UNIVERSITÀ POLITECNICA DELLE MARCHE

FACOLTÀ DI INGEGNERIA

Corso di Laurea triennale in *Ingegneria Informatica e dell'Automazione*

Studio e configurazione di una VPN site-to-site in ambiente CG-NAT

Study and configuration of a site-to-site VPN in CG-NAT environment

Relatore:
Prof. Ennio Gambi

Correlatore:
Ing. Adelmo De Santis

Tesi di Laurea di:
Alessandro Illuminati
matricola 1078466

Anno accademico 2020-2021

Prefazione

Nell'ambito del mio percorso universitario ho avuto modo di approfondire le tematiche relative al mondo delle reti e del networking, a tal proposito grazie alla possibilità offerta dal Dipartimento di Ingegneria dell'Informazione, dal Prof. Ennio Gambi e dall'Ing. Adelmo De Santis ho conseguito con successo la certificazione "*HUAWEI HCIA Routing and Switching*". Successivamente, grazie alle competenze acquisite, ho collaborato con alcuni miei colleghi per progettare e realizzare una implementazione di una VPN site-to-site attraverso una connessione radiomobile per conto dell'azienda Esse-ti S.r.l.
In questo elaborato verranno esposte le principali fasi del progetto realizzato, ponendo un particolare focus sulle problematiche iniziali affrontate e all'architettura di rete nel cui ambito è stata realizzata la comunicazione tramite un canale sicuro.

Indice

Elenco delle figure

Nella didascalia di ogni immagine vi è il link della pagina web da cui è stata presa, inoltre, sono citate anche accanto ai link nella sitografia.

Capitolo 1

Introduzione

1.1 Scopo e analisi del progetto

Nell'ambito di una convenzione stipulata con il Dipartimento di Ingengeria dell'Informazione, l'azienda **Esse-ti S.r.l.** ha esposto il suo progetto di fornire ad un certo gruppo dei propri clienti un router 4G per permettere di raggiungere e controllare dispositivi domotici, cablati e non, esterni alla rete locale dell'utente. Il gateway fornito al cliente risulta dotato di una batteria e di uno slot SIM quindi in grado di connettersi a *global internet* attraverso una connessione geografica radiomobile, in particolare mediante la connettività 4G garantita da un *Internet Service Provider* nazionale. Questa caratteristica permettere ai dispositivi connessi al gateway di fruire di un accesso ad internet e della possibilità di gestire comunicazione vocali, con il vantaggio di essere indipendenti da eventuali guasti che possono occorrere all'alimentazione elettrica o alla connettività via cavo nel luogo d'installazione dell'apparato.
Il lavoro si è focalizzato sul rendere possibile una comunicazione sicura tra un calcolatore autorizzato del cliente, situato nella rete locale dello stesso, e un dispositivo installato in un'altra sede fisica connesso al gateway fornito, nonostante le reti dei grandi provider mobili adottino nella maggior parte dei casi l'uso del protocollo **CG-NAT**, che impedisce la comunicazione diretta tra i due *end-point* della trasmissione. Per realizzare questa particolare configurazione di rete è stato perciò necessario utilizzare un server esterno dotato di un indirizzo IP pubblico, appoggiandosi ad un servizio *VPS* fornito in particolare dal provider **OVHCloud**. In seguito si è dovuto provvedere alla creazione di una connessione sicura per i dati nel trasito attraverso la rete pubblica dal calcolatore del cliente al cloud server e infine dallo stesso al device domotico finale. Una volta ottenuto l'accesso all'istanza server remota, dopo una verifica delle caratteristiche computazionali e di compatibilità software della stessa, si è deciso di adottare la suite open-suorce **OpenVPN** per l'implementazione dei tunnel cifrati attraverso i quali instaurare la comunicazione; questo software, a configurazione conclusa, garantirà un canale virtualmente diretto tra i due *end-point*, in altre parole essi risulteranno connessi ad una stessa rete locale.

Per la realizzazione e la verifica della configurazione richiesta, la problematica è stata schematizzata in una topologia di rete di test facendo le seguenti semplificazioni ed osservazioni:

- Ogni cliente ha accesso ad un unico gateway remoto;
- Ogni gateway è caratterizzato da più interfaccie, una di queste è connessa a global internet tramite la tecnologia radiomobile;

- Le restanti interfaccie del gateway sono tutte caratterizzata da uno spazio degli indirizzi privato, in generale ad esse possono essere collegati diversi dispositivi;
- La connessione sicura dal calcolatore del cliente al server remoto sarà di facile configurazione tramite l'interfaccia grafica del software OpenVPN;
- Dovrà essere possibile raggiungere dall'elaboratore del cliente, con il comando di debug *ping*, uno dei device connessi al gateway remoto, garantendo la bidirezionalità della comunicazione.

Di seguito (Figura 1.1) viene proposto lo schema di principio che permette di realizzare la comunicazione desiderata con i vincoli posti, adottando le tecniche già citate.

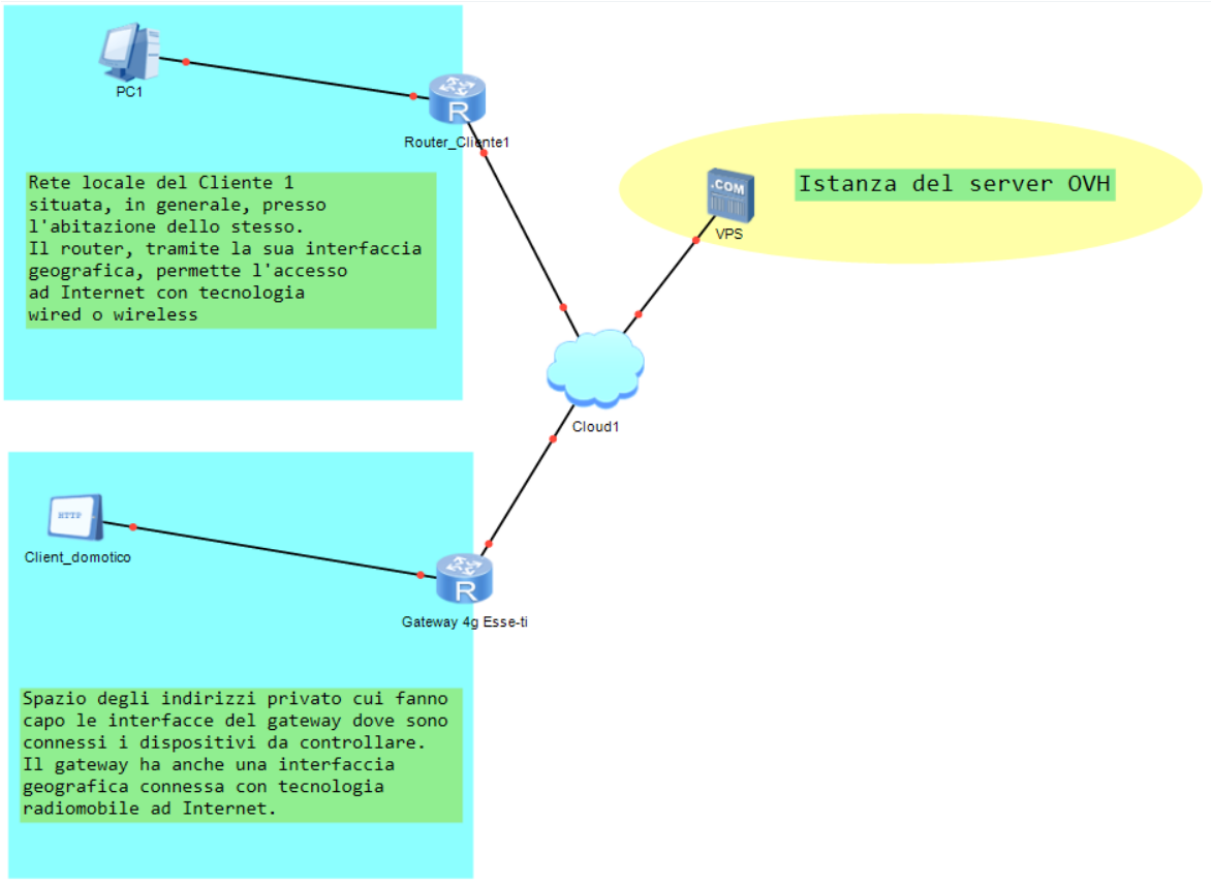

Figura 1.1: Topologia di rete di principio adottata per la comunicazione

1.2 Generalità sui servizi VPS e caratteristiche del particolare servizio scelto

Per realizzare la comunicazione progettata si è evidenziata la necessità di un server remoto, che provveda a veicolare i dati tra i due *end point* della comunicazione. In particolare l'azienda ha

richiesto un servizio che, seppur costoso, sia in grado di garantire un'alta affidabilità, bassa latenza e che in generale ponga pochi vincoli ad ulteriori e futuri sviluppi (quali ad esempio VNC o un servizio di desktop remoto), sia in termini di prestazioni offerte, sia in quanto a banda garantita. Ad una prima analisi, ci sono 3 grandi player che offrono sul mercato servizi cloud altamente configurabili, potenti e granitici: *Amazon AWS*, *Microsoft Azure* e *Google Cloud*. I prezzi proposti variano molto in base al servizio richiesto, abbiamo importi contenuti per macchine che lavorano a "trigger", fino a cifre più importanti per macchine always-on che riservano staticamente delle precise risorse; inoltre è possibile anche configurare dei limiti di budget con i relativi avvisi. In una successiva discussione si è deciso di usare un servizio più economico per le finalità di test preposte, e la scelta si è orientata su due provider in particolare, Aruba ed OVHCloud, che offrono entrambi un ampia gamma di server privati virtuali, con molte opzioni configurabili.
L'adozione di un *Virtual Private Server* mette a disposizione una singola istanza di un sistema operativo che viene eseguito in ambiente virtuale, di conseguenza più VPS possono essere eseguiti contemporaneamente sullo stesso hardware fisico. Questa caratteristica permette di lavorare in maniera del tutto indipendente dai vincoli associati all'hardware (evoluzione o upgrade dei componenti, malfunzionamenti tecnici, monitoraggio dello stato dei Dischi, RAM e CPU ecc...) dato che le singole istanze possono risultare anche migrabili su diverse macchine fisiche. Si ha così il vantaggio di avere un controllo totale sul proprio server per finalizzare al meglio i propri obiettivi, pur mantenendo nella maggior parte delle situazioni le performance di un ambiente dedicato. I costi minori dovuti alla condivisione tra molte istanze di uno stesso hardware fisico permettono l'accesso ai clienti finali a piani che possono anche essere molto economici. In generale le VPS sono adatte alla maggior parte degli utilizzi Web e per progetti di dimensioni contenute, anche in ambienti di produzione dove possono garantire delle prestazioni costanti, bisogna però dimensionare le caratteristiche del servizio scelto in base agli applicativi da eseguire. L'utilizzo di un VPS richiede delle discrete competenze in amministrazione di server, in particolare queste nozioni sono fondamentali per gestire il sistema operativo della macchina virtuale, installare e configurare applicazioni. Nel nostro caso andremo ad utilizzare il software OpenVPN per permettere la comunicazione sicura tra server e client, si richiede perciò una fondamentale esperienza nel networking e del funzionamento dello stack TCP/IP, per la configurazione del firewall e il debug.

Le soluzioni proposte per i server virtuali del provider OVH garantiscono prestazioni elevate, scalabilità, semplicità e la localizzazione presso un Data Center non in territorio Italiano, ma comunque Europeo per una buona latenza della comunicazione (le opzioni consigliate a riguardo sono Francia o Germania), il tutto ad un prezzo ragionevole, perciò si è deciso di appoggiarsi ai servizi proposti da questa azienda.
Tra le opzioni offerte da OVH per le istanze VPS, è stato concordato l'acquisto della VPS di gamma *Essential* con in più l'opzione di backup *Snapshot*: essa risulta essere un ottimo compromesso per l'ambiente di testing da predisporre, oltretutto disporre in anticipo di tutte le risorse non è essenziale: è infatti possibile aggiungerle quando necessario, direttamente dalla DashBoard dello spazio cliente, in questo modo la gestione del budget è più semplice. Ovviamente, in ambiente di produzione, quando si suppone che il traffico veicolato sarà decisamente maggiore con centinaia di host, una VPS con specifiche più generose di certo garantirà un servizio migliore per l'utente finale, ma questi aspetti esulano dal setup progettuale, per cui le risorse a disposizione con la macchina virtuale opzionata sono più che abbondanti.
Dal punto di vista tecnico, tutte le VPS offerte sono basate su architetture Intel di ultima generazione, con storage NVMe ed è possibile opzionare un'ampia scelta di distribuzioni Linux preinstallate, così come di interfaccie di gestione web. Di seguito (Figura 1.2) sono riepilogate le

Processore	1 vCore
Memoria	2 GB
Storage	40 GB SSD NVMe
Banda passante	250 Mbps illimitato*
Anti-DDos	✓
KVM	✓
Accesso root	✓
API	✓
Indirizzo IPv4	1
Indirizzo IPv6	/128
Localizzazione	8
Monitoraggio e interventi	24/7
SLA	99.9%

Opzioni disponibili

Indirizzo IPv4	2 € +IVA/IP cioè 2,44 € IVA incl./IP			
Snapshots	✓	✓	✓	✓
Dischi aggiuntivi	✓	✓	✓	✓
Backup automatizzato	✓	✓	✓	✓

Figura 1.2: Caratteristiche e opzioni agguntive disponibili della soluzione VPS acquistata (link)

principali caratteristiche del servizio acquistato. Tra le feature incluse spicca la banda passante al VPS, che è garantita e si riferisce alla velocità di trasmissione minima assegnata, inoltre è incluso il sistema di protezione *anti-DDoS OVHcloud*.
Una vasta gamma di sistemi operativi sono equipaggiabili per la macchina virtuale, quali Windows Server, Debian, Fedora, CentOS ed Ubuntu, in particolare si è scelto di adottare **Ubuntu 16.04 LTS**. Inoltre è da sottolineare che il *Service Level Agreement* per il servizio scelto è caratterizzato da un tasso di disponibilità mensile pari al 99,9%.
Una volta finalizzato il pagamento, viene fornito l'accesso alla dashboard principale del servizio scelto tramite lo spazio utente (Figura 1.3). Da qui, è possibile accedere al servizio acquistato direttamente con un *click* nella sezione server, ma anche alle ultime fatture pagate, nonchè andare a gestire tutto ciò che riguarda l'account utente con il pannello sulla destra della schermata. A partire dalla dashboard si individuano due aree diverse, una per la gestione del nostro account e le informazioni personali, l'altra per la gestione dei servizi acquistati. La dashboard per la gestione delle informazioni personali dell'utente permette di scaricare le fatture dei pagamenti effettuati i servizi attivi, con lo stato di funzionamento, e la modalità di rinnovo (manuale o automatica), inoltre è possibile modificare, aggiungere e rimuovere i metodi di pagamento ed infine di aprire e gestire eventuali ticket, sia per assistenza tecnica che assistenza commerciale, con i relativi contatti di supporto. Per quanto riguarda invece la gestione dei servizi acquistati come appunto VPS, server dedicati ecc., possiamo accedere, a partire dalla dashboard principale sotto la voce *My product and services*, ad un pannello di controllo generale dove è possibile selezionare quale prodotto, tra quelli acquistati, andare a gestire. Possiamo fare click direttamente

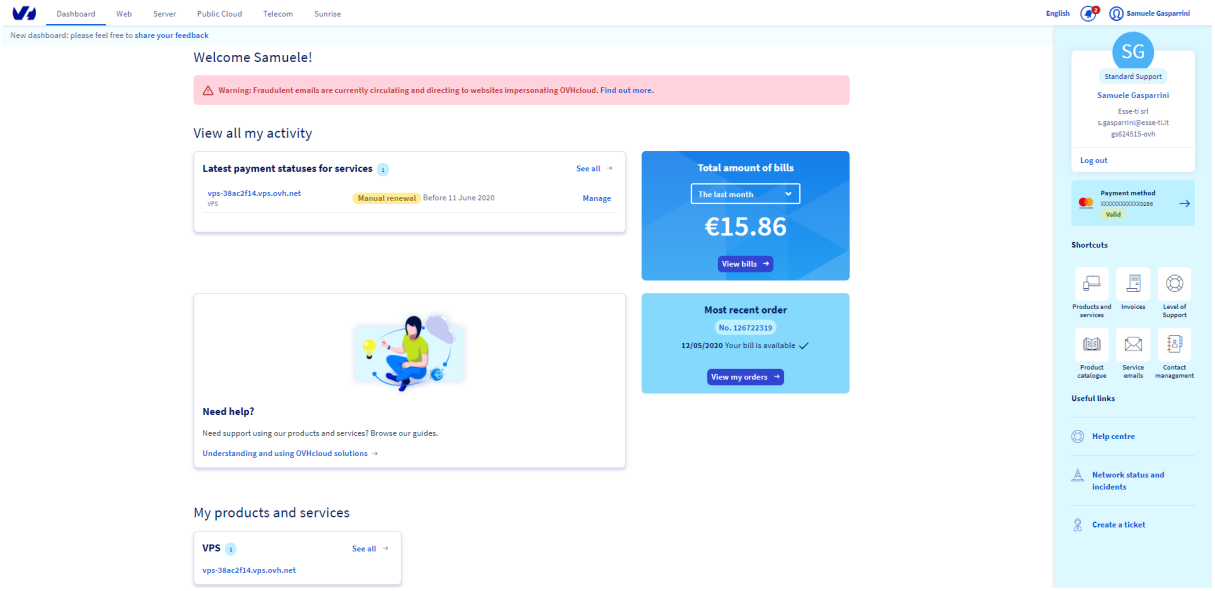

Figura 1.3: Dashboard OVHCloud

sull'hostname della VPS acquistata e verremo reindirizzati al pannello di riepilogo (Figura 1.4).

Esso presenta tutte le informazioni di cui possiamo aver bisogno per la gestione della nostra macchina virtuale, in particolare:

- informazioni sul sistema operativo;
- localizzazione fisica della *server farm* presso cui la VPS è installata;
- l'indirizzo IP attraverso il quale è possibile accede alla macchina remota tramite il protocollo sicuro SSH;
- un riepilogo delle opzioni attivate o disattivate che sono state opzionate all'acquisto della macchina, così come il piano attuale.

Come già evidenziato, con un paio di *click* è possibile fornire più risorse hardware, in termini di RAM o storage, alla nostra VPS, è inoltre possibile aumentare il numero di unità elaborative passando ad una VPS di livello superiore.

1.3 Caratteristiche del gateway adottato dall'azienda

L'azienda Esse-ti S.r.l. ha fornito due gateway con funzionalità di router identici, modello *4G.Router* (Figura 1.5), ognuno corredato di una SIM per la connessione all'operatore radiomobile partner. Il modello in questione offre connettività Internet e consente il telecontrollo dei dispositivi connessi via Wi-Fi, porta LAN o porta seriale. Ad oggi l'azienda impiega questo dispositivo nel panorama dell'IoT applicato al settore dell'elevazione, con funzionalità che spaziano in molti ambiti per garantire la massima flessibilità d'impiego:

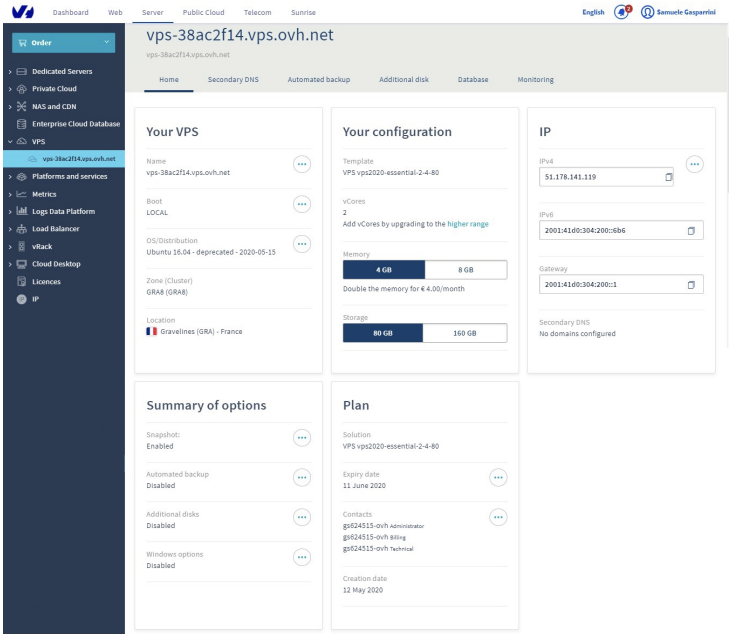

Figura 1.4: Pannello di controllo del servizio VPS acquistato

- Access Point wireless per offrire connettività Internet Wi-Fi a dispositivi wireless;
- Client Dynamic DNS per consentire all'utente di raggiungere da remoto, tramite Internet, il router stesso e tutti i dispositivi connessi via Wi-Fi o porta LAN;
- Trasmissione dati in standard RS-232/RS-485/CAN-bus per consentire all'utente di monitorare da remoto, tramite servizio COMNet, i dispositivi connessi alla porta seriale, oppure per consentire ai dispositivi connessi alla porta seriale di inviare automaticamente dati, segnalazioni, notifiche tramite servizio COMNet;
- Gateway telefonico per consentire l'invio e la ricezione di chiamate attraverso la rete 4G LTE/UMTS/GSM a telefoni fissi, combinatori o altri dispositivi telefonici collegati all'ingresso FXS, con la possibilità di visualizzare l'identificativo del chiamate;
- Gestione servizio roaming;
- Ingressi digitali programmabili, configurabili anche con antifurti tecnologici;
- Uscite relè attivabili localmente o via SMS, possono anche segnalare eventi come la mancata alimentazione e l'assenza di segnale radiomobile;
- Programmazione locale o remota del gateway telefonico tramite telefono (toni DTMF) o via SMS;
- Lettura programmazione via SMS;
- Invio di segnalazioni ed avvisi tecnici tramite SMS per il controllo della scandenza della scheda SIM, stato della batteria e dell'alimentazione esterna;
- Batterie interne di backup per garantire il funzionamento anche in assenza di alimentazione;
- Aggiornamento firmare *over-the-air*.

Figura 1.5: Gateway 4G.Router fornito ai clienti Esse-ti (link)

Le caratteristiche hardware del gateway includono:

- Modulo LTE Cat 1 Penta-Band / UMTS HSPA+ Dual-Band / GSM Dual-Band
- Frequenze LTE (700/800/900/1800/2100 MHz) / UMTS HSPA+ (900/2100 MHz) / GSM (900/1800 MHz);
- Velocità LTE Cat 1, download max. 10,2 Mbps / upload max. 5,2 Mbps;
- Wi-Fi 2.4 GHz - IEEE 802.11b/g/n con supporto ai protocolli di sicurezza WEP, WPA, WPA2, WPA-WPA2, WPA-WPA2-AES;
- Dotazione di ingressi e uscite:
  - Porta LAN con ingresso RJ45 10/100 Mbps;
  - Porta FXS (morsetto);
  - Morsettiera per trasmissione dati in standard RS-232, RS-485 e CAN-bus;
  - Due Uscite relè (NA e NA/NC; 1 A 24 V);
  - Due Ingressi optoisolati per allarmi tecnologici;
  - Porta micro USB A/B per connessione a pc;
  - Alloggiamento SIM Card;
  - Connettore antenne esterne SMA.
- Molteplici LED di segnalazione per stato del dispositivo, trasmissione dati COMNet, stato dell'alimentazione, livello del segnale radiomobile ricevuto, stato della linea telefonica connessa alla porta FXS;
- Alimentazione da 11 a 26 Vdc con apposito morsetto o tramite jack per alimentatore esterno 100-240 Vac;
- Batteria di backup a tecnologia Ni-MH con capacità di 800mAh a 7,2V che garantisce fino a 8 ore di funzionamento in stand-by o 2 ore di funzionamento attivo.