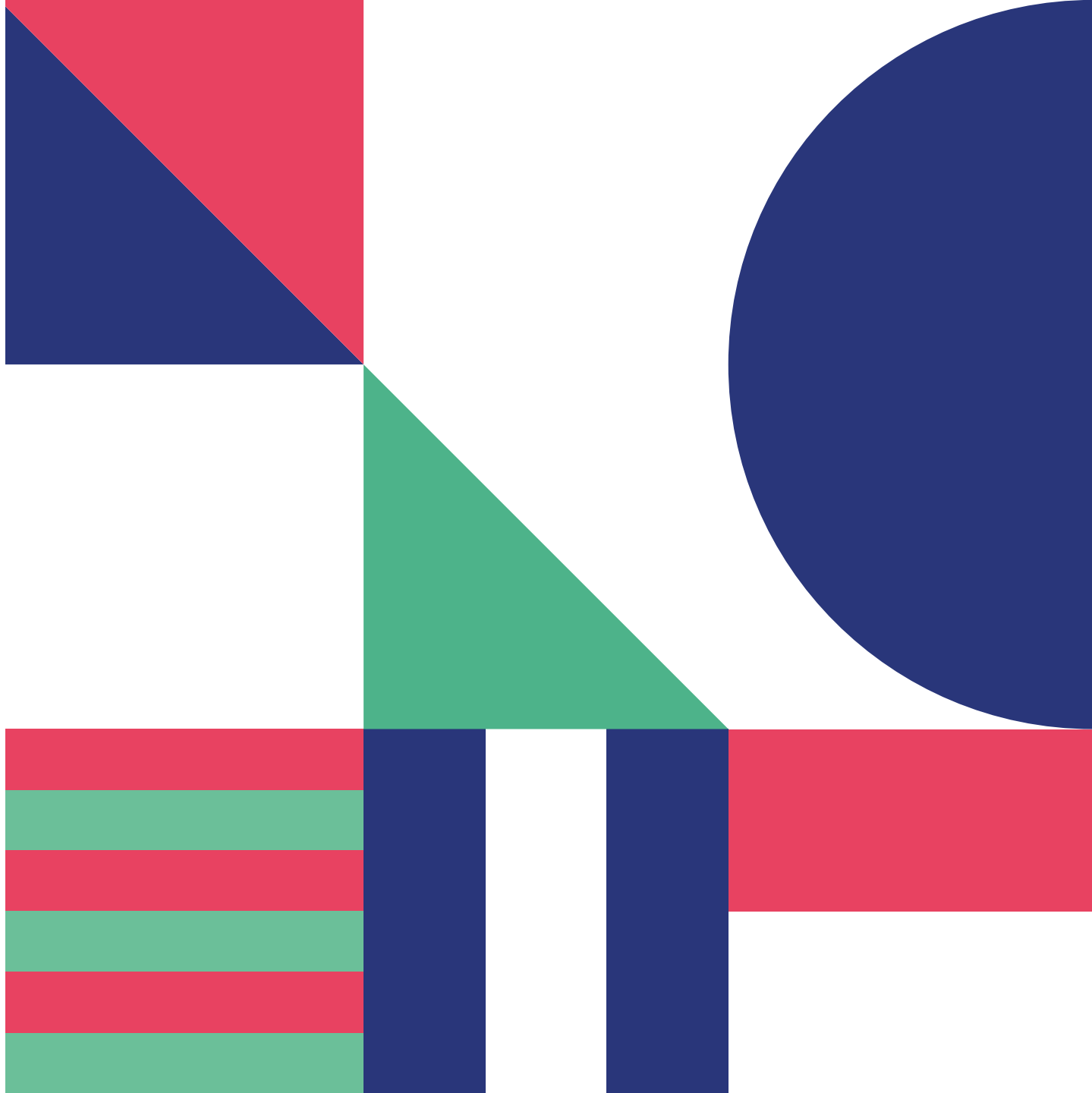


- FiberTelecom Winery Tour 2022 – 21 Aprile 2022

CONNESI

BGP Security Automation
for ISP



- 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

- 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



- **La Open Peering Policy**

Cosa vuol dire avere una Open Peering Policy

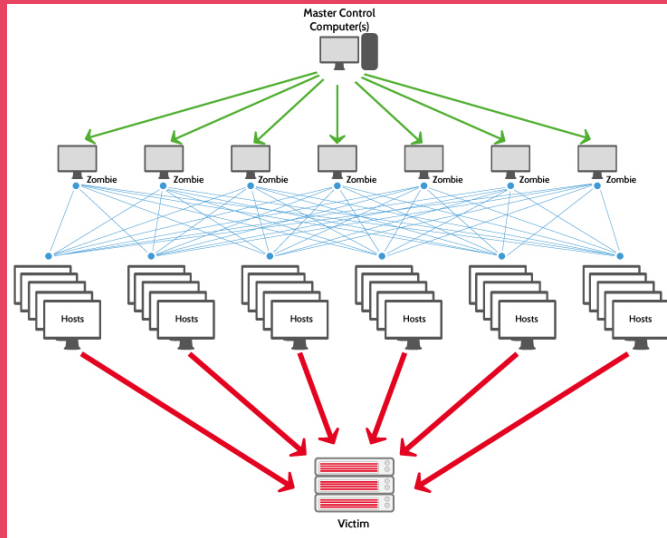
- Una Open Peering Policy è una policy di routing che ammette l'interconnessione diretta tra operatori senza limiti, senza prerequisiti su rapporti di Upload e Download o corrispettivi economici.
 - Massimizzare il numero di collegamenti con altri operatori e produttori di contenuti
 - Aumentare il valore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

La Open peering Policy è impegnativa...

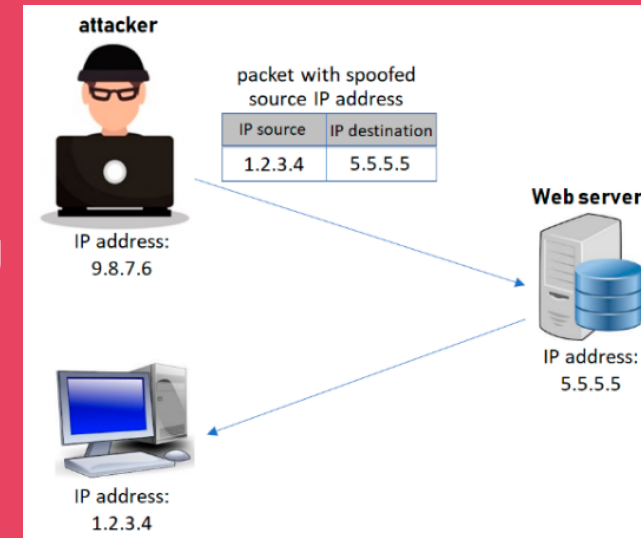
- «Da grandi poteri derivano grandi responsabilità»
- Alti costi di gestione e Personale NOC
- Troubleshooting problematico nel complesso
- Aumento consumi risorse router di frontiera (CPU, RAM, Dimensioni RIB)
- Alto rischio di errore umano
- Avere il controllo vuol dire dover fronteggiare le minacce

- Le minacce

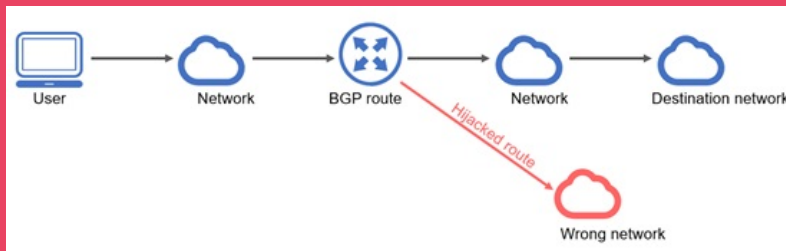
Attacchi DDoS



IP Spoofing



BGP Hijacking



Route Leaks



- **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

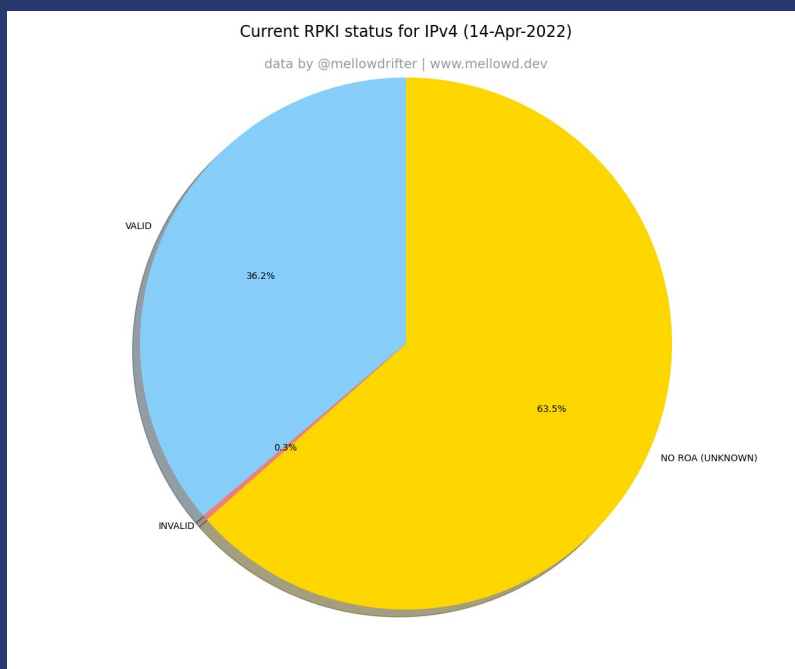


• Le Contromisure tradizionali non sono abbastanza...

- 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...



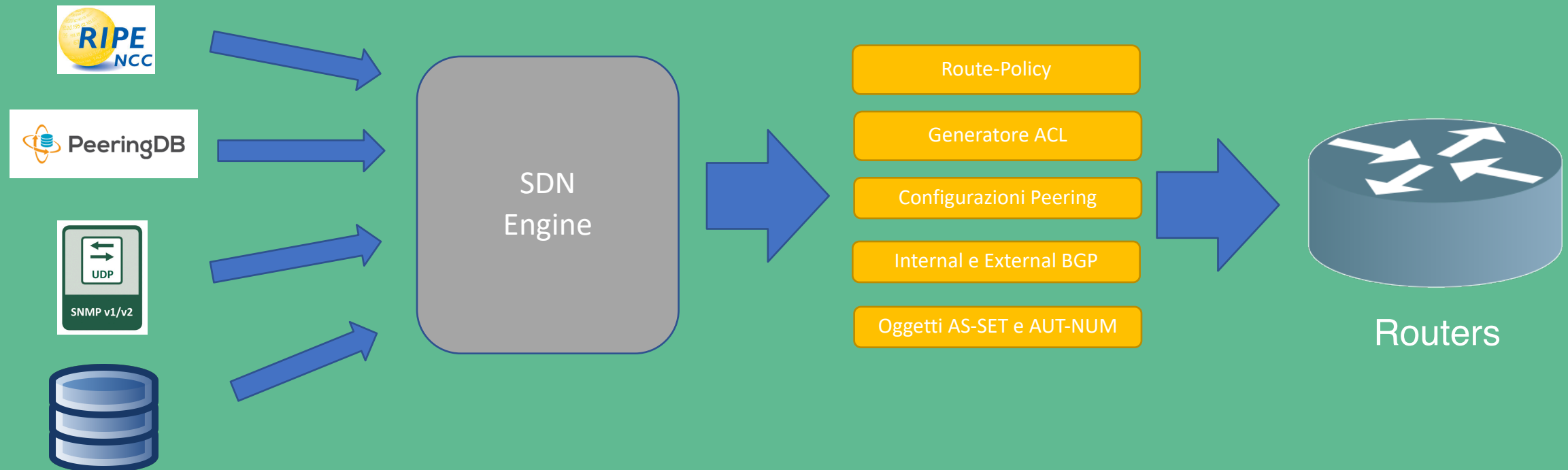
- La modalità loose di uRPF serve a poco alle frontiere per proteggersi dagli attacchi DDoS
- L'impiego di ACL per permettere il traffico delle sole classi pubbliche è complesso in caso di fornitura di transiti e necessitano frequenti modifiche

Serve un sistema automatico per la generazione dei filtri di sicurezza

• 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

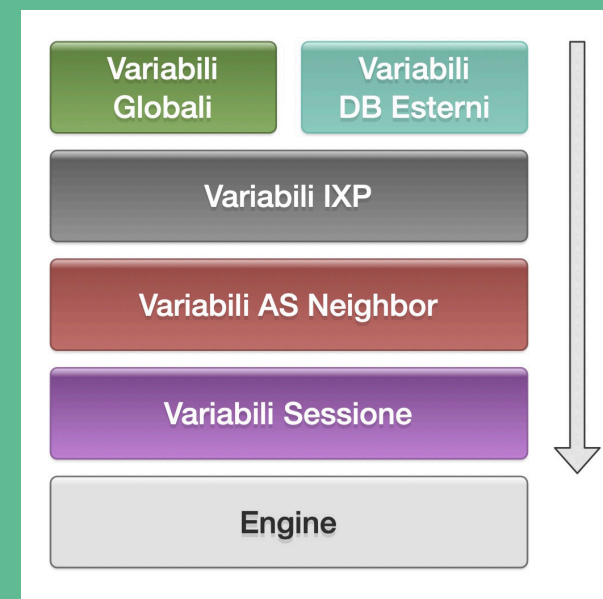
- Punto di partenza per AS-SET e Indirizzi IP destinati alle sessioni
- API molto ben documentate
- Base dati per max-prefix, peering contacts, nomi reti, IXP, e molto altro...

<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
# Convergence 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

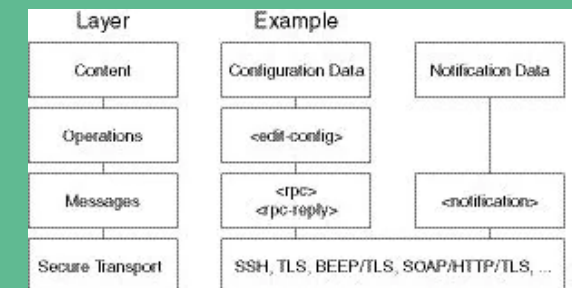
- Trasporto SSH o Telnet
- Interfaccia più utilizzata
- Relativamente uniforme tra le release IOS-XR
- La configuration versioning di IOS-XR
- Il trattamento dell'errore è complesso

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)

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



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

NameX	NameX	NameX	NameX	NameX	NameX	NameX	NameX	NameX	NameX	NameX	NameX	NameX
Holy See	BT Italia	Telecom It...	WINDTRE	IRIDEOS (I...	Convergenz...	Sky Italia...	Amazon.com	Retail Sp...	Amazon.com	Aruba	Panservice	
8978	8968	3269	1267	3302	39120	210278	16509	28716	16509	31034	20912	
193.201.28.7	193.201.28.9	193.201.28.10	193.201.28.11	193.201.28.13	193.201.28.14	193.201.28.17	193.201.28.18	193.201.28.22	193.201.28.25	193.201.28.27	193.201.28.31	

NameX	NameX	NameX	NameX	NameX	NameX	NameX	NameX	NameX	NameX	NameX	NameX	NameX
Meta	Convergenz...	Holy See	Meta	NameX Serv...	Microsoft	Microsoft	Packet Cle...	Subspace	Faaly, In...	Faaly, In...		
32934	39120	8978	32934	24796	8075	8075	42	3856	32261	54113	54113	
193.201.28.87	193.201.28.90	193.201.28.91	193.201.28.97	193.201.28.100	193.201.28.116	193.201.28.129	193.201.28.152	193.201.28.153	193.201.28.177	193.201.28.183	193.201.28.184	

NameX	NameX	NameX	NameX	NameX	NameX	NameX	NameX	NameX	NameX	NameX	NameX	NameX
Panservice	Akamai Tec...	NameX Serv...	Retail Sp...	Vodafone I...	Aruba	Subspace	Meta	Convergenz...	IVO by D.L...	Fastly, In...	WARIAN	
20912	20940	24796	28716	30722	31034	32261	32934	39120	49605	54113	56911	
2001:78b:1...	2001:78b:1...	2001:78b:1...	2001:78b:1...	2001:78b:1...	2001:78b:1...	2001:78b:1...	2001:78b:1...	2001:78b:1...	2001:78b:1...	2001:78b:1...	2001:78b:1...	

Mix	Mix	Mix	Mix	Mix	Mix	Mix	Mix	Mix	Mix	Mix	Mix	Mix
Sky Italia...	MIX-IT Ser...	RIPE NCC R...	WINDTRE	IRIDEOS (I...	IRIDEOS (I...	VerSign G...	RAI - Rad...	Telecom It...	PosteCom	GARR	BT Italia	
60772	16004	12654	1267	5602	3302	26415	8234	3269	16720	137	8968	
109.73.82.186	217.29.66.1	217.29.66.6	217.29.66.9	217.29.66.10	217.29.66.11	217.29.66.20	217.29.66.26	217.29.66.34	217.29.66.38	217.29.66.39	217.29.66.40	

Mix	Mix	Mix	Mix	Mix	Mix	Mix	Mix	Mix	Mix	Mix	Mix	Mix
Active Net...	Uno Commu...	Aruba	Fondazion...	Microsoft	Continent...	Estracom S...	Hurricane ...	Meta	Subspace	Sky Italia...	Meta	
197075	9137	31034	50112	8075	14537	31319	6939	32934	32261	210278	32934	
217.29.66.76	217.29.66.82	217.29.66.90	217.29.66.95	217.29.66.112	217.29.66.121	217.29.66.122	217.29.66.125	217.29.66.131	217.29.66.142	217.29.66.154	217.29.66.156	

Mix	Mix	Mix	Mix	Mix	Mix	Mix	Mix	Mix	Mix	Mix	Mix	Mix
Blizzard E...	WARIAN	Convergenz...	Dropbox	Amazon.com	Amazon (IVS...	Amazon (IVS...	Vodafone L...	Cisco Umbr...	EuropDYS	Panservice	Netnod	
57976	56911	39120	19679	16509	46489	46489	30722	36692	202347	20912	8674	
217.29.66.217	217.29.66.226	217.29.66.236	217.29.67.10	217.29.67.16	217.29.67.17	217.29.67.18	217.29.67.27	217.29.67.41	217.29.67.44	217.29.67.54	217.29.67.57	

Mix	Mix	Mix	Mix	Mix	Mix	Mix	Mix	Mix	Mix	Mix	Mix	Mix
Malta It...	Sky Italia...	Sky Italia...	GARR	WINDTRE	ATA&T EMEA...	IRIDEOS (I...	Hurricane ...	Microsoft	Microsoft	Netnod	Netnod	
209222	210278	210278	137	1267	2686	3302	6939	8075	8075	8674	8674	
2001:78b:...	2001:78b:...	2001:78b:...	2001:78b:...	2001:78b:...	2001:78b:...	2001:78b:...	2001:78b:...	2001:78b:...	2001:78b:...	2001:78b:...	2001:78b:...	

Mix	Mix	Mix	Mix	Mix	Mix	Mix	Mix	Mix	Mix	Mix	Mix	Mix
Dropbox	Panservice	Akamai Tec...	VerSign G...	Retail Sp...	Vodafone I...	Aruba	Subspace	Meta	Meta	Giulio Lo ...	IGT Lotter...	

Gestione email tra operatori

Peering Request

From: **noc@connesi.it**
 BCC: **noc@connesi.it**
 To: **peering-to@amazon.com blankman@amazon.com**

Already peering at:
 NaMeX Rome IXP
 MIX-IT
 DE-CIX Management GmbH
 Amsterdam Internet Exchange

Message:

Hello, Amazon.com
 We are Connesi S.p.A. (AS 15605) and we would like to setup a peering between our AS to optimize latency and throughput.

We are both present in the following IXPs:
 - NaMeX Rome IXP
 - MIX-IT
 - DE-CIX Management GmbH
 - Amsterdam Internet Exchange

Our data:
 -- NaMeX Rome IXP --

Close Send message

«Trova Peering»

Legenda

- Viola - Peering Presenti
- Verde - Operatore inserito ma peering non presente
- Giallo - Peering non presente - Policy Selettiva
- Rosso - Peering non presente - Policy Restrittiva

PeeringDB ID	Nome	ASN	Website	Looking Glass	v4 Pfx	v6 Pfx	Policy
10250	2Bite	35617	Website		100	20	Open
9063	AGESCI - Associazione Guide e Scout Cattolici Italiani	42463	Website		5	2	Open
25550	AIRNET Italy	209301	Website		1024	0	Open
3715	Active Network S.p.A.	197075	Website		30	10	Open AS-ACTI
12537	Airbeam	50877	Website		100	50	Open RIPE::AS
17271	Airgrid	201198	Website		4	1	Open AS20119
2	Akamai Technologies	20940	Website		12000	5000	Open AS-AKA
19646	Alida	56376	Website		6	1	Open AS56376
27840	Alpaky	202146	Website		15	5	Open AS-ALP
1418	Amazon.com	16509	Website		7500	2500	Selective AS-AMA
10000	Ant-Space.com	41180	Website		10	0	Open

Generatore di Aut-num

Copia negli appunti Apri pagina RIPE

```

aut-num:         AS15605
as-name:         CONNESI
descr:           Connesi S.p.A.
descr:           Via IV Novembre 12 Foligno (PG)
descr:           www.connesi.it
org:             ORG-IVUs1-RIPE
remarks:         ===== TRANSITS =====
remarks:
remarks:         -- Fiber Telecom (FT) --
mp-import:       from AS41327 accept ANY
mp-export:       to AS41327 announce AS-CONNESI
    
```

• 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

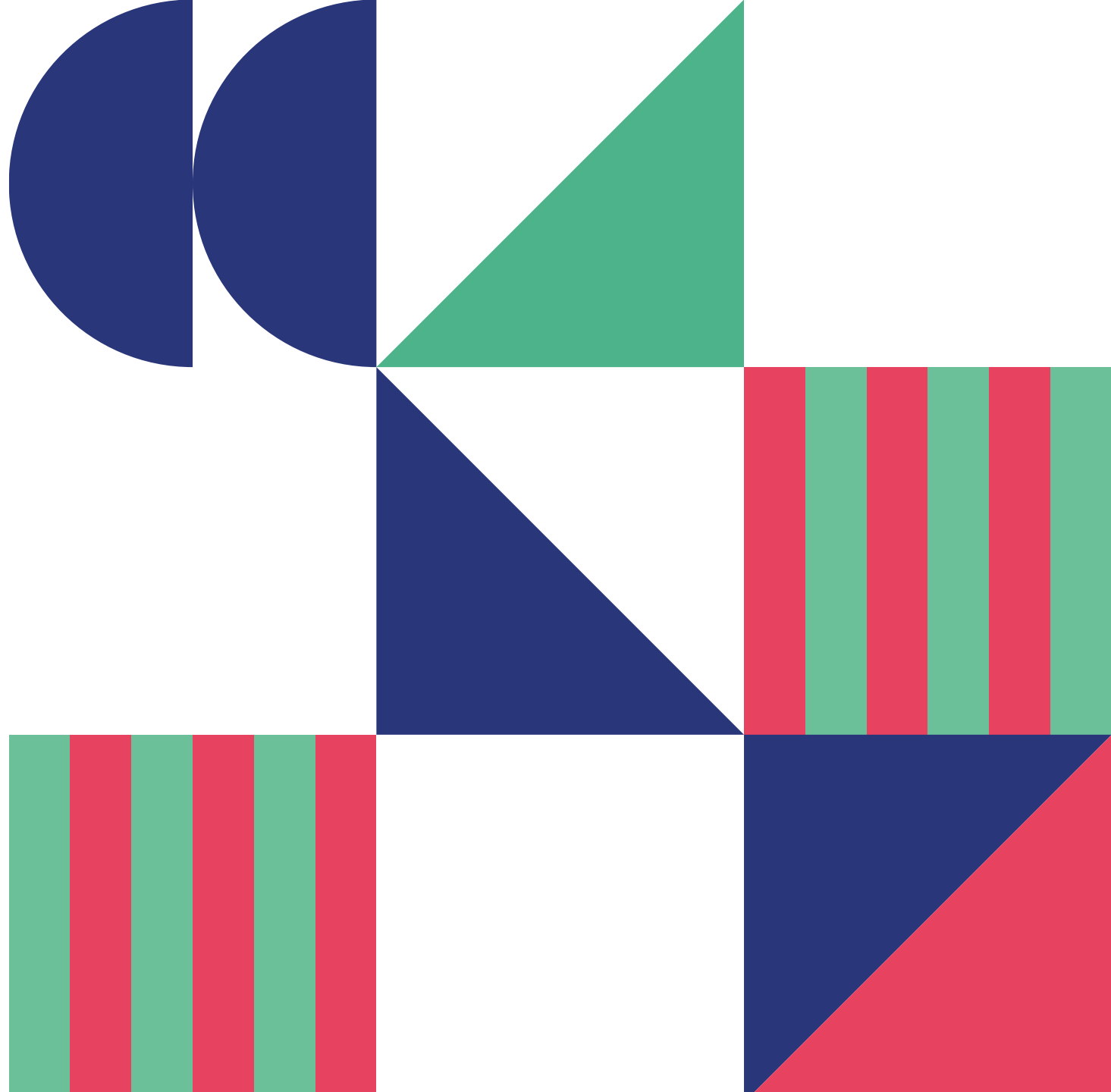
Sviluppi Futuri

- 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?