- **FiberTelecom Winery Tour 2022 – 21 Aprile 2022**

CONNESI

BGP Security Automation for ISP

connesi®
TUTTI SEMPRE OVUNQUE

connesi

• Chi è Connesi S.p.A.

- Nasce nel 2007 come Wisp per fornire connettività in zone in digital-divide della zona
- Fin da subito è un operatore «infrastrutturato»
- 15 Anni di esperienza nel network building
- Focalizzato su servizi Business

• I nostri numeri

- 250 Radiofari
- 750 Km di cavi di fibra ottica
- 6.000 punti di consegna
- 54.600 Numerazioni Telefoniche
- 114.000 Utenti finali
- 300 POP
- 4 IXP
- 120 Gigabit di capacità alle frontiere

connesi

- I nostri obiettivi

- Net-Neutrality e il diritto di accesso alla rete
- Combattere il digital-divide
- Avanzamento tecnologico del territorio
- Realizzare Infrastrutture strategiche
- Essere protagonisti nella realizzazione dei servizi

Autonomous System

Routing Building

Ripe LIR

Open Peering Policy

Controllo sulla RT

Custom Routes

Operatore di Primo Livello

Basse latenze

Ottimizzazione Percorsi

IPv6

IXPs

La Open Peering Policy

Cosa vuol dire avere una Open Peering Policy

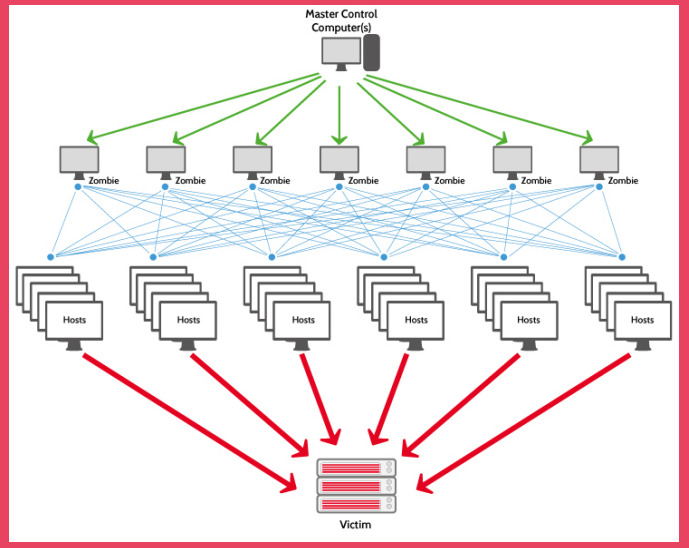
•Una Open Peering Policy è una policy di routing che ammette l'interconnessione diretta tra operatori senza limiti, senza prerequisiti su rapporti di Upload e Donwload o corrispettivi economici.
•Massimizzare il numero di collegamenti con altri operatori e produttori di contenuti
•Aumentare il valore della propria tabella di routing

La Open peering Policy è impegnativa...

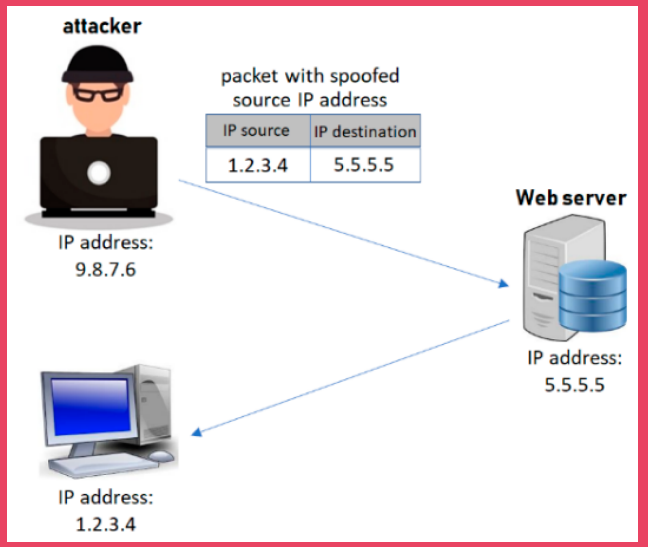
•«Da grandi poteri derivano grandi responsabilità»
•Alti costi di gestione e Personale NOC
•Troubleshooting problematico nel complesso
•Aumento consumi risorse router di frontiera (CPU, RAM, Dimensioni RIB)
•Alto rischio di errore umano
•Avere il controllo vuol dire dover fronteggiare le minacce

- Le minacce

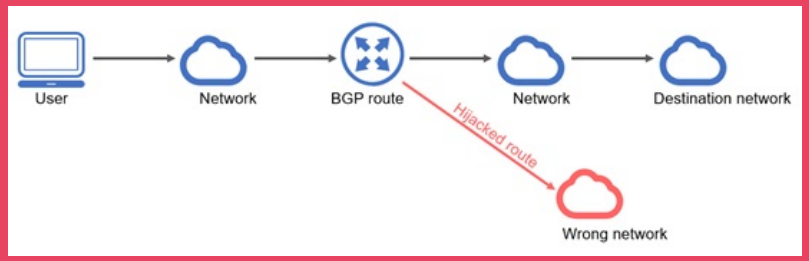
Attacchi DDoS



IP Spoofing



BGP Hijacking



Route Leaks

connesi

• Le Contromisure tradizionali

Attacchi DDoS e Spoofing

•Deployment Unicast Reverse Path Forwarding (uRPF)

•Monitoraggio e mitigazione attacchi tramite Black Hole Routes o BGP Flowspec

•DDoS Mitigation

BGP Hijacking

•Registrazione classi su database RPKI

•Discard delle rotte di tipo invalid

Route Leaks

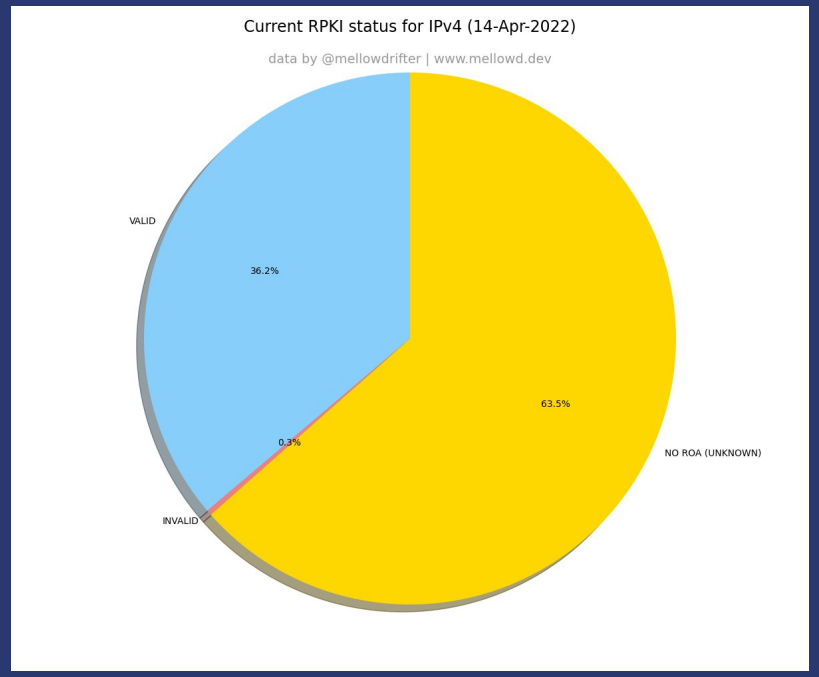
•Imposizione di limiti di tipo max-prefix

•Filtri su annunci e as-path

• Le Contromisure tradizionali non sono abbastanza...

- Le policy di filtraggio sono statiche e manca un sistema di «svecchiamento delle regole»
- Gli AS-SET, i prefissi e i parametri cambiano nel tempo con conseguente necessità di procedure per effettuare il change management mediante intervento umano

Diffusione RPKI Limitata
(63,5% dei prefissi NO ROA al 14-Apr-2022)



Anti-Spoofing non solo per il traffico generato
ma anche per quello ricevuto…

- La modalità loose di uRPF serve a poco alle frontiere per proteggersi dagli attacchi DDoS
- L'Impiego di ACL per permettere il traffico delle sole classi pubbliche è complesso in caso di fornitura di transiti e necessitano frequenti modifiche

<u>Serve un sistema automatico per
la generazione dei filtri di sicurezza</u>

• La piattaforma SDN

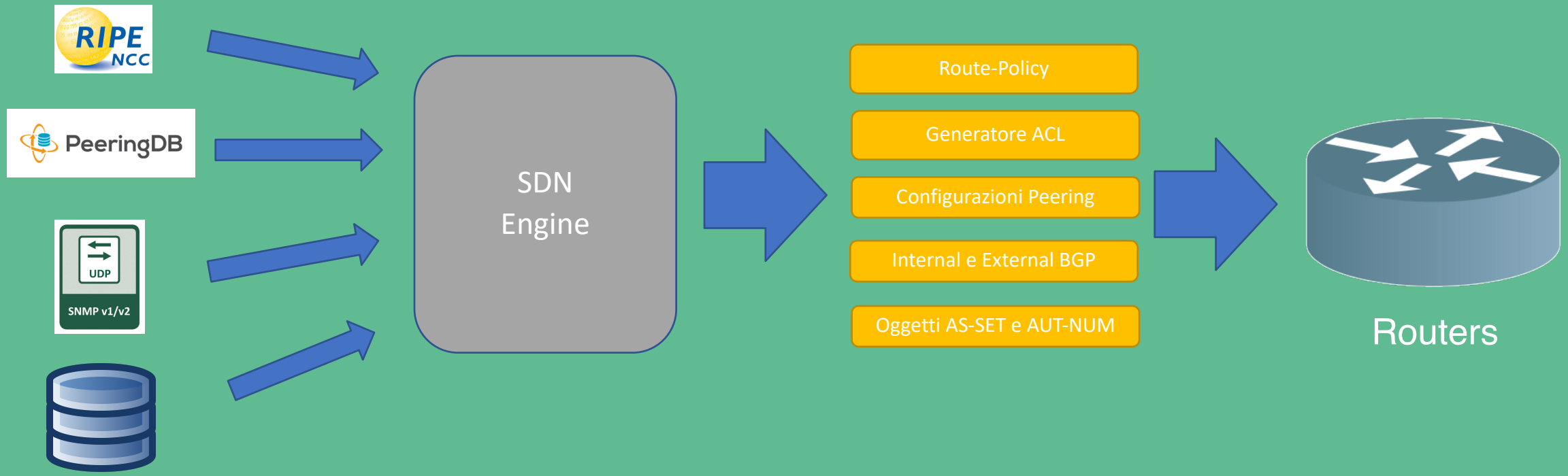
Deployment History

•Nasce come progetto di ricerca nel 2018 (prima release inizio 2019)

•Focalizzato su piattaforma IOS-XR ma compatibile anche con versioni precedenti (IOS, IOS-XE, NX-OS)

•Obiettivo è l'automazione per la configurazione e la gestione della sicurezza del protocollo BGP

•Sviluppo «agile» e continuo



• La piattaforma SDN – Data Gathering

Ripe DB e altri IRR

•Database «autoritativo» per prefissi e AS-SET

•Utilizza il protocollo WHOIS

•Traduzione AS-SET in prefix-lists con bgpq3

https://github.com/snar/bgpq3

PeeringDB

•Punto di partenza per AS-SET e Indirizzi IP destinati alle sessioni

•API molto ben documentate

•Base dati per max-prefix, peering contacts, nomi reti, IXP, e molto altro…

https://www.peeringdb.com/apidocs/

SNMP

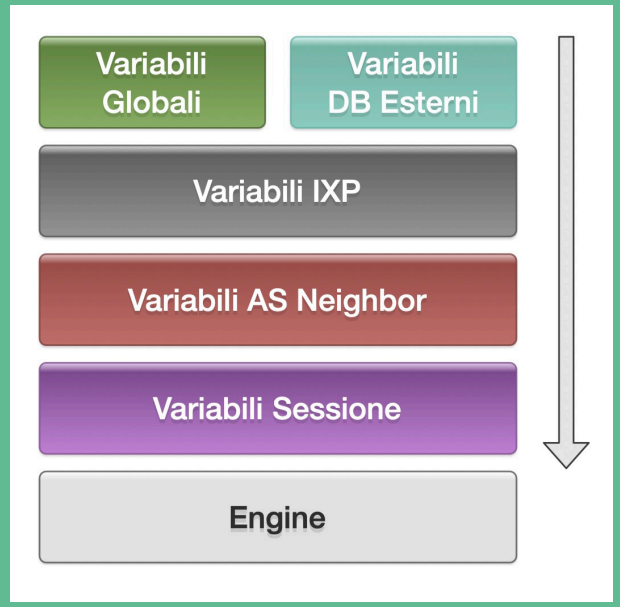
•Principale metodo per ottenere dati dagli apparati

•Standard «de-facto» per il monitoraggio

•Mib BGP4 standard e cross platform (ma non IPv6)

•Cisco ha esteso il mib con CISCO-BGP-MIBv2 (proprietario ma implementato anche da altri vendor)

Gerarchia delle Variabili



• La piattaforma SDN – L'Engine per la Sicurezza

Generazione di policy di routing e filtri per AS-SET o Prefix-list

```
as-path-set AUTO-AS39120
  # Convergenze S.p.A.
  # Autogenerated from AS-SET AS-CONVERGENZE
  ios-regex '^39120(_39120)*$',
  ios-regex '^39120(_[0-9]+)*_(24796|45015|49360|52054|56911|198128)$',
  ios-regex '^39120(_[0-9]+)*_(200345|203726|204739|205498|208642|210869)$'
end-set
```

Generazione delle ACL Anti-Spoofing sulle interfacce di transito

- Blocco delle classi Bogons (sia IPv4 che IPv6)
- Gestione classi degli AS per cui si fornisce transito
- Gestione classi di trasporto «esterne»
- Regole personalizzate per interfaccia e contesto

Templating delle Route-Policy

```
 set med <IXP_MED>
if as-path in <AS-PATH-SET> and as-neighbor is <NEIGH_AS> then
    set local-preference <IXP_LOCALPREF>
    set community <IXP_COMMUNITY> additive
    # Apply RPKI Filtering
    apply RPKI-POLICY
    pass
  else
    drop
  endif
```

- Policy di sicurezza definite a livello di IXP o di singolo Neighbor.
- Le variabili vengono sostituite in base alla gerarchia
- Gestione ricorsiva dei riferimenti a Route-Policy esterne
- Validazione Sintassi RPL

• La piattaforma SDN – L'Engine per l'Automazione

One-Click direct-peering

•Sincronizzazione dei parametri con RIPE e PeeringDB (max-prefix, as-set, Indirizzi, etc..)

•Definizione Policy di Sicurezza

•Generazione e upload configurazione

•Invio mail per la richiesta di peering

Gestione delle sessioni con i Route-Server IXP

•Gestione delle community per il controllo dei RS

•Sincronizzazione dei parametri con PeeringDB

Gestione dei internal BGP e dei route-reflectors

•Configurazione internal Peerings

•Configurazione peering vs i Route Reflectors

•Gestione prefissi e as-path da annunciare

Configurazione sempre personalizzabile

•Review della configurazione generata a schermo

•Gestione automatica per i riferimenti esterni delle route-map

•Comandi aggiuntivi opzionali per sessione peering (rotte statiche, opzioni bgp particolari, etc…)

•Override dei parametri ottenuti tramite data gathering

•Massima flessibilità per gli operatori NOC

• La piattaforma SDN – Router Programming Technique

Command Line Interface

•Trasporto SSH o Telnet

•Interfaccia più utilizzata

•Relativamente uniforme tra le release IOS-XR

•La configuration versioning di IOS-XR

•Il trattamento dell'errore è complesso

NetConf - RFC6241 e RFC6244

•Principalmente SSH + XML (o YANG)

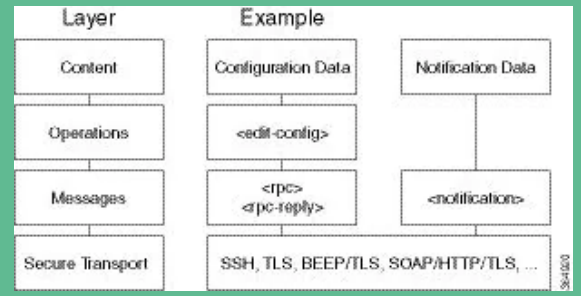
•Approccio a Layer

•Template XML essenziale

•Rigido e limitato

•Molto Sicuro

•Supporta meccanismi di locking della configurazione



gRPC

•Principalmente RPC over HTTP/2

•Implementazione Open Source

•Comunicazioni in binario

•Necessita di file che definiscono le features supportate per ogni versione di IOS-XR (come per NetConf)

RestConf – RFC8040

•HTTPS + JSON (o XML)

•La soluzione più facile da implementare (REST API)

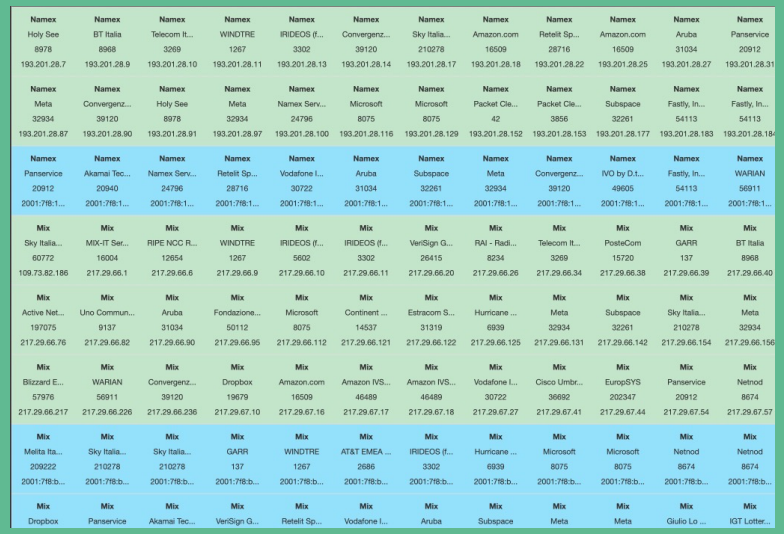
•Meno tempo di sviluppo rispetto Netconf o gRPC

•Non implementata in IOS-XR

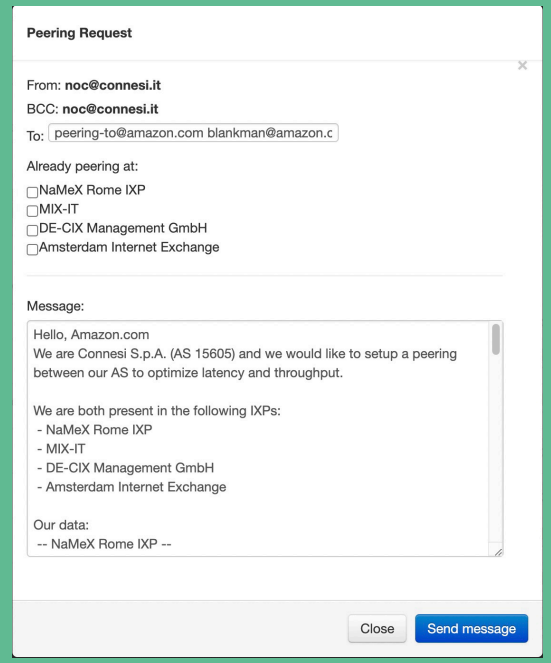
•Supportata da IOS-XE e NX-OS

• La piattaforma SDN – Non Solo Generatore di Configurazioni

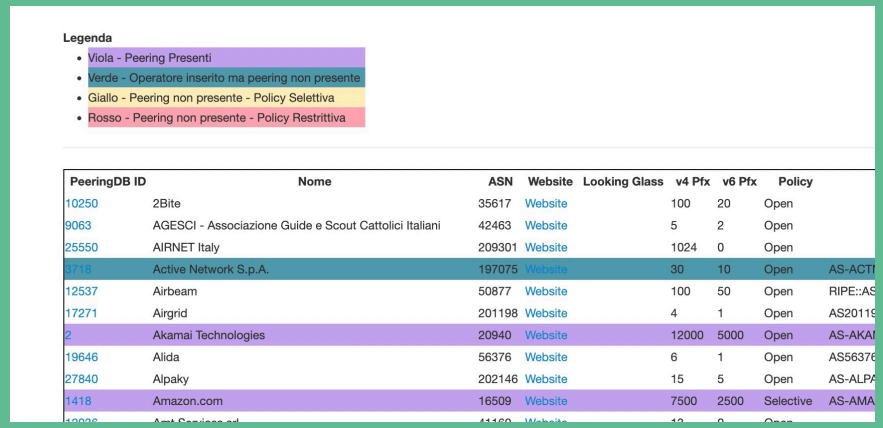
Monitoraggio delle Sessioni: Quadro Sinottico



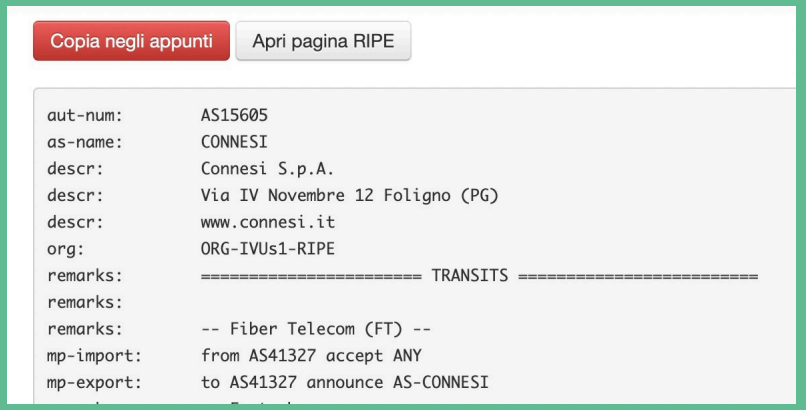
Gestione email tra operatori



«Trova Peering»



Generatore di Aut-num



• La piattaforma SDN

Obiettivi Raggiunti

•600+ peering gestiti e monitorati

•50 Route Policy e 12 Templates

•4 Internet Exchange Points

•100+ routers gestiti

•Errore umano ridotto al minimo

•Viene garantita l'uniformità nelle policy di sicurezza

•Dati aggiornati automaticamente ogni 24 ore

Sviluppi Futuri

•Funzioni di service provisioning

•Oltre il BGP… VRF, MPLS e altro

•Intent-based networking

•Rilascio codice Open-Source (a partire dalla ver 2.0)

•Sviluppo per altre piattaforme (Juniper, Mikrotik, etc..)

•Sviluppo API per integrazioni esterne

Connesi è settima in Italia per adiacenze IPv4 e quinta per numero di adiacenze IPv6 (Fonte https://bgp.he.net/country/IT)

Country Info

Networks: Italy

ASN	Name	Adjacencies v4 ↓	Routes v4	Adjacencies v6	Routes v6
AS60501	Sirius Technology SRL	3,334	18	1,440	4
AS39120	Convergenze S.p.A.	3,050	69	800	3
AS5394	UNIDATA S.p.A.	2,393	27	96	2
AS41327	Fiber Telecom S.p.A.	2,120	551	1,240	80
AS12779	IT.Gate S.p.A.	1,966	371	1,429	29
AS49605	Digital Telecommunication Services S.r.l.	1,378	16	362	4
AS15605	Connesi s.p.a.	1,362	21	989	1
AS1267	WIND TRE S.P.A.	1,152	550	180	8
AS20811	Brennercom S.p.A.	1,103	68	815	10

https://lg.connesi.it

Domande?

connesi®
TUTTI SEMPRE OVUNQUE