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

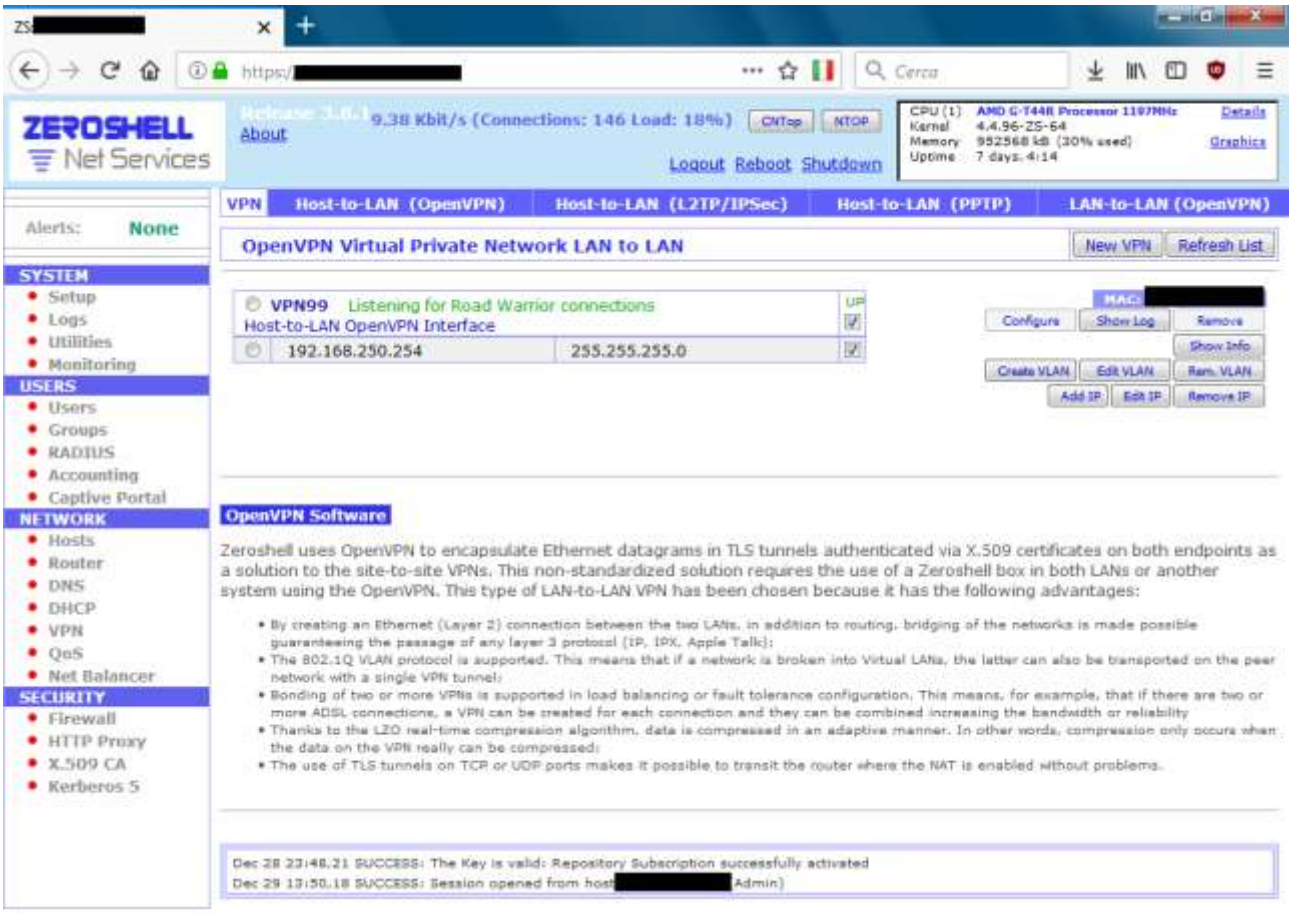
- Un Router Zeroshell nella LAN principale (LAN 1).
- Una minima conoscenza di come funziona una rete informatica (cos'è un gateway, una subnet etc.)
- Un' infarinatura generale sulle operazioni di base di Zeroshell: creazione di un profilo, configurazione utenti etc.
- Un indirizzo IP statico oppure 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

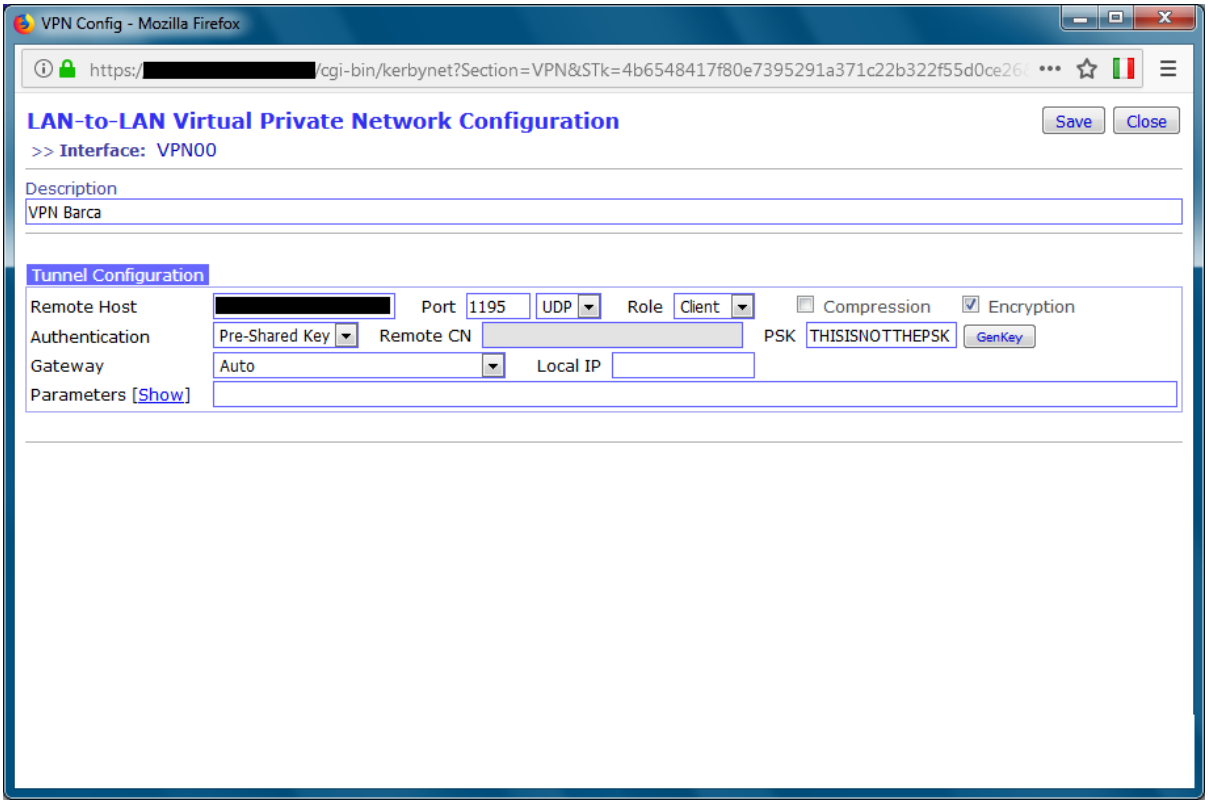
In primo luogo è necessario rimediare un PC su cui installare Zeroshell nella seconda LAN: per ragioni di spazio ed energia ho scelto un OrangePI Zero (la versione da 256 MB di RAM va benissimo) ma potrebbe anche essere usato un Raspberry Pi, un Alix, un thin client un PC portatile o fisso. I requisiti 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.

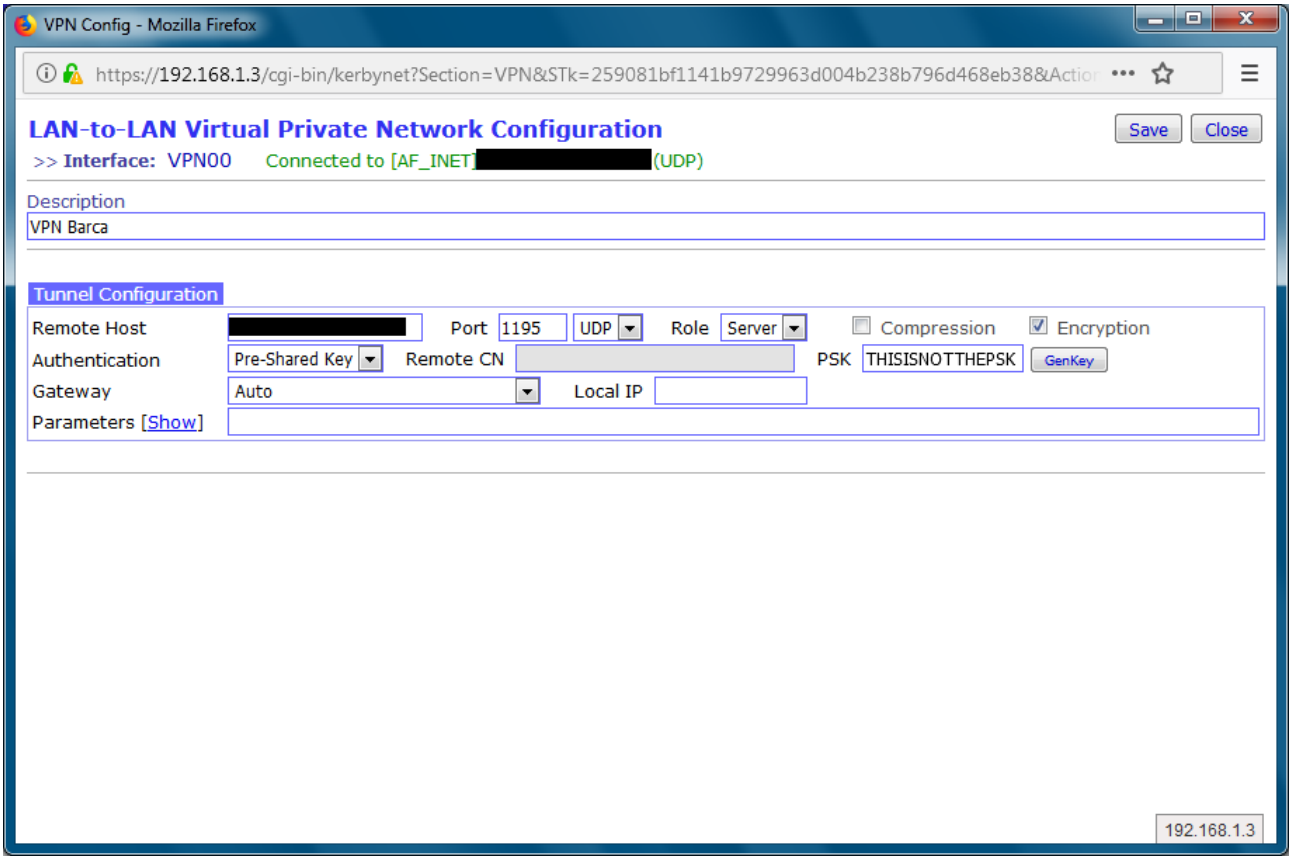


Fare clic su LAN-to-LAN (OpenVPN) e New VPN. Si aprirà una finestra:



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:

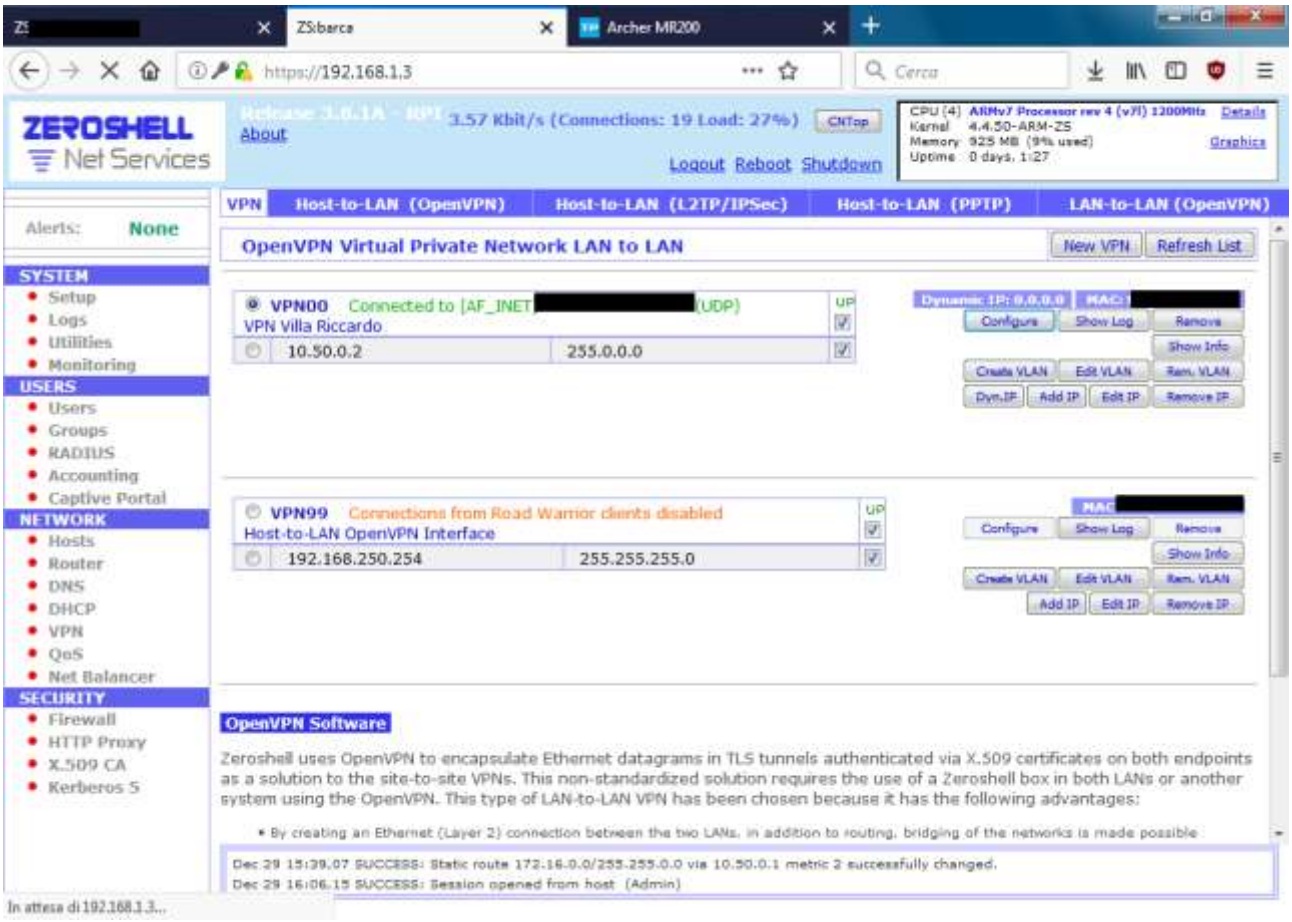


Impostare i parametri come prima. In Remote Host inserire l'indirizzo IP o nome host di ZS 1 ed impostare il ruolo a server. Assicurarsi inoltre che la chiave PSK e le impostazioni di crittografia e compressione siano identiche su tutti e due i ZS.

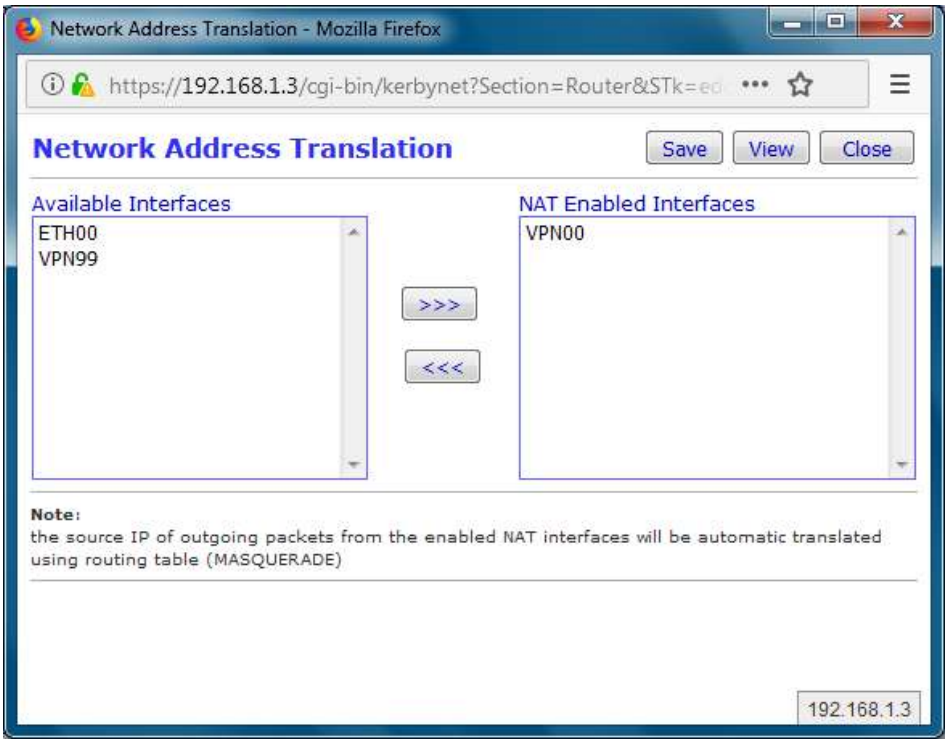
Una volta salvate le impostazioni, abilitare la VPN utilizzando la casellina Up su entrambi i ZS. Se tutto va bene, dovrebbe comparire una scritta verde Connected.

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!).

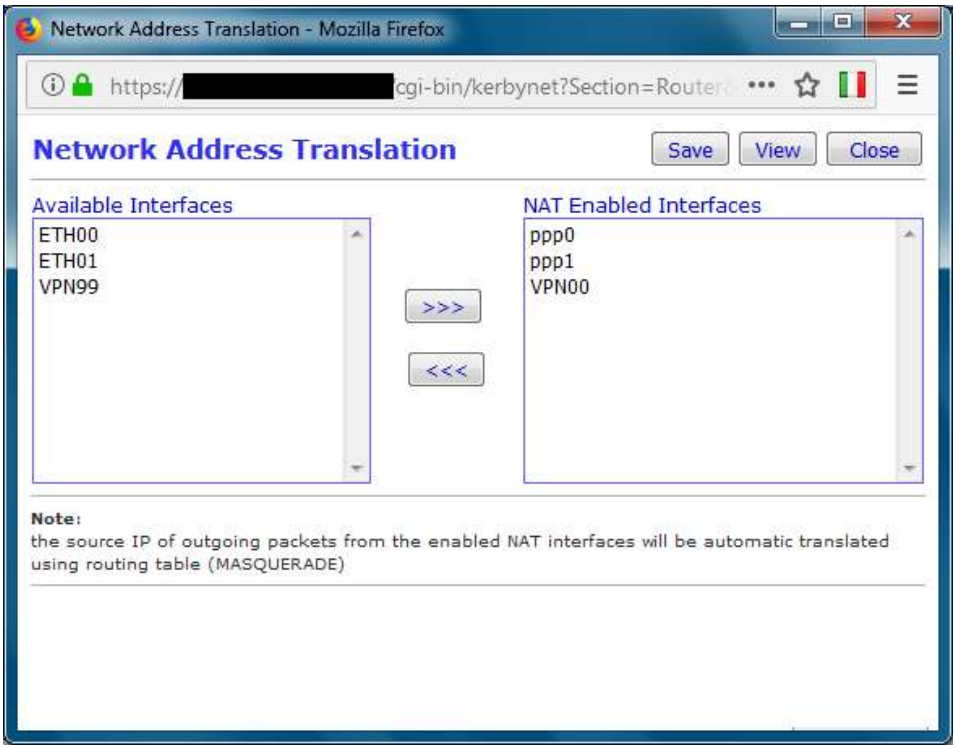
La pagina Networking dovrebbe apparire così:



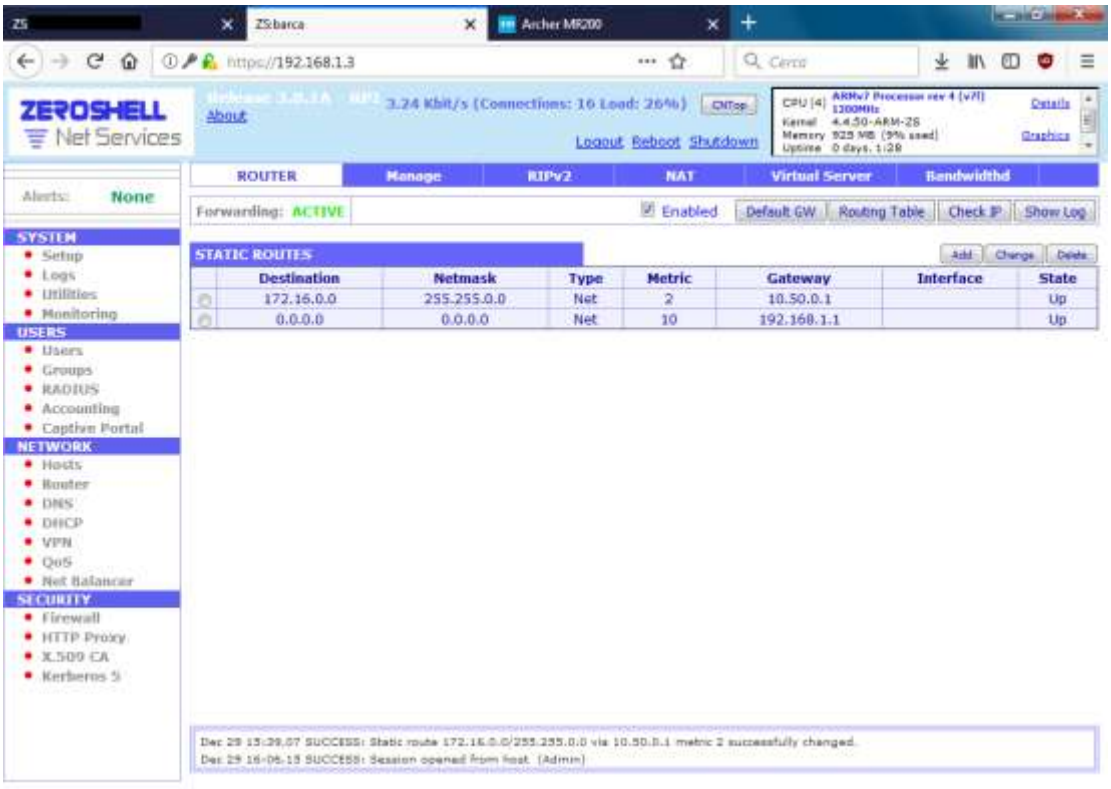
Il prossimo passo è quello di abilitare il NAT. Su ZS 2, recarsi sulla pagina Router -> NAT e abilitare l'interfaccia VPN00 alla NAT come nello screenshot:



Effettuare la stessa operazione su ZS 1:

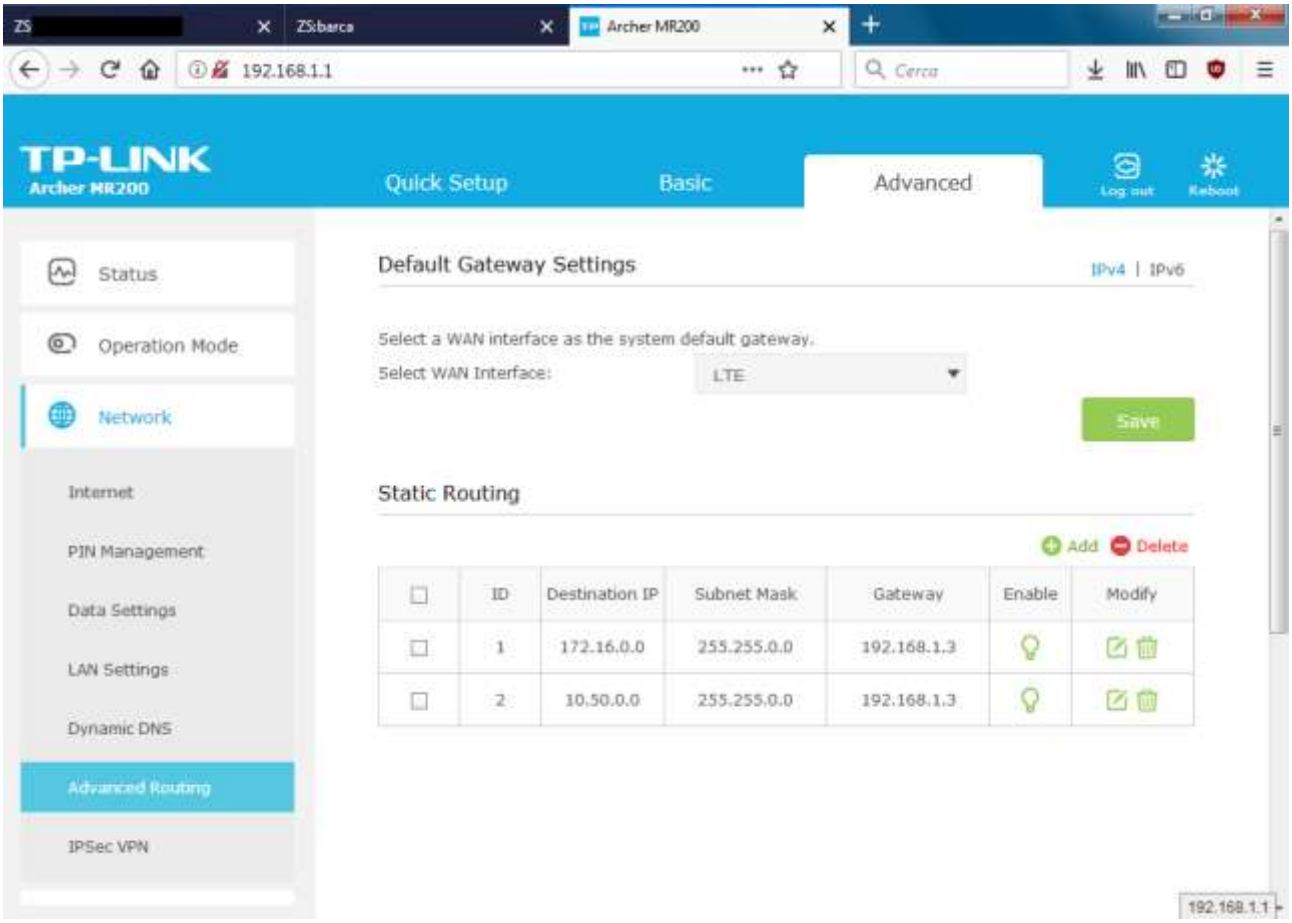


A questo punto bisogna aggiungere una route statica su ZS 2, in modo che sappia che i pacchetti indirizzati a *172.16.0.0/16* vanno inoltrati sulla VPN e non sulla WAN. Nella pagina Router cliccare su Add. La nuova route statica dovrà avere come destination la subnet della LAN 1 e come gateway l'indirizzo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

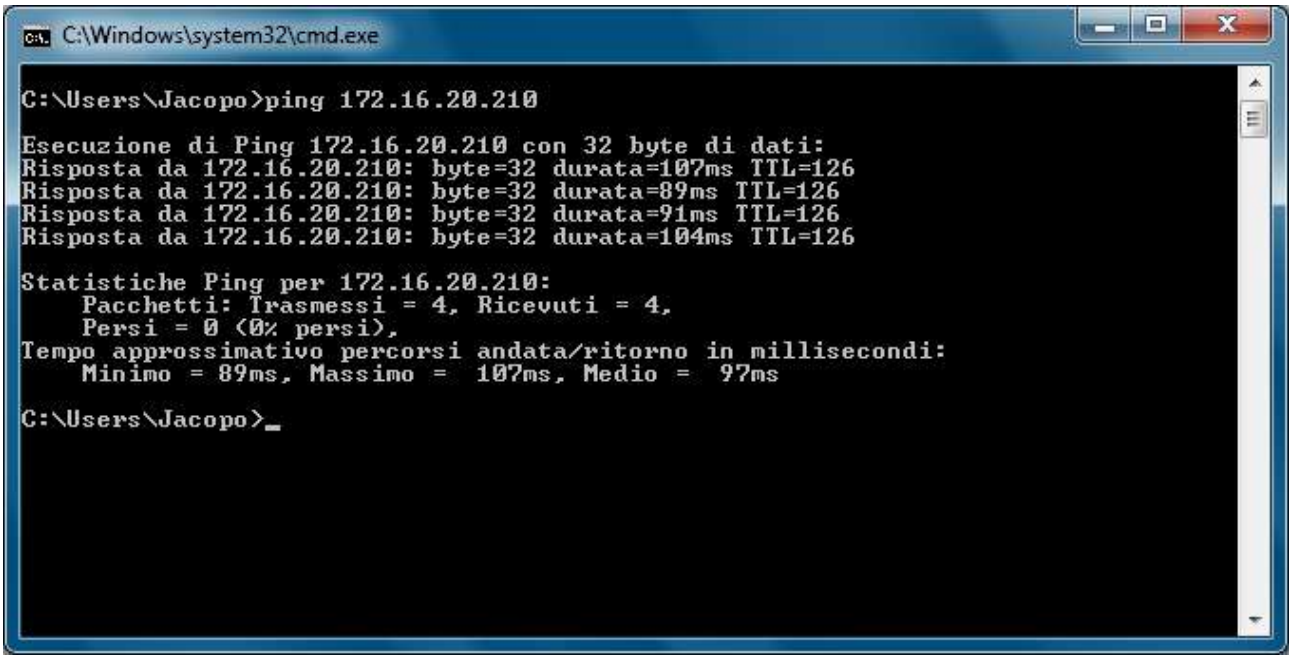


Ora occorre recarsi sulla pagina di configurazione del router della LAN 2 e andare nella pagina di configurazione delle route statiche. Nel mio caso la pagina si chiamava Advanced routing. Tutti i router hanno la possibilità di avere route statiche, occorre solo trovare il modo per impostarle! I costruttori di router tendono a nasconderle 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...

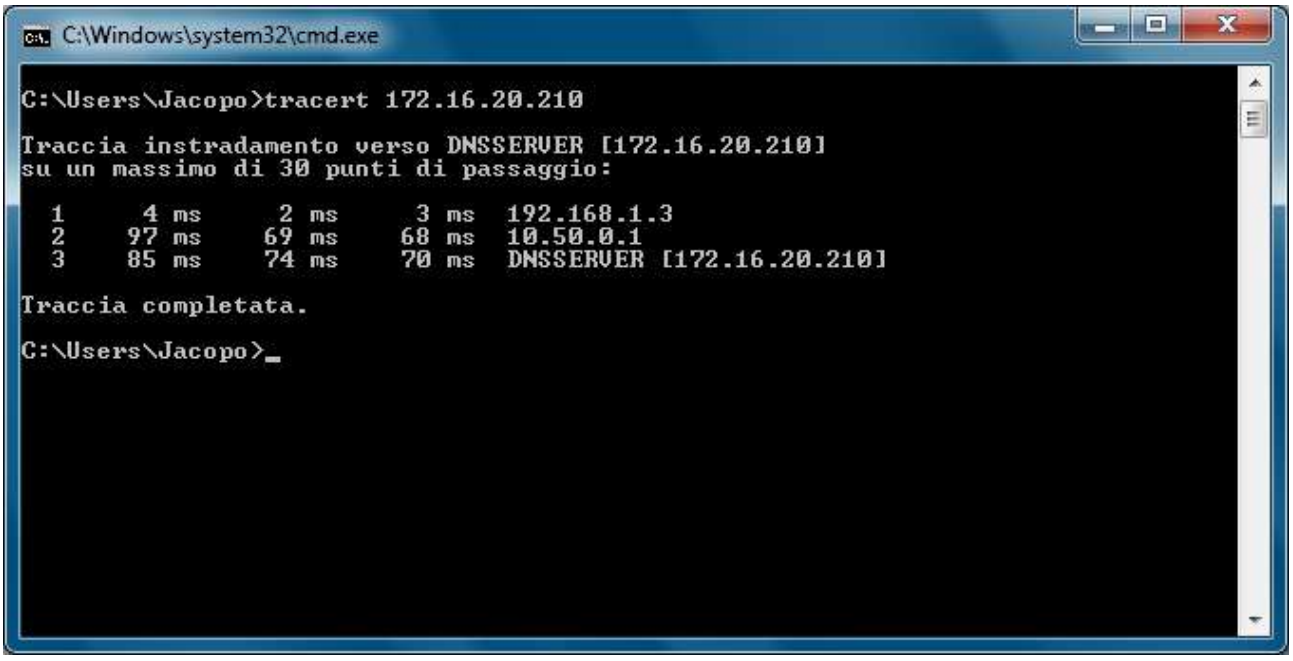
Impostare due route statiche, una avente come destination la subnet della LAN 1 e una con la subnet della VPN. Il gateway dev'essere in entrambi i casi l'IP del ZS 2.



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:



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



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.