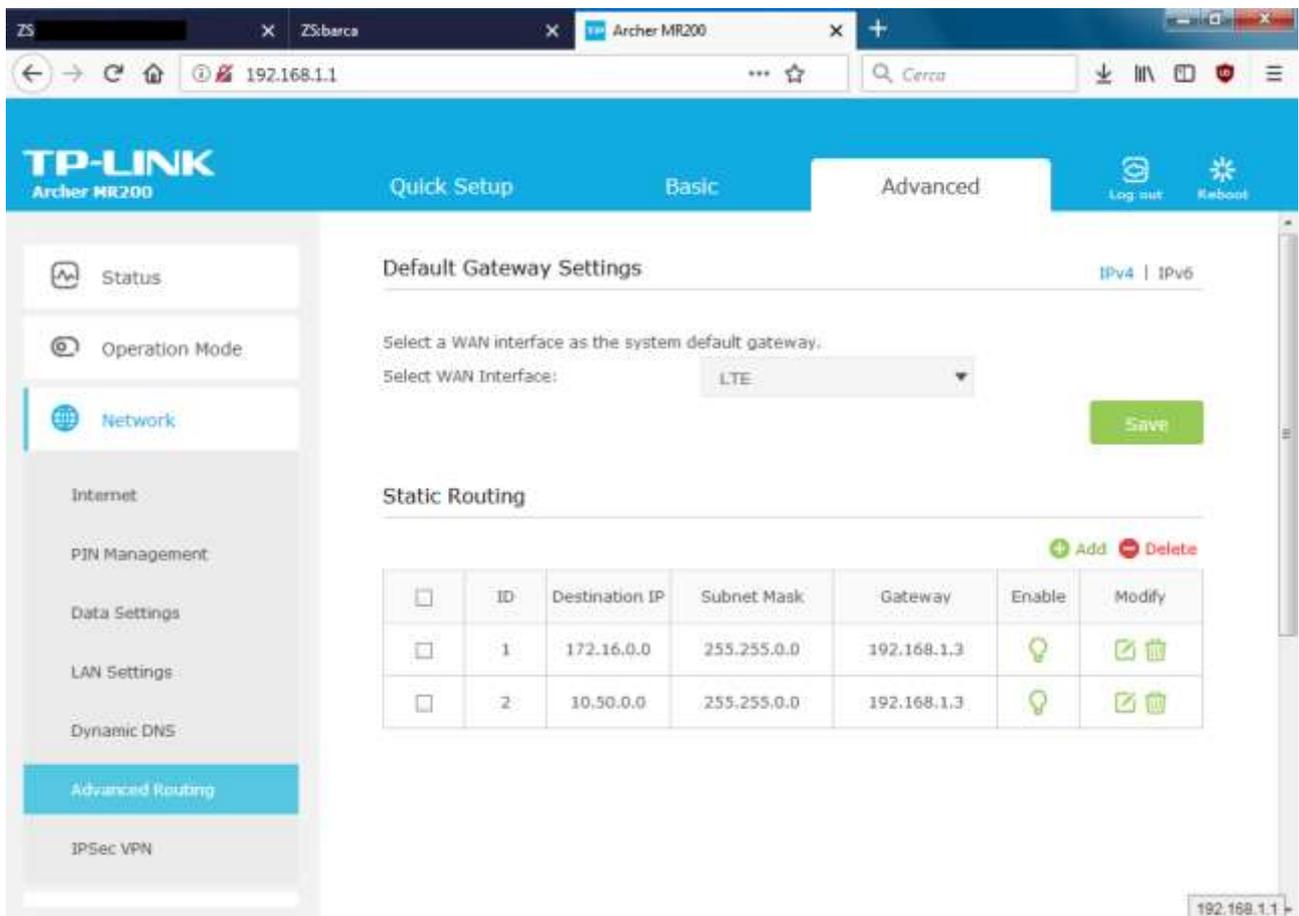


A questo punto bisogna aggiungere una route statica su ZS 2, in modo che sappia che i pacchetti indirizzati a 172.16.0.0/16 vanno inoltrati sulla VPN e non sulla WAN. Nella pagina Router cliccare su Add. La nuova route statica dovrà avere come destination la subnet della LAN 1 e come gateway l'indirizzo dell'interfaccia VPN sul ZS 1.



Ora occorre recarsi sulla pagina di configurazione del router della LAN 2 e andare nella pagina di configurazione delle route statiche. Nel mio caso la pagina si chiamava Advanced routing. Tutti i router hanno la possibilità di avere route statiche, occorre solo trovare il modo per impostarle! I costruttori di router tendono a nascondere in pagine sperdute nell'interfaccia di configurazione (magari chiamandole anche con nomi criptici), a cui si accede talvolta solo conoscendo l'URL, abilitando una modalità speciale/amministratore/supervisore/utente avanzato o ancora tramite Telnet...

Impostare due route statiche, una avente come destination la subnet della LAN 1 e una con la subnet della VPN. Il gateway dev'essere in entrambi i casi l'IP del ZS 2.



The screenshot shows the TP-Link Archer MR200 web interface. The browser address bar shows the URL 192.168.1.1. The interface has a blue header with the TP-LINK logo and navigation tabs for 'Quick Setup', 'Basic', and 'Advanced'. The 'Advanced' tab is selected, and the 'Advanced Routing' option is highlighted in the left sidebar. The main content area is divided into two sections: 'Default Gateway Settings' and 'Static Routing'. In the 'Default Gateway Settings' section, the 'Select WAN Interface' dropdown is set to 'LTE', and there is a 'Save' button. The 'Static Routing' section contains a table with two entries:

| ID | Destination IP | Subnet Mask | Gateway | Enable | Modify |
|----|----------------|-------------|-------------|-------------------------------------|---|
| 1 | 172.16.0.0 | 255.255.0.0 | 192.168.1.3 | <input checked="" type="checkbox"/> |   |
| 2 | 10.50.0.0 | 255.255.0.0 | 192.168.1.3 | <input checked="" type="checkbox"/> |   |

L'ultima cosa che ci rimane da fare è fare un bel ping su un IP della LAN 1 e verificare che risponda come dovuto:

```
C:\Windows\system32\cmd.exe

C:\Users\Jacopo>ping 172.16.20.210

Esecuzione di Ping 172.16.20.210 con 32 byte di dati:
Risposta da 172.16.20.210: byte=32 durata=107ms TTL=126
Risposta da 172.16.20.210: byte=32 durata=89ms TTL=126
Risposta da 172.16.20.210: byte=32 durata=91ms TTL=126
Risposta da 172.16.20.210: byte=32 durata=104ms TTL=126

Statistiche Ping per 172.16.20.210:
    Pacchetti: Trasmessi = 4, Ricevuti = 4,
    Persi = 0 (0% persi),
Tempo approssimativo percorsi andata/ritorno in millisecondi:
    Minimo = 89ms, Massimo = 107ms, Medio = 97ms

C:\Users\Jacopo>_
```

Si può anche effettuare un traceroute verso lo stesso IP per verificare che la VPN funzioni a dovere:

```
C:\Windows\system32\cmd.exe

C:\Users\Jacopo>tracert 172.16.20.210

Traccia instradamento verso DNSSERUER [172.16.20.210]
su un massimo di 30 punti di passaggio:

 1      4 ms      2 ms      3 ms    192.168.1.3
 2     97 ms     69 ms     68 ms    10.50.0.1
 3     85 ms     74 ms     70 ms    DNSSERUER [172.16.20.210]

Traccia completata.

C:\Users\Jacopo>_
```

Passi successivi

Questa configurazione di base è sufficiente per risolvere il mio problema. Tuttavia, nulla vieta di configurare altri aspetti di Zeroshell, come il QoS, il firewall, il failover etc.