WIREGUARD PROTOCOL

WHOLESALE WINERY FT Tour

Pasquale Troccoli

Wireguard - Analisi e case study

ITNOG ON THE ROAD

CHI SIAMO


Concessionaria licenze Lucy Radius e Lucy Hotspot
TSI
Progettazione di rete e consulenza
Peering9
Consulenza Software & Cloud Interventi Namex

Cos’è Wireguard?

- Tunnel L3 con supporto a IPv4 e IPv6
- Focus su sicurezza e velocità
- Basato su UDP
- Implementato nel kernel linux dalla versione 5.6
- Implementato come interfaccia di tipo tun

Caratteristiche

Auditability

- Open Source
- ~4000 linee di codice (minore superficie di attacco)
- Possibilità di essere analizzato anche da 1/2 persone anziché un grosso team

- Comparazione
  OpenVPN: ~117.000 linee di codice
  StrongSwan: ~406.000 linee di codice

Sicurezza

- Curve25519: per lo scambio della chiave
  Come vedremo nella configurazione lo strato esterno utilizza la crittografia a chiave asimmetrica e mediante questa avviene lo scambio della chiave simmetrica condivisa
- ChaCha20: per la crittografia a chiave simmetrica del messaggio
- Poly1035: per l'autenticazione e garanzia di integrità

- Implementazione degli algoritmi di crittografia è di Daniel J. Bernstein, risalenti al 2008

Sicurezza

- ChaCha20

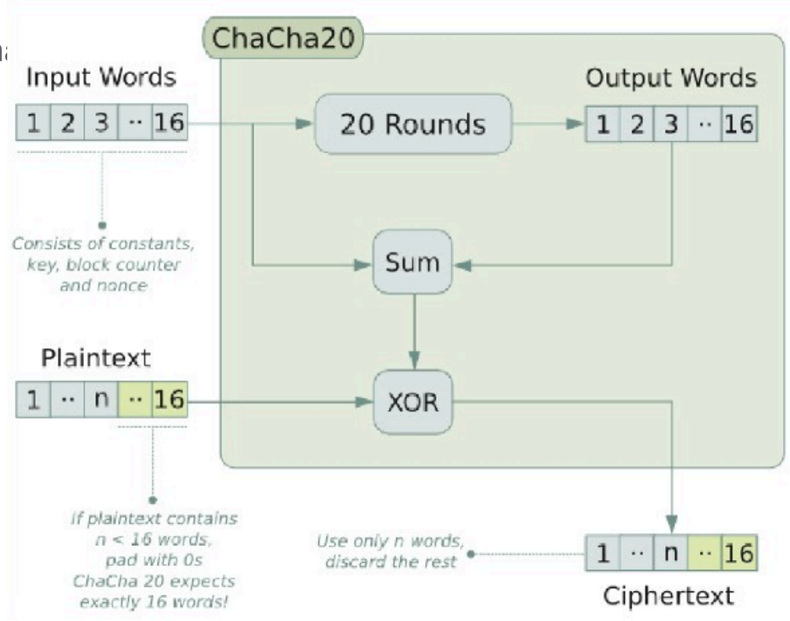
  Algoritmo a chiave simmetrica di 256 bit

  Inizialmente implementato come cifrario a flusso poi modificato in cifrario a blocchi

  Progettato per resistere agli attacchi conosciuti

  Altamente parallelizzabile quindi adatto alle moderne architetture con molti core

- Funzion



Input		Output
A	B	A xor B
0	0	0
0	1	1
1	0	1
1	1	0

Configurazione

- Estremamente semplice da configurare
- Utilizzo di una sola porta UDP
- Si presenta come un’interfaccia

Configurazione

- Server Config

  [Interface]

  PrivateKey =

  yAnz5TF+lXXJte14tji3zlMNq+hd2rYUIgJBgB3fBmk=

  ListenPort = 5062

  [Peer]

  PublicKey =

  4htodjb6e697QjLERt1NAB4mZqp8Dg=

  .150.0.10/32,10.200.0.0/24

- Client Config

  [Interface]

  PrivateKey = gI6EdUSYvn8ugXOt8QQD6Yc+JyiZxIhp3GInSWRfWGE=

  ListenPort = 21841

  [Peer]

  PublicKey = HIgo9xNzJMWLKASShiTqIybxZ0U3wGLiUeJ1PKf8ykw=

  Endpoint = 192.0.2.1:5062

  0.0.0/0

Configurazione su Mikrotik


```
/interface/wireguard
add listen-port=13231 name=wireguard1
```

Office1

```
/interface/wireguard print
Flags: X - disabled; R - running
 0  R name="wireguard1" mtu=1420 listen-port=13231 private-key="yKt9NJ4e5qlaSgh48WnPCDCEkDmq+VsBTt/DDEBWfEo="
      public-key="u7gYAg5tkicJDcm3hyS7pm79eADKPs/ZUGON6/fF3iI="

/interface/wireguard/peers
add allowed-address=10.1.101.0/24 endpoint-address=192.168.80.1 endpoint-port=13231 interface=wireguard1 \
public-key="v/oIzPyFm1FPHrqhytZgsKjU7mUToQHLrW+Tb5e601M="
```

Office2

```
/interface/wireguard/print
Flags: X - disabled; R - running
 0  R name="wireguard1" mtu=1420 listen-port=13231 private-key="KMwxqe/iXAU8Jn9ddlo5pPdHep2blGxNWm9I944/I24="
      public-key="v/oIzPyFm1FPHrqhytZgsKjU7mUToQHLrW+Tb5e601M="
/interface/wireguard/peers
add allowed-address=10.1.202.0/24 endpoint-address=192.168.90.1 endpoint-port=13231 interface=wireguard1 \
public-key="u7gYAg5tkicJDcm3hyS7pm79eADKPs/ZUGON6/fF3iI="
```

Prestazioni

- Implementato nel kernel
  I pacchetti non devono spostarsi più volte tra user space e kernel space
- Basato su UDP
- Tempo per stabilire una connessione
  Mediamente 100ms
- Capacità di attraversare firewall più facilmente (se non viene fatta DPI)

- IPsec si difende molto bene ma non sempre è disponibile l’instruction set per AES in hardware

Overhead

WIREGUARD

- 20-byte IPv4 header or 40 byte IPv6 header
- 8-byte UDP header

Wireguard (32 byte)

- 4-byte type
- 4-byte key index
- 8-byte nonce
- N-byte encrypted data
- 16-byte authentication tag

OPEN VPN

- 20-byte IPv4 header or 40 byte IPv6 header
- 8-byte UDP header

Open VPN (41 byte)

- 1-byte packet tag
- 20-byte HMAC SHA1 signature
- 16-byte initialisation vector
- 4-byte sequence number
- N-byte encrypted data

IPsec
Mode: Tunnel
Encryption: ESP-AES-128/192/256
Integrity: ESP-SHA-HMAC

- 20-byte IPv4 header or 40 byte IPv6 header

IPsec (52 byte)

- 8-byte ESP header
- 16-byte ESP IV
- N-byte encrypted data
- 28-byte ESP trailer (variabile)

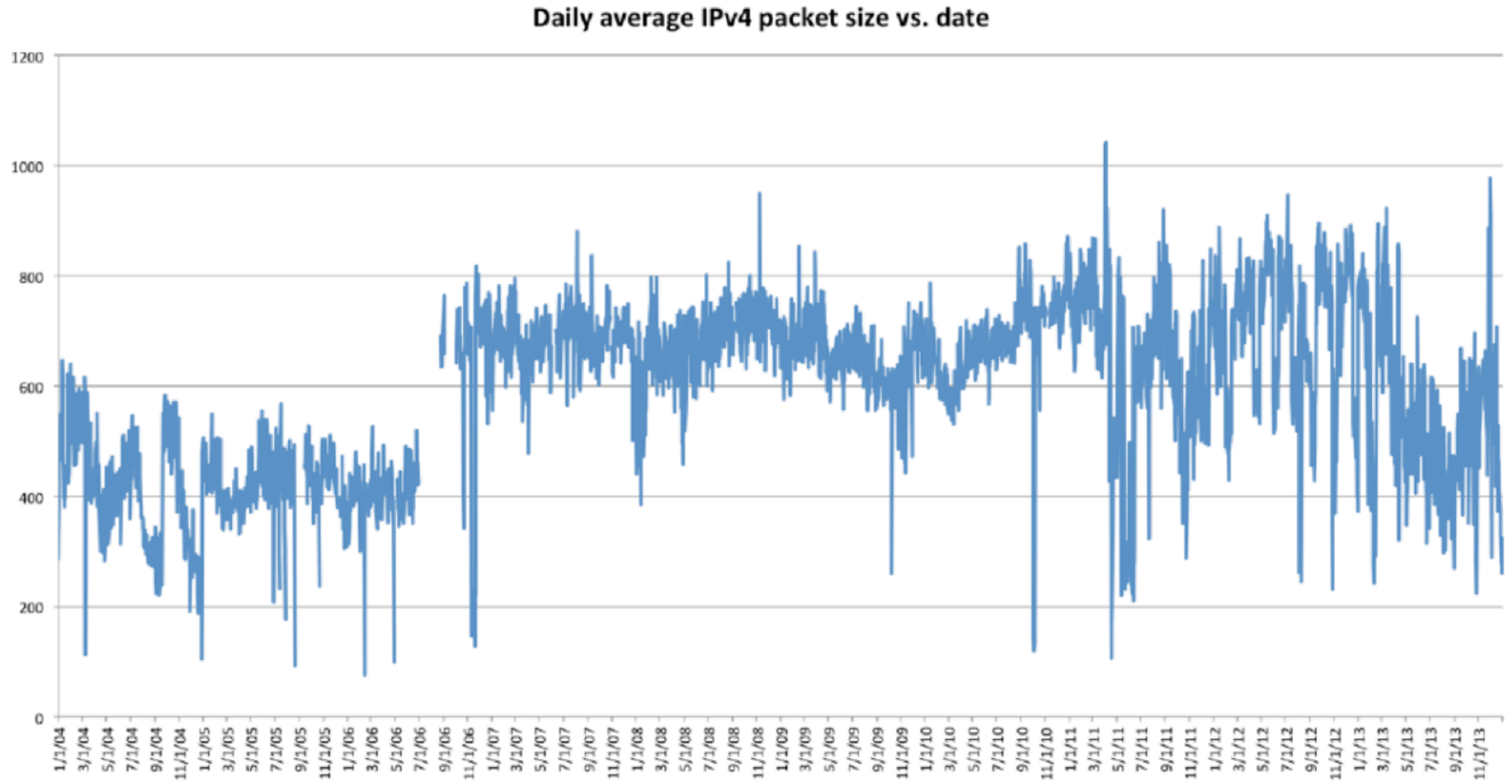
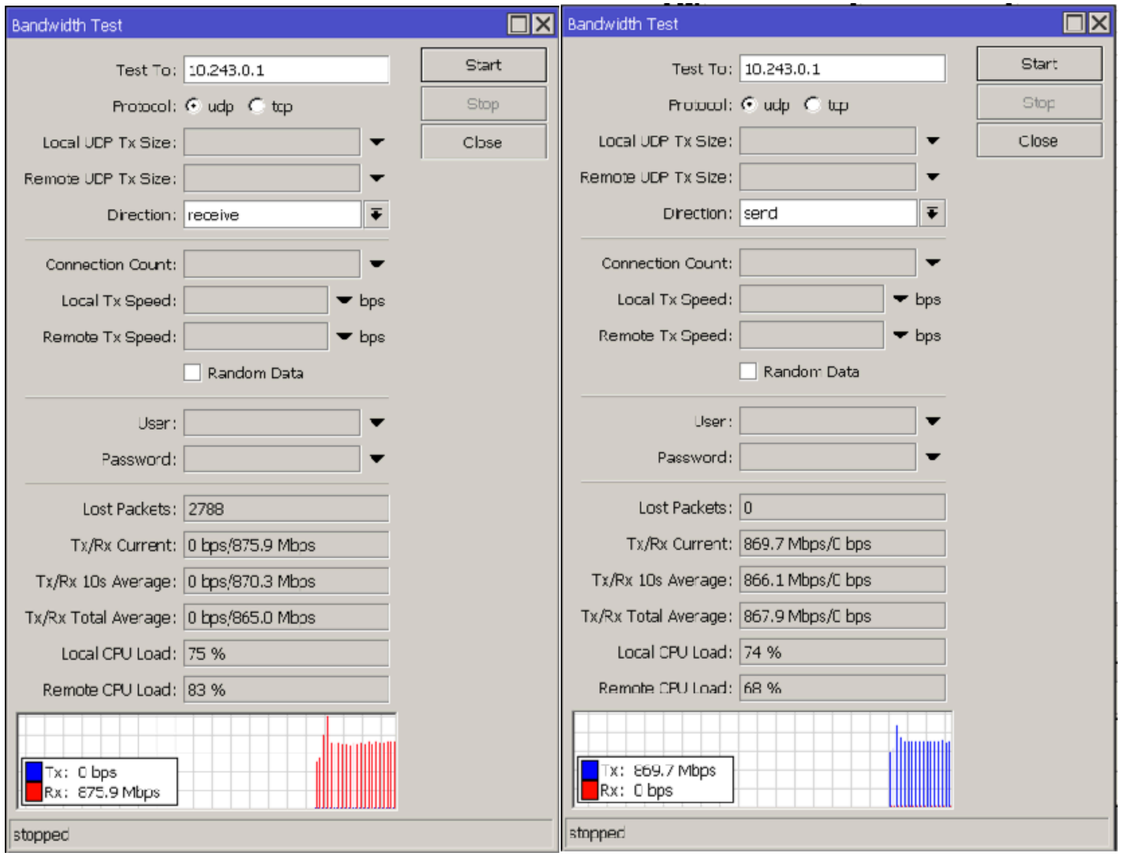


FIGURE 3. Average IPv4 daily packet sizes, between 1/1/2004 and 31/12/2013 (in Bytes).

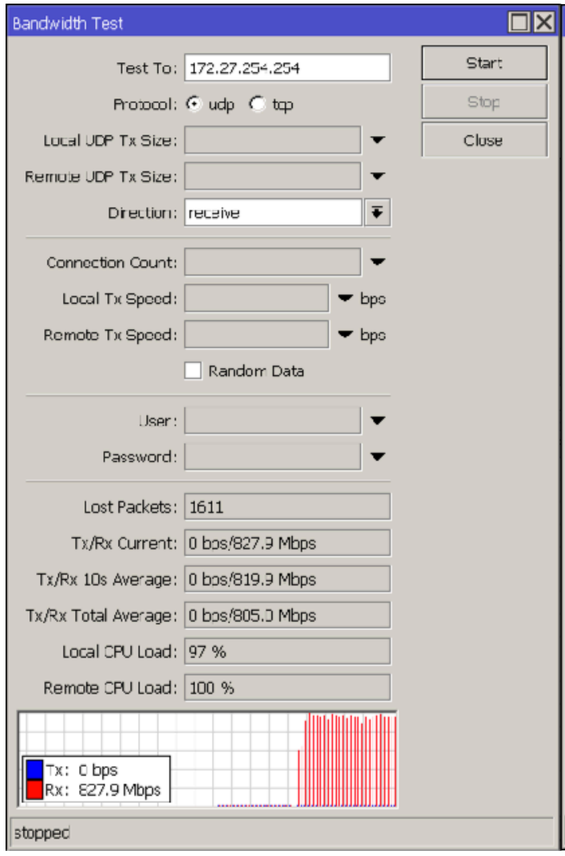
Fonte: https://www.researchgate.net/publication/330946435_Keyed_User_Datagram_Protocol_Concepts_and_Operation_of_an_Almost_Reliable_Connectionless_Transport_Protocol

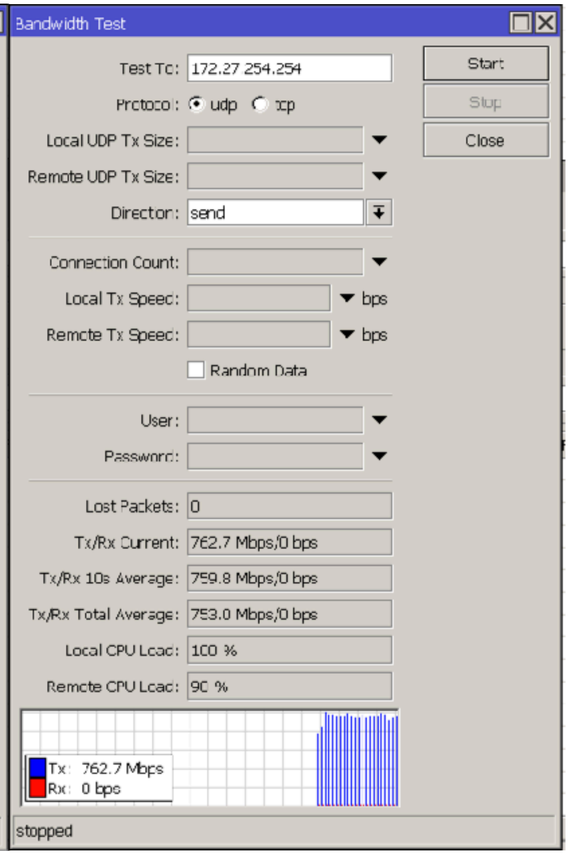
Test su Mikrotik

Test tra 2 CHR hostate su Aruba con 1 vCPU



Wireguard





IPsec AES256-CBC

Casi d’uso

- IOT
- VPN Site to Site
- VPN Road Warrior
- Implementazioni di custom SDWAN
- Efficiente in termini di overhead quando non sono disponibili routable interface

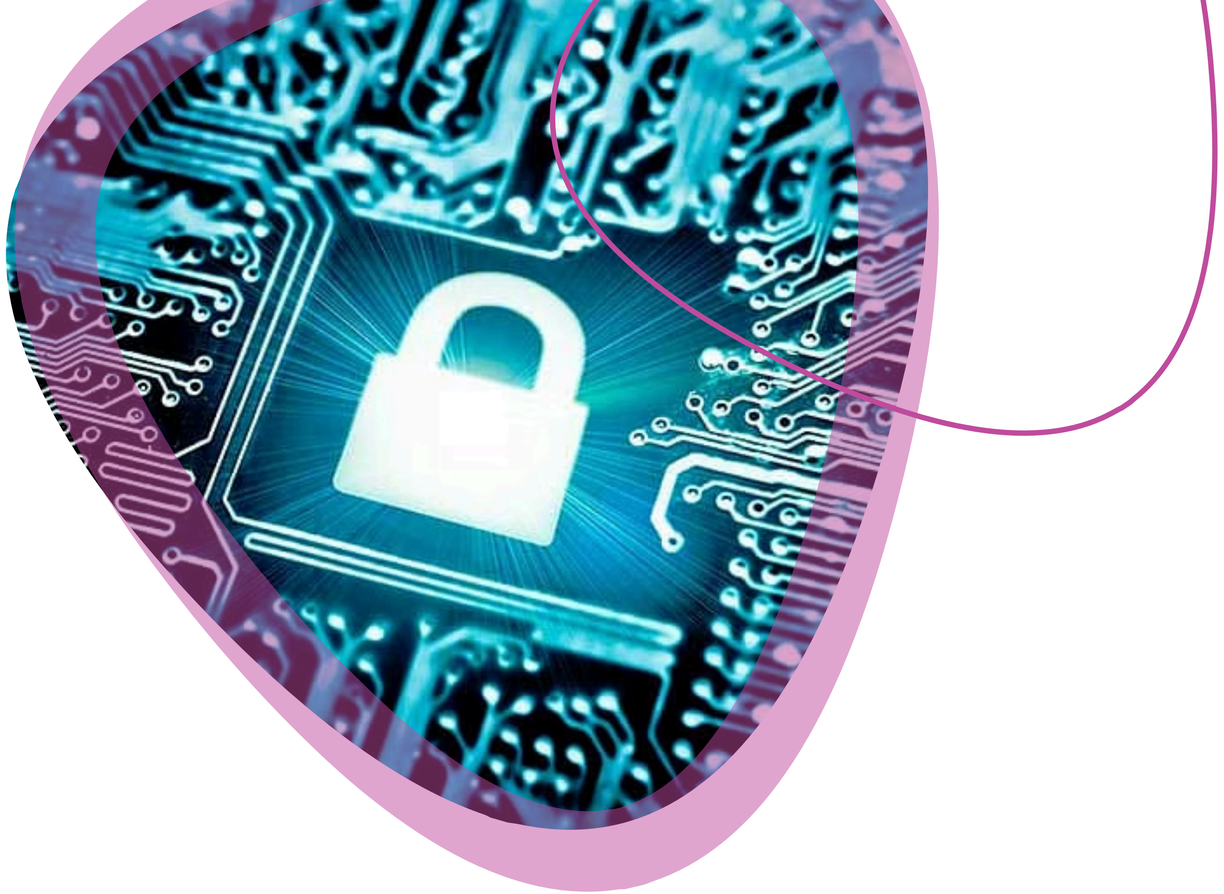
IPsec can provide either end-to-end security between nodes or channel security (for example, via a site-to-site IPsec VPN), making it possible to provide secure communication for all (or a subset of) communication flows at the IP layer between pairs of Internet nodes. IPsec has two standard operating modes: Tunnel-mode and Transport-mode. In Tunnel-mode, IPsec provides network-layer security and protects an entire IP packet by encapsulating the original IP packet and then prepending a new IP header. In Transport-mode, IPsec provides security for the transport layer (and above) by encapsulating only the transport-layer (and above) portion of the IP packet (i.e., without adding a second IP header).

Although IPsec can be used with manual keying in some cases, such usage has limited applicability and is not recommended.

A range of security technologies and approaches proliferate today (e.g., IPsec, Transport Layer Security (TLS), Secure SHell (SSH), TLS VPNS, etc.). No single approach has emerged as an ideal technology for all needs and environments. Moreover, IPsec is not viewed as the ideal security technology in all cases and is unlikely to displace the others.

Previously, IPv6 mandated implementation of IPsec and recommended the key-management approach of IKE. RFC 6434 updated that recommendation by making support of the IPsec architecture [RFC4301] a SHOULD for all IPv6 nodes, and this document retains that recommendation. Note that the IPsec Architecture requires the implementation of both manual and automatic key management (e.g., Section 4.5 of RFC 4301). Currently, the recommended automated key-management protocol to implement is IKEv2 [RFC7296].

This document recognizes that there exists a range of device types and environments where approaches to security other than IPsec can be

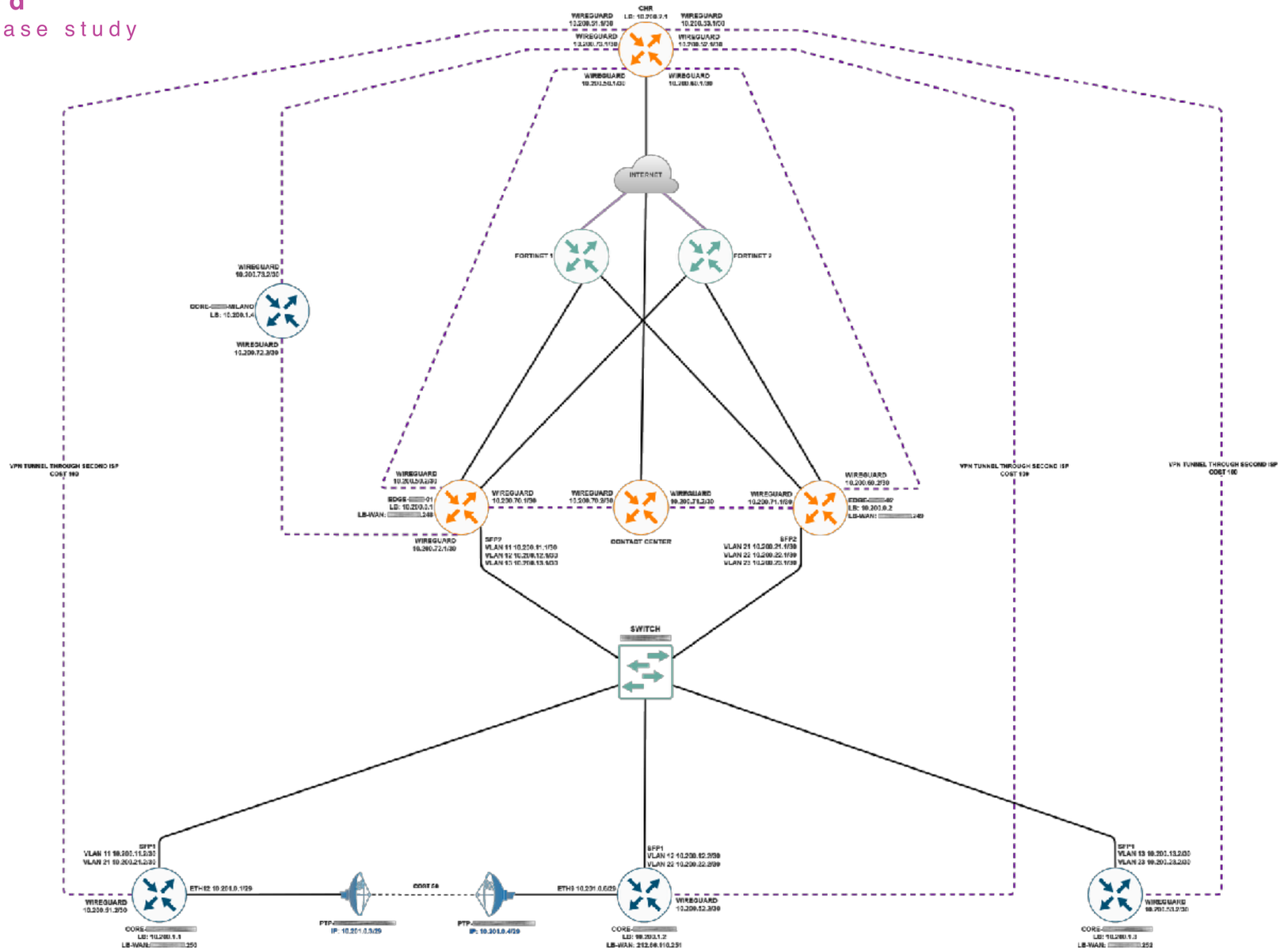


Svantaggi

- Solo Layer 3
- No offuscamento, i firewall che fanno DPI possono rilevarlo
- No indirizzi dinamici
- Niente stato, è un protocollo connection-less
- Mancanza di cipher agility

Wireguard

Analisi e case study



SEDI

3 sedi collegate in L2

1 sede collegata in L3

COLLEGAMENTI

Ogni sede dispone di una connettività secondaria fornita da un carrier diverso e su tecnologia differente

TUNNEL

In viola tratteggiato sono indicati i tunnel wireguard che vengono instaurati attraverso la connettività secondaria dalle sedi

SERVIZI

Server interni nelle sedi 1 e 2

Servizi cloud forniti dal contact center

ROUTING

OSPF (attenzione al tipo sulle interfacce wireguard)

MPLS tra le 3 sedi e l'edge

Le EDGE distribuiscono la default route

La CHR distribuisce una default con peso maggiore


troccolisistemi.com