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

Design and implementation of a VPN "Hub & Spoke" Architecture for secure interconnection of geographically distributed sensor networks

Antonio Francesco Gentile[1],

RT-ICAR-CS-19-01 **Febbraio 2019**

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

Design and implementation of a VPN “Hub & Spoke” Architecture for secure interconnection of geographically distributed sensor networks

Esigenza di progetto

L’esigenza primaria di questo progetto era connettere in modo sicuro le sedi operative:

1. Unical Cubo 41C Ponte Pietro Bucci
2. Icar CNR (Unical Cubo 8/9C Ponte Pietro Bucci)
3. ITIS Monaco sito in Cosenza
4. Distaccamento “Chiodo 2” (Unical)
5. Rete di Sensori del progetto “Res Novae” (Corso Mazzini Cosenza) (in via di definizione)
6. Permettere un accesso Road Warrior

Panoramica della topologia VPN

Le VPN sono diventate un fattore molto importante sia per le aziende, sia per gli enti di ricerca. Soprattutto quando un progetto cresce, più siti remoti richiedono connettività verso i centri d’elaborazione dati e connettività mobile per gli utenti “road warriors”, e le VPN sono tecnologie indispensabili per supportare tale crescita in modo flessibile. Sono quattro le possibili implementazioni di servizi VPN:

- Site to site
  Permette la connessione tra due siti VPN collegati direttamente tra loro, nella stragrande maggioranza dei casi implementata via IPSEC mediante la creazione di criteri firewall in ingresso e in uscita per permettere il traffico dati tra i due endpoint.
- Hub and Spoke
  In questa topologia tutti i siti remoti si collegano alla sede centrale. Per uno scenario VPN multi sito questa è l'implementazione più comune, inoltre l’hub centrale permette la connettività dal sito remoto all'hub e dall'hub ai siti remoti e funge da gateway per i siti remoti per comunicare tra loro tramite l'hub.
- Road Warrior
  Quest’implementazione permette l’accesso alle risorse della rete interna da parte degli utenti che si trovano all’esterno dei network aziendali.
- VPN Mesh
  Questa topologia è la più complessa e fornisce la massima affidabilità, in quanto tutti i siti sono collegati tra loro senza hub. Nella precedente topologia Hub and spoke, se l'hub muore o c'è un problema di connessione all'hub, tutti i siti non avranno connettività. Tuttavia in questo caso non esiste un hub, quindi se un sito ha un guasto hardware, solo quel sito sarà inattivo, tutti gli altri siti possono ancora comunicare tra loro.

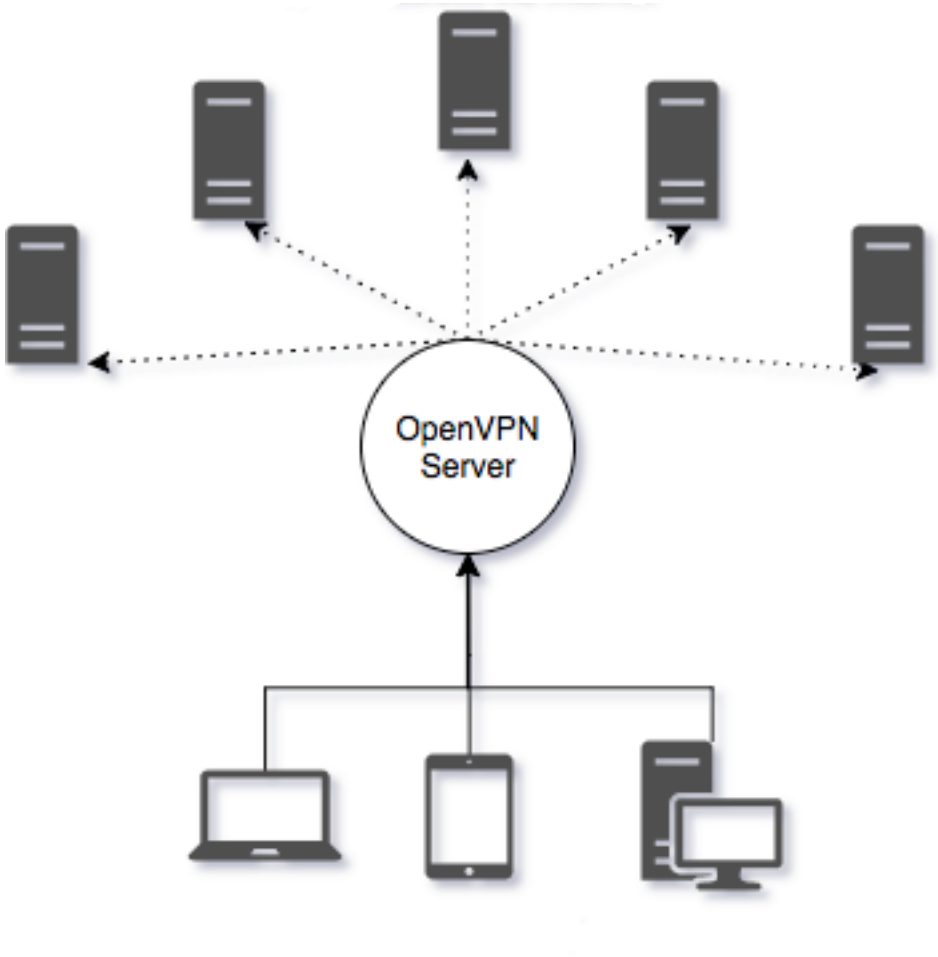
OpenVPN SSL VPN (Secure Socket Layer VPN)

SSL offre un'eccellente sicurezza per gli utenti di accesso remoto e facilità d'uso, Il deploy risulta più configurabile rispetto ad IPSec. Il traffico IPSec a volte è bloccato in luoghi pubblici come hotel, caffè ed uffici, mentre di solito quello SSL è sempre permesso.

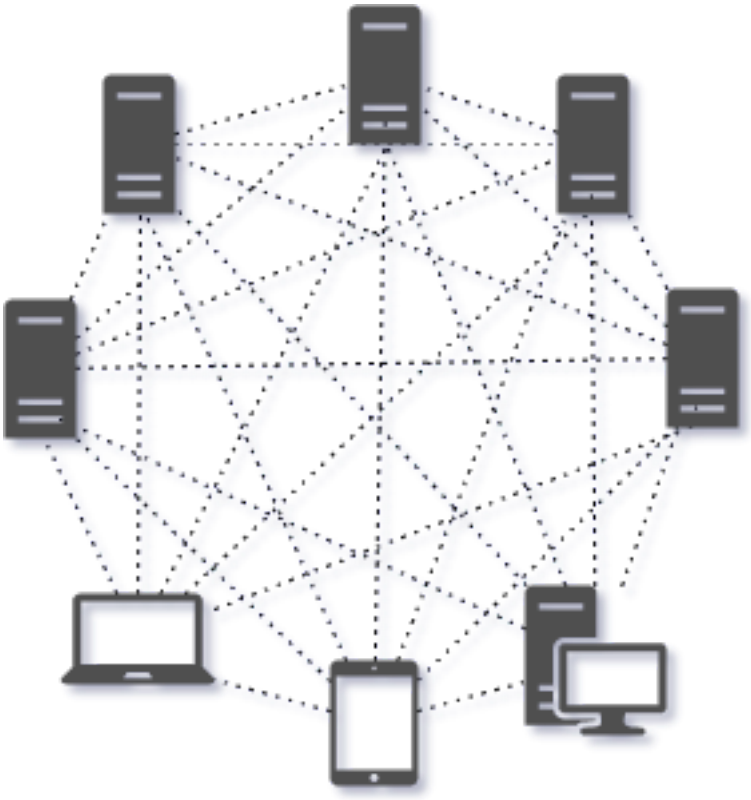
SSL VPN ha un controllo molto più stretto rispetto ad IPSEC e può essere configurato in modo tale che alcuni utenti ottengano l'accesso solo a determinate applicazioni e possano accedere alla rete solo se esistono apposite policy.

Un'implementazione di OpenVPN consente la portabilità tra sistemi operativi, operazioni firewall e NAT-friendly, supporto di indirizzi dinamici e supporto di più protocolli.

Ci sono vantaggi e svantaggi per entrambi gli approcci. I principali vantaggi dell'approccio di OpenVPN sono portabilità, facilità di configurazione e compatibilità con NAT e indirizzi dinamici.
Storicamente, uno dei vantaggi di IPSec è stato il supporto di più produttori, anche se questo sta cominciando a cambiare in quanto il supporto di OpenVPN sta iniziando a comparire anche su dispositivi hardware dedicati.



Configurazione hub-and-spoke di OpenVPN
Normalmente l'hub OpenVPN, diventa un "single point of failure", in quanto nelle architetture client-server, se il server non funziona, i client non riescono a comunicare con esso, per questo il sistema è stato pensato per avere (non al momento della scrittura del presente) più di un gw Openvpn a cui far capo, in modo da garantire affidabilità del servizio. Inoltre, appositi cronjob provvederanno a riallineare i dati dei server locali alla riconnessione, in caso di problemi sulle WAN.
La gestione di una CA e delle configurazioni / certificati client dell'infrastruttura OpenVPN non è un compito banale, e per facilitare la gestione sono stati creati script ad-hoc per la gestione dei client roadwarriors e dei singoli hub periferici.



Rete mesh (Res Novae lungo Corso Mazzini)

Ogni sistema sulla rete mesh può comunicare in modo sicuro con ogni altro sistema. Ciò significa che le app non sicure possono comunicare all'interno della rete senza il rischio di intercettazione. La scelta di OpenVPN permette di avere:

- Supporto nativo in ambienti NAT (network address translation)
- Supporto nativo per indirizzi IP dinamici
- Monitoraggio robusto della connessione e riconnessioni automatiche
- Assegnazione degli indirizzi ip in base al common name
- Granularità estrema nell'assegnazione dei network / servizi raggiungibili dal singolo host/LAN
- Autenticazione a due fattori per maggior sicurezza
- Capacità di interconnettere network geograficamente distinti con la minima interazione lato sede periferica
- Tutto il traffico tra le sedi fluisce esclusivamente via VPN

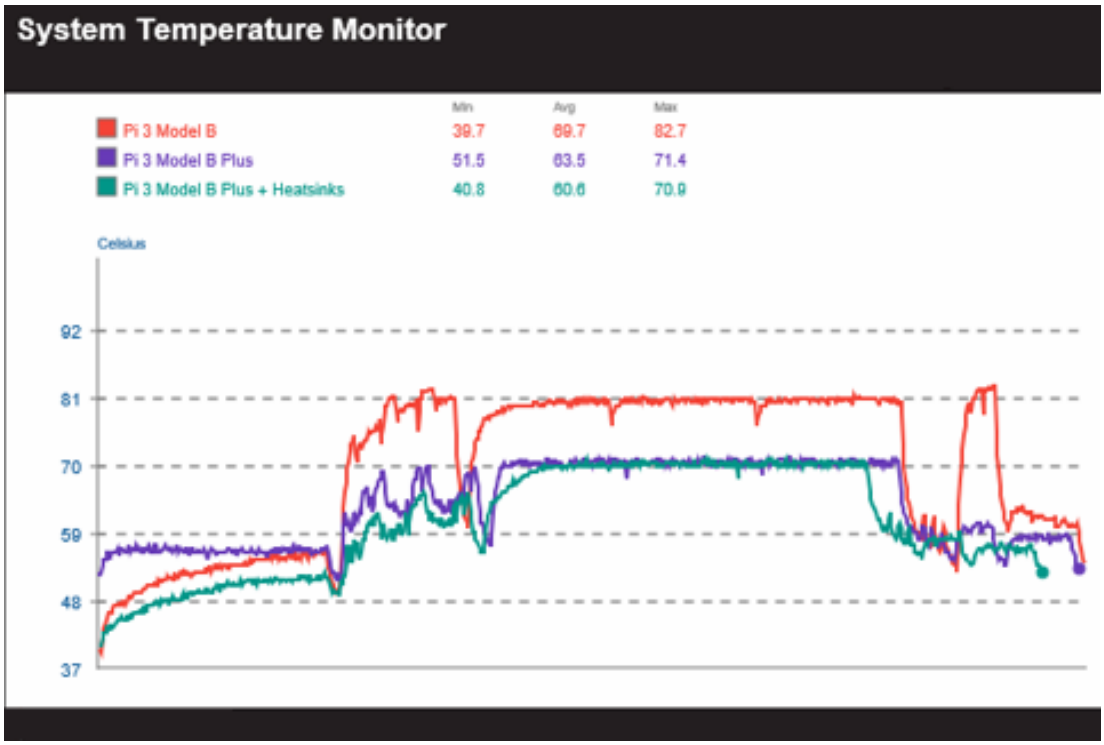
In quest'architettura, si realizza un ambiente ibrido hub e spoke in cui molte reti di sensori periferiche si connettono a una singola sede centrale e VPN mesh in cui ogni sito si collega a tutti gli altri siti locali, e da un hub generale al data center di destinazione.

Hw / Sw dei nodi Hub periferici
La scelta del dispositivo su cui installare gli Hub periferici è caduta sulle Raspberry Pi3 B+ perché offrono un buon compromesso qualità prezzo e sono relativamente poco invasive, potendo comodamente essere installate in un rack oppure in un qualsiasi punto raggiungibile dalla copertura di rete locale.

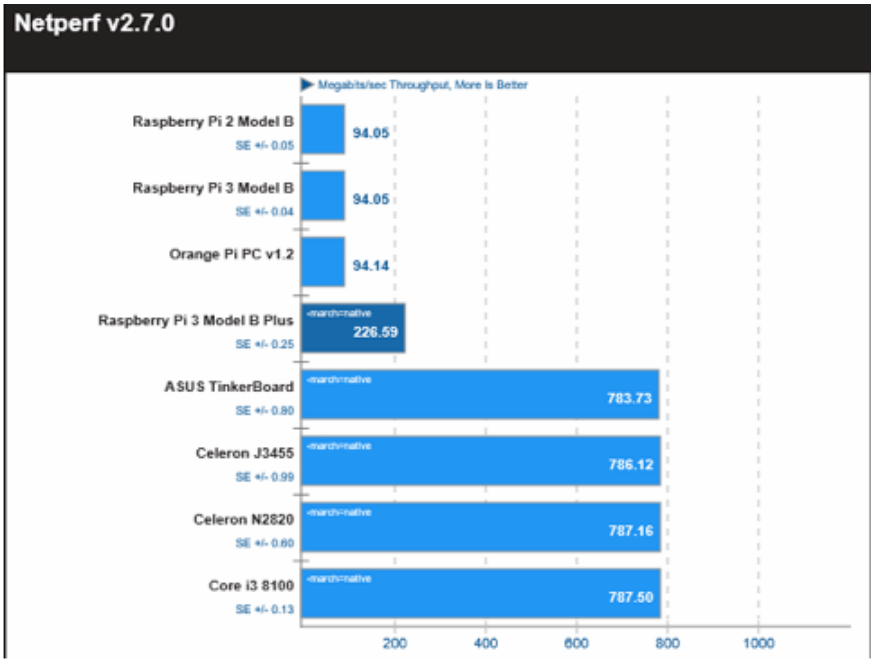
Sia sul server principale, sia sugli Hub periferici sia sui client è stato installato OpenVPN 2.4.x. La connettività è stata testata sui seguenti S.O. con esiti positivi:

- Debian 9.x
- Centos 7.x
- Archlinux (latest)
- Windows 10 (client)
- OSX 10.13.6 (tunnelblick)
- Raspberry Pi 3 B+

Benchmark delle temperature del SoC quad-core Broadcom, migliorate sotto carico; il grafico a seguire vede un confronto con Raspberry Pi 3 e lo stesso Model B3+.



Performance di rete



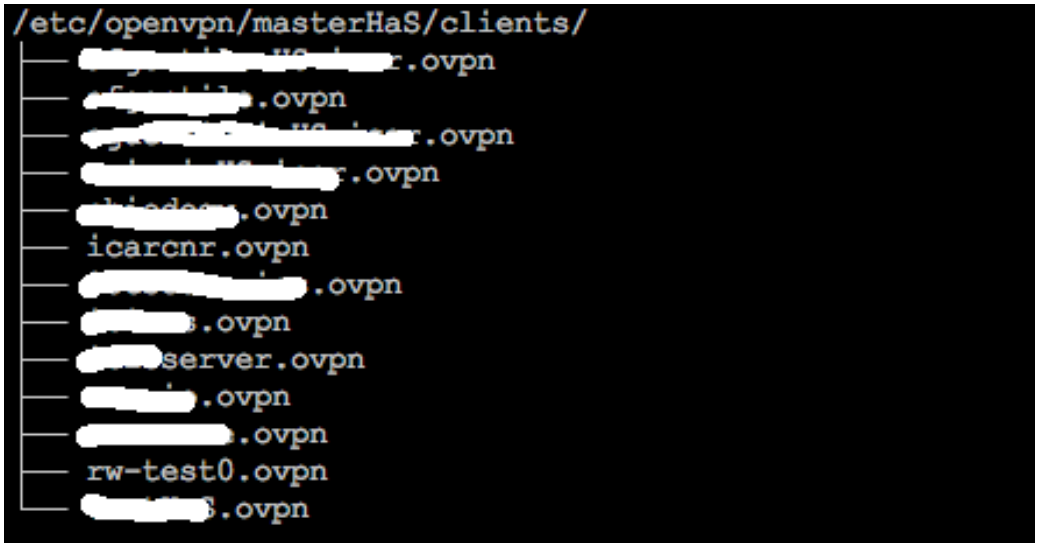
Configurazione del Master Server

```
# OpenVPN masterHaS.conf
dev tun
persist-key
persist-tun
topology subnet
port 443
proto tcp
keepalive 10 120

ca /etc/openvpn/masterHaS/easy-rsa/keys/ca.crt
cert /etc/openvpn/masterHaS/easy-rsa/keys/masterHaS.crt
key /etc/openvpn/masterHaS/easy-rsa/keys/masterHaS.key
dh /etc/openvpn/masterHaS/easy-rsa/keys/dh2048.pem

# The VPN's address block starts here.
server K.W.Y.0 255.255.255.0
#explicit-exit-notify 1

user openvpn
group openvpn

persist-key
persist-tun

client-to-client
duplicate-cn
#comp-lzo
#comp-lzo
#comp-lzo adaptive
client-config-dir /etc/openvpn/masterHaS/ccd
username-as-common-name
plugin /usr/lib/openvpn/openvpn-plugin-auth-pam.so login

tls-crypt /etc/openvpn/masterHaS/easy-rsa/keys/ta.key
auth SHA512     # This needs to be in client.ovpn too though.
tls-version-min 1.2
tls-cipher TLS-DHE-RSA-WITH-AES-256-GCM-SHA384:TLS-DHE-RSA-WITH-AES-256-CBC-SHA256
ncp-ciphers AES-256-GCM:AES-256-CBC

script-security 2
```

```
#push "redirect-gateway def1"
push "dhcp-option DNS A.B.C.D"
push "dhcp-option DNS E.F.G.H"

#
push "route K.W.Y.0 255.255.255.0 10.0.0.2 1"
…
push "route X.Y.Z.0 255.255.255.0"
…
```

Qui sono pubblicate le varie rotte di comunicazione tra tutte le sedi dell'architettura.

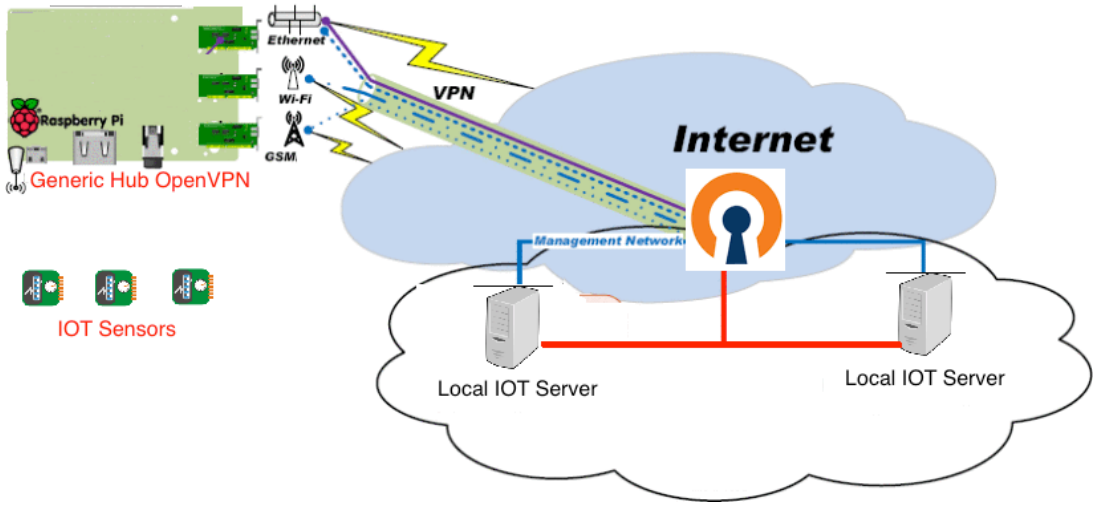
```
…
push "route X.Y.Z.0 255.255.255.0"


# Logging options.
ifconfig-pool-persist /etc/openvpn/masterHaS/ipp.txt 0
status /var/log/openvpn/masterHaS/masterHaS-status.log
log /var/log/openvpn/masterHaS/masterHaS.log
verb 3
```



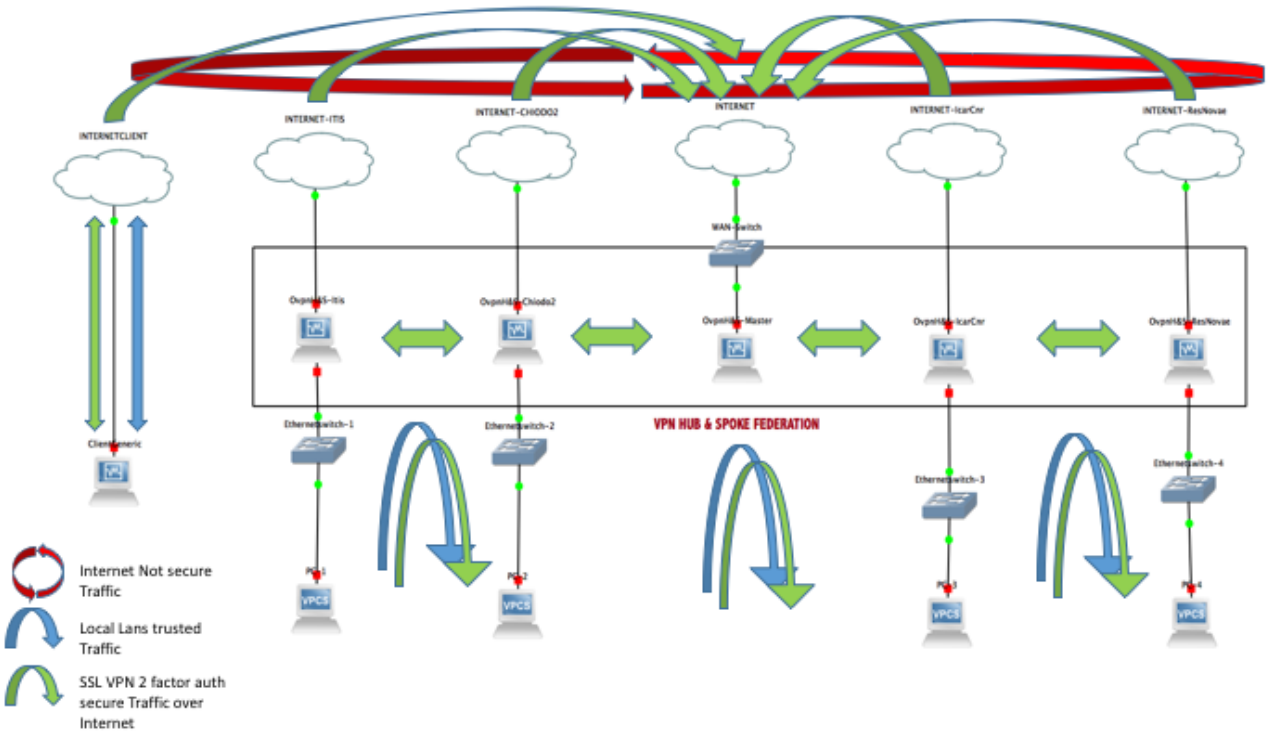
I raspberry Pi 3 che fungono da Hub sono configurati in modo da permettere la comunicazione tra sedi intra vpn mediante apposite configurazioni nella client configuration directory del server OpenVPN principale di cui segue un esempio:

```
root@fgwg-ovpnmaster:/etc/openvpn/masterHaS/ccd# cat rw-test0
ifconfig-push K.W.Y.5 255.255.255.0
iroute 10.1.Z.0 255.255.248.0
```

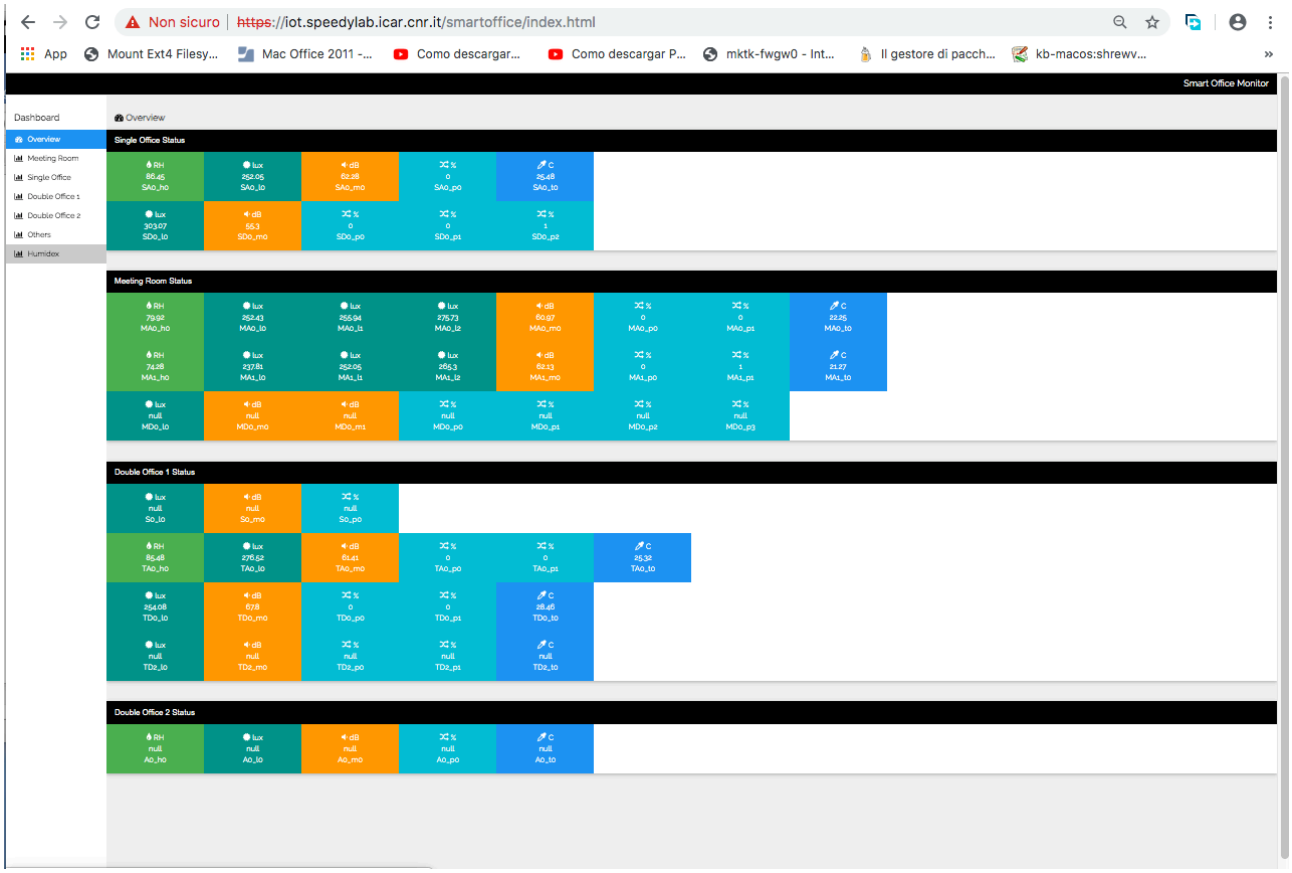
Utilizzando un approccio di tipo routed VPN si rende più semplice procedere al deploy e si crea un'architettura effettivamente indipendente dal tipo di connessione che userà il raspberry in rete locale (LTE/3G WIFI ETHERNET).



L'architettura finale, già funzionante eccetto per le subnet di Corso Mazzini (tempi burocratici di accesso ai locali) è quella in topologia:



I dati vengono trasferiti alla piattaforma interna sul server https://iot.speedylab.icar.cnr.it



Ing. Antonio Francesco Gentile