Consiglio Nazionale delle Ricerche
Istituto di Calcolo e Reti ad Alte Prestazioni

Configurazione di router con firmware open source con Failover o Load Balancing su rete LTE ed UMTS e VPN Client

Antonio Francesco Gentile[1], Davide Macrì[2], Emilio Greco[3]

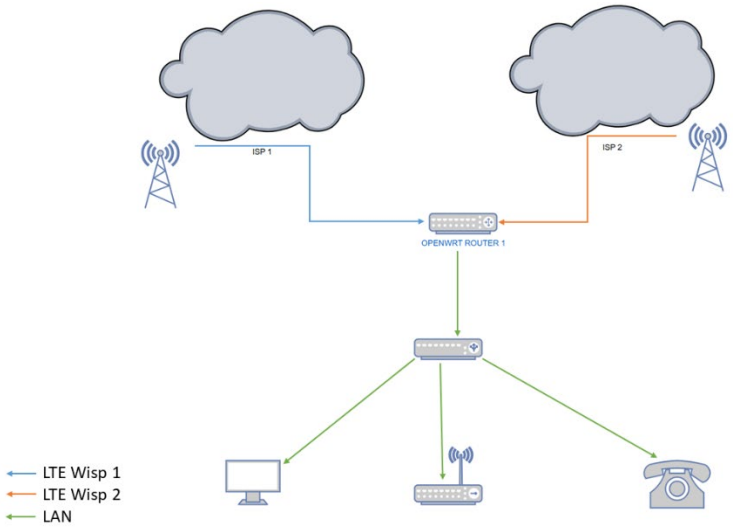
RT-ICAR-CS-24-03 **Ottobre 2024**

Consiglio Nazionale delle Ricerche, Istituto di Calcolo e Reti ad Alte Prestazioni (ICAR)
– Sede di Cosenza, Via P. Bucci 8-9C, 87036 Rende, Italy, URL: www.icar.cnr.it
– Sezione di Napoli, Via P. Castellino 111, 80131 Napoli, URL: www.icar.cnr.it
– Sezione di Palermo, Via Ugo La Malfa, 153, 90146 Palermo, URL: www.icar.cnr.it

Sommario

Questa relazione tecnica descrive la configurazione di **OpenWrt** per gestire due connessioni WAN (una tramite LTE con chipset Qualcomm e una tramite dongle USB UMTS), utilizzando **mwan3** per il failover e il bilanciamento del carico. Inoltre, spiega come configurare un client **WireGuard VPN** per connettersi a una sede centrale (`xxx.sito.com`), instradando il traffico della rete `10.10.179.0/24` tramite il tunnel WireGuard. Infine, include la configurazione per abilitare il **Masquerading** e il **MSS Clamping** per garantire la compatibilità e la sicurezza del traffico VPN.

La figura seguente illustra il deploy realizzato:



1. Introduzione

OpenWrt è un sistema operativo open-source per router che supporta una vasta gamma di configurazioni di rete avanzate. In questo progetto, si richiede:

- Gestione di due connessioni WAN (una LTE con APN `ibox.tim.it` e una UMTS con APN `internet.it`).
- Utilizzo di **mwan3** per gestire il **failover** o il **bilanciamento del carico** tra le due WAN.
- Configurazione di un client **WireGuard** per connettersi a una sede centrale, instradando il traffico della sottorete `10.10.179.0/24`.
- Abilitazione di **Masquerading** e **MSS Clamping** per l'interfaccia WireGuard.

---

2. Configurazione della rete WAN e VPN

2.1 Configurazione delle Interfacce di Rete (WAN1: LTE e WAN2: UMTS)

Per la gestione delle due connessioni WAN, utilizziamo rispettivamente **LTE** e **UMTS**, configurando due interfacce in `/etc/config/network`.

1. **WAN1 (LTE)**: utilizza il protocollo **QMI** per il modem LTE con APN `ibox.tim.tim.it`.
2. **WAN2 (UMTS)**: utilizza il protocollo **3g** per il dongle USB UMTS con APN `internet.it`.

Configurazione del file `/etc/config/network`:

```
config interface 'loopback'
    option ifname 'lo'
    option proto 'static'
```

```
    option ipaddr '127.0.0.1'
    option netmask '255.0.0.0'

#### LTE - Interfaccia WAN1 (ibox.tim.it) ####
config interface 'wan1'
    option proto 'qmi'
    option device '/dev/cdc-wdm0'   # Device del modem LTE Qualcomm
    option apn 'ibox.tim.it'
    option auth 'none'              # Senza autenticazione
    option metric '10'              # Priorità più alta per failover (connessione
primaria)
    option auto '1'
    option ipv6 '0'

#### UMTS - Interfaccia WAN2 (internet.it) ####
config interface 'wan2'
    option proto '3g'
    option device '/dev/ttyUSB0'     # Device del dongle USB UMTS
    option apn 'internet.it'
    option service 'umts'
    option auth 'none'               # Senza autenticazione
    option metric '20'               # Priorità più bassa per failover (connessione
secondaria)
    option auto '1'
    option ipv6 '0'
```

2.2 Configurazione del Client WireGuard VPN

Il client **WireGuard** viene configurato per instradare il traffico della sottorete `10.10.179.0/24` attraverso un tunnel VPN, connesso alla sede centrale con endpoint `xxx.sito.com`. Per questa configurazione, usiamo chiavi pubbliche e private generate in precedenza.

Configurazione del file `/etc/config/network`:

```
#### WireGuard - Connessione VPN ####
config interface 'wg0'
    option proto 'wireguard'
    option private_key 'YOUR_PRIVATE_KEY'    # Chiave privata generata
    option listen_port '51820'               # Porta di ascolto per WireGuard
    list addresses '10.10.179.2/32'          # IP locale su WireGuard

config wireguard_wg0
    option public_key 'PEER_PUBLIC_KEY'      # Chiave pubblica della sede centrale
    option endpoint_host 'xxx.sito.com'      # Host della sede centrale
    option endpoint_port '51820'             # Porta del server WireGuard remoto
    option persistent_keepalive '25'         # Mantiene il tunnel attivo
    list allowed_ips '10.10.179.0/24'        # Rete remota instradata tramite il tunnel
    option route_allowed_ips '1'             # Abilita la rotta per il traffico destinato
a questa rete

#### Routing statico per il traffico destinato alla rete 10.10.179.0/24 ####
config route
    option interface 'wg0'
    option target '10.10.179.0'
    option netmask '255.255.255.0'
```

3. Configurazione di mwan3 per Failover e Load Balancing

3.1 Installazione e Attivazione di mwan3

Per installare il pacchetto **mwan3**, esegui i seguenti comandi:

```
opkg update
opkg install mwan3 luci-app-mwan3
/etc/init.d/mwan3 enable
/etc/init.d/mwan3 start
```

3.2 Configurazione di mwan3 per Failover

1. Vai in **Network > Load Balancing**.
2. Aggiungi entrambe le interfacce WAN (`wan1` per LTE e `wan2` per UMTS).
3. Configura il **failover** assegnando una priorità maggiore a `wan1` rispetto a `wan2`:
    - **wan1 (LTE)**: Peso 1 (connessione primaria).
    - **wan2 (UMTS)**: Peso 0 (connessione di backup).

3.3 Configurazione di mwan3 per Load Balancing

Se desideri il bilanciamento del carico (distribuire il traffico su entrambe le connessioni):

1. Aggiungi entrambe le interfacce WAN come in precedenza.
2. Configura il **load balancing** assegnando lo stesso peso a entrambe le interfacce:
    - **wan1 (LTE)**: Peso 1.
    - **wan2 (UMTS)**: Peso 1.

---

4. Abilitare Masquerade e MSS Clamping per l'Interfaccia WireGuard (`wg0`)

4.1 Masquerading

Il **masquerading** è utilizzato per riscrivere l'indirizzo IP sorgente dei pacchetti provenienti dalla rete locale (LAN) con l'indirizzo dell'interfaccia **WireGuard** (`wg0`). Questo è necessario quando la rete remota (sede centrale) non gestisce i tuoi IP locali.

4.2 MSS Clamping

Il **MSS Clamping** viene utilizzato per evitare problemi di frammentazione dei pacchetti TCP nel tunnel VPN, poiché i pacchetti incapsulati in una VPN spesso superano la dimensione massima supportata dalla rete sottostante (MTU). Questo garantisce che i pacchetti TCP inviati attraverso la VPN non vengano frammentati, prevenendo perdite di pacchetti.

Configurazione del file `/etc/config/firewall`:

```
config zone
    option name 'wg'
    option input 'ACCEPT'
    option output 'ACCEPT'
    option forward 'REJECT'
    option network 'wg0'
    option masq '1'                 # Abilita il masquerading (NAT)
    option mtu_fix '1'               # Abilita MSS Clamping
```

```
config forwarding
    option src 'lan'
    option dest 'wg'
```

---

5. Scelta di WireGuard per la Sicurezza su Connessioni di Tipo LTE/UMTS

WireGuard è stato scelto come soluzione VPN per le sue caratteristiche di sicurezza, efficienza e semplicità. Rispetto ad altri tipi di VPN, come **OpenVPN** o **IPsec**, WireGuard presenta alcuni vantaggi chiave:

- **Sicurezza Avanzata**: WireGuard utilizza algoritmi crittografici moderni e robusti, come **ChaCha20** per la crittografia e **Poly1305** per l'autenticazione, che offrono un elevato livello di sicurezza. Questo è particolarmente importante in connessioni mobili come LTE e UMTS, dove il traffico può essere vulnerabile a intercettazioni e attacchi.
- **Prestazioni Elevate**: Grazie alla sua implementazione semplice e leggera, WireGuard è in grado di offrire velocità superiori rispetto ad altre soluzioni VPN. Questo è fondamentale per connessioni a banda limitata come LTE/UMTS, dove ogni kilobyte conta e l'overhead della VPN deve essere minimizzato.
- **Facilità di Configurazione**: WireGuard è progettato per essere facile da configurare e gestire. Le chiavi di crittografia possono essere generate e distribuite in modo semplice, senza la necessità di configurazioni complesse come in altri protocolli VPN.
- **Meno Consumo di Risorse**: WireGuard richiede meno risorse di CPU e memoria, il che lo rende ideale per dispositivi con hardware limitato, come router e dongle USB utilizzati in scenari LTE/UMTS.

---

6. Importanza della Diversificazione delle Connessioni in Aree con Difficoltà di Connettività

In contesti in cui la connettività Internet è inaffidabile, l'uso di più connessioni WAN può essere cruciale. Le aree rurali o quelle con infrastrutture limitate possono sperimentare interruzioni di servizio, latenza elevata o scarsa larghezza di banda. Avere a disposizione più opzioni di connettività consente:

- **Affidabilità**: L'implementazione di **failover** garantisce che, in caso di caduta di una connessione, il traffico venga automaticamente instradato verso l'altra, riducendo al minimo il downtime.
- **Performance**: Il **bilanciamento del carico** distribuisce il traffico tra le due connessioni, migliorando la velocità complessiva e la reattività della rete.
- **Scalabilità**: Questa configurazione è facilmente scalabile; aggiungere ulteriori connessioni può migliorare ulteriormente l'affidabilità e le prestazioni.

Tuttavia, ci sono alcuni **contro** associati a questa implementazione:

- **Costi**: La gestione di più connessioni WAN può comportare costi aggiuntivi, sia per le tariffe mensili dei fornitori di servizi che per l'hardware necessario.
- **Complessità**: La configurazione e la gestione di soluzioni software e hardware per il bilanciamento del carico e il failover possono richiedere competenze tecniche avanzate e un monitoraggio costante.

---

7. Conclusioni

La configurazione di **OpenWrt** con **mwan3** per gestire più connessioni WAN, combinata con l'implementazione di un client **WireGuard VPN**, rappresenta una soluzione robusta e flessibile per garantire connettività in scenari complessi. Questa architettura offre diversi vantaggi, tra cui affidabilità, prestazioni migliorate e scalabilità. Tuttavia, è essenziale considerare i costi e la complessità associati alla gestione di più connessioni.

L'adozione di soluzioni open-source come **OpenWrt** e **WireGuard** non solo favorisce la personalizzazione e la flessibilità, ma consente anche di evitare le restrizioni legate ai fornitori di hardware e software commerciali. Con la giusta configurazione e manutenzione, queste tecnologie possono fornire una connettività Internet affidabile e sicura anche in ambienti difficili.