neacademy

DATAFEST

DAL DATA CENTER A INTERNET: anatomia delle reti Aruba

aruba.it

Andrea Colangelo

3 - 4 GIUGNO 2026

DA PIÙ DI 30 ANNI PIONIERI DEL DIGITALE IN ITALIA

1994

2000
aruba.it

2003

1° Data Center Arezzo

2005
forpsi

2006
Aruba PEC

2008

Tessere Sanitarie

2009
ACTALIS
Autorità di certificazione Europea

2011
aruba CLOUD

2° Data Center Arezzo

2013
aruba CLOUD

2014
.CLOUD

2015
aruba.it Ducati Superbike Team
aruba.it BUSINESS

2016
Pratiche.it
aruba.it SPID

2017

Data Center IT3-A

2018
.CLOUD

2019
aruba.it ENTERPRISE

2020
ACTALIS

2021
aruba.it FIBRA

2022

Data Center IT3-B/C

2023
aruba.it KUBE

2024

Data Center IT4-A

ARUBA AT A GLANCE

16M
UTENTI SERVITI

100+
PAESI SERVITI

30+
ANNI DI CRESCITA

5
DATA CENTER PROPRIETARI

- PONTE SAN PIETRO
- ROMA
- AREZZO x 2
- KTIŠ (CZ)

Campus Data Center IT 3
Ponte San Pietro (BG)
200.000 m² di Proprietà

Campus Data Center IT 4
Roma
74.000 m² di Proprietà

Data Center IT 1 e IT2
Arezzo 5.000 m² e 2.000 m² di Proprietà

Infrastrutture Cloud Partner

Data Center DE 1
Francoforte

Data Center FR 1
Parigi

Data Center UK 1
Londra

Data Center PL 1
Varsavia

DATA CENTERS

- 300K+ metri quadrati nei nostri Campus DC in Italia
- 70MW+ potenza IT raggiungibile nei nostri data center italiani

CLOUD

- 8 Cloud Region in 6 Paesi europei
- 200K clienti cloud
- 10 Mil email gestite
- 2.7 Mil domini registrati e gestiti

CONNECTIVITY

- > 1 Tbps capacità di interconnessione Internet
- 10+ Gb/s velocità di connettività cloud VPS

TRUST & SECURITY

- 1,8 Bil firme digitali all'anno
- 62,4 Mil tessere sanitarie italiane
- 2 Mil di identità digitali gestite
- 1 Mil certificati SSL attivi
- 10 Mil account PEC gestiti

TANTI SERVIZI: UNA RETE PER DOMARLI...

Hosting/Housing provider? Cloud provider? Data Center provider?
ISP per contenuti? ISP per accesso broadband?
Orientati al business? Al residenziale?

HOSTING / HOUSING PROVIDER
- Grandi architetture locali
- Fanout fisici complessi
- Server farm ad alta densità

CLOUD PROVIDER
- Architetture di reti locali complesse
- Overlay e multi-tenancy
- Automazione e isolamento

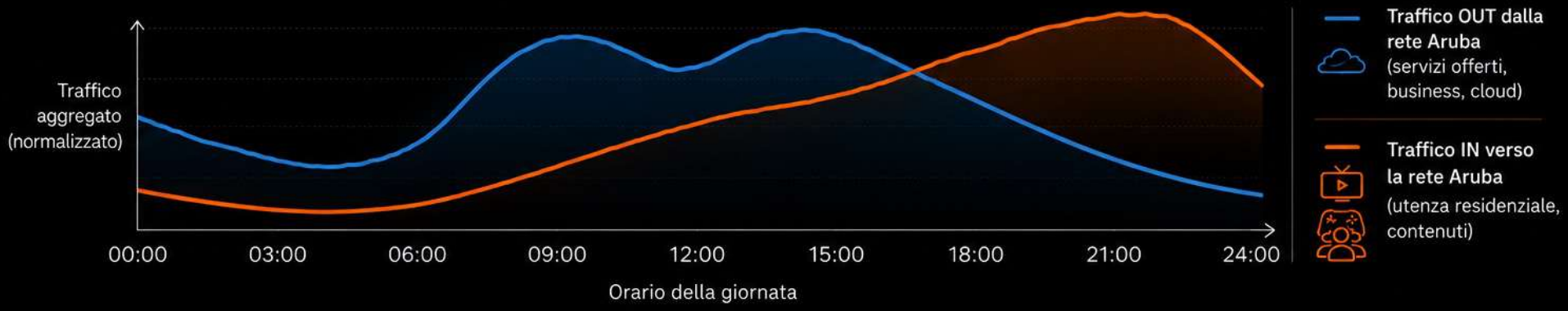
DATA CENTER PROVIDER
- Campus distribuiti
- Interconnessione tra data center
- Carrier neutrality

ISP PER CONTENUTI (TRANSIT & PEERING)
- Backbone Internet
- Peering internazionale
- Accesso ai principali IX europei

ISP PER ACCESSO BROADBAND
- Traffico residenziale
- Picchi serali
- Streaming, gaming, social

ORIENTATI AL BUSINESS
- Workload enterprise
- Traffico diurno
- Applicazioni cloud e SaaS

ORIENTATI AL RESIDENZIALE
- Utenti consumer
- Traffico serale
- Contenuti digitali e intrattenimento



LE PRINCIPALI PIATTAFORME DI RETE ARUBA (E PER LA RETE ARUBA)

ETHERNET FABRIC

Connettività interna ai Data Center

- Spine-Leaf
- EVPN / VXLAN
- Multi-tenancy
- Ottimizzata per traffico East-West e cloud

TRANSPORT BACKBONE

Backbone geografico multi-servizio

- SR-MPLS
- EVPN
- Resilienza e ridondanza
- Traffic Engineering
- Alta capacità e bassa latenza
- Piattaforma per servizi diversificati:

DC Interconnection (DCI) | Interconnessione tra DC Fabric | L2VPN / L3VPN (servizi carrier) | Cloud Interconnection

INTERNET BACKBONE

Interconnessione globale con Internet

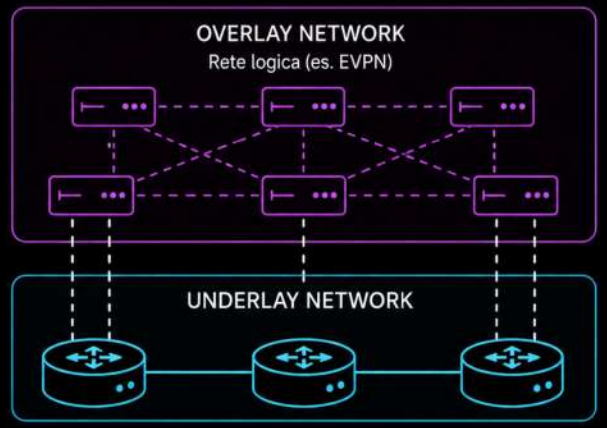
- Peering su IX
- Transit
- Content Delivery Network
- Dual Stack IPv4 / IPv6

DDOS DEFENCE

Protezione dei servizi Internet e dell'infrastruttura

- Mitigazione distribuita
- FlowSpec
- Scrubbing (on-prem e cloud)
- Rilevamento e analisi real-time

APPROFONDIMENTO: OVERLAY NETWORKS



- Separazione tra trasporto e servizio
- La rete fisica e logica underlay fornisce connettività, capacità e resilienza; l'overlay abilita servizi, domini virtuali e policy
- Indipendenza dalla topologia fisica

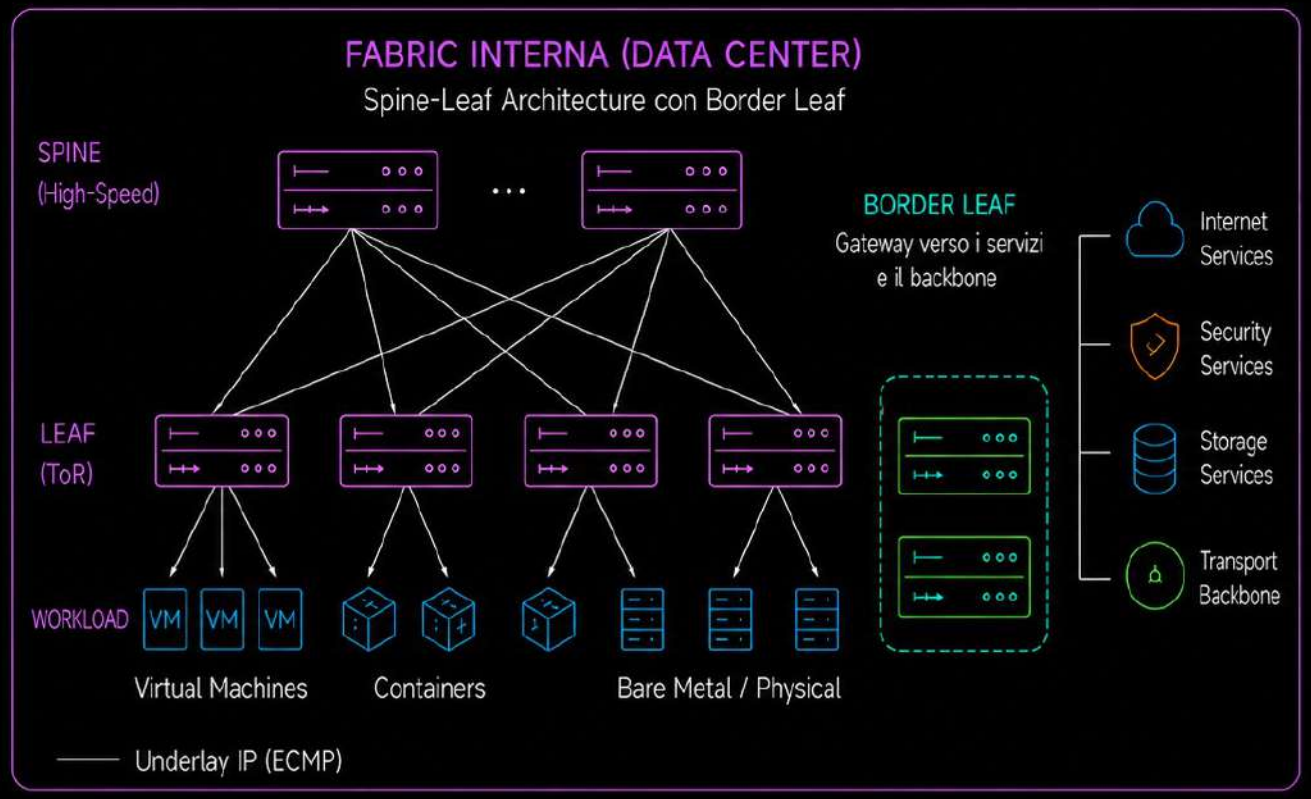
SEGMENTAZIONE LOGICA
Tenant, ambienti, clienti e workload possono essere isolati sulla stessa infrastruttura condivisa.

SCALABILITÀ
L'underlay rimane semplice e stabile, mentre l'overlay cresce in modo più dinamico con nuovi servizi e nuovi domini.

TRAFFIC ENGINEERING E POLICY
L'overlay permette di applicare percorsi, trattamenti e policy diverse in base al tipo di servizio o traffico.

Ethernet Fabric

ETHERNET FABRIC: DENTRO IL DATA CENTER



PERCHÉ UNA ETHERNET FABRIC

1. SEPARAZIONE UNDERLAY / OVERLAY

Semplice underlay IP per il trasporto, overlay VXLAN per reti virtuali flessibili e indipendenti.

2. SCALABILITÀ E MULTI-TENANCY

Estensione L2 senza i limiti dei domini broadcast tradizionali.

Isolamento e segmentazione nativa.

3. OTTIMIZZAZIONE TRAFFICO EAST-WEST

Percorsi ottimizzati all'interno della fabric (best path)

4. AUTOMAZIONE E WORKLOAD MOBILITY

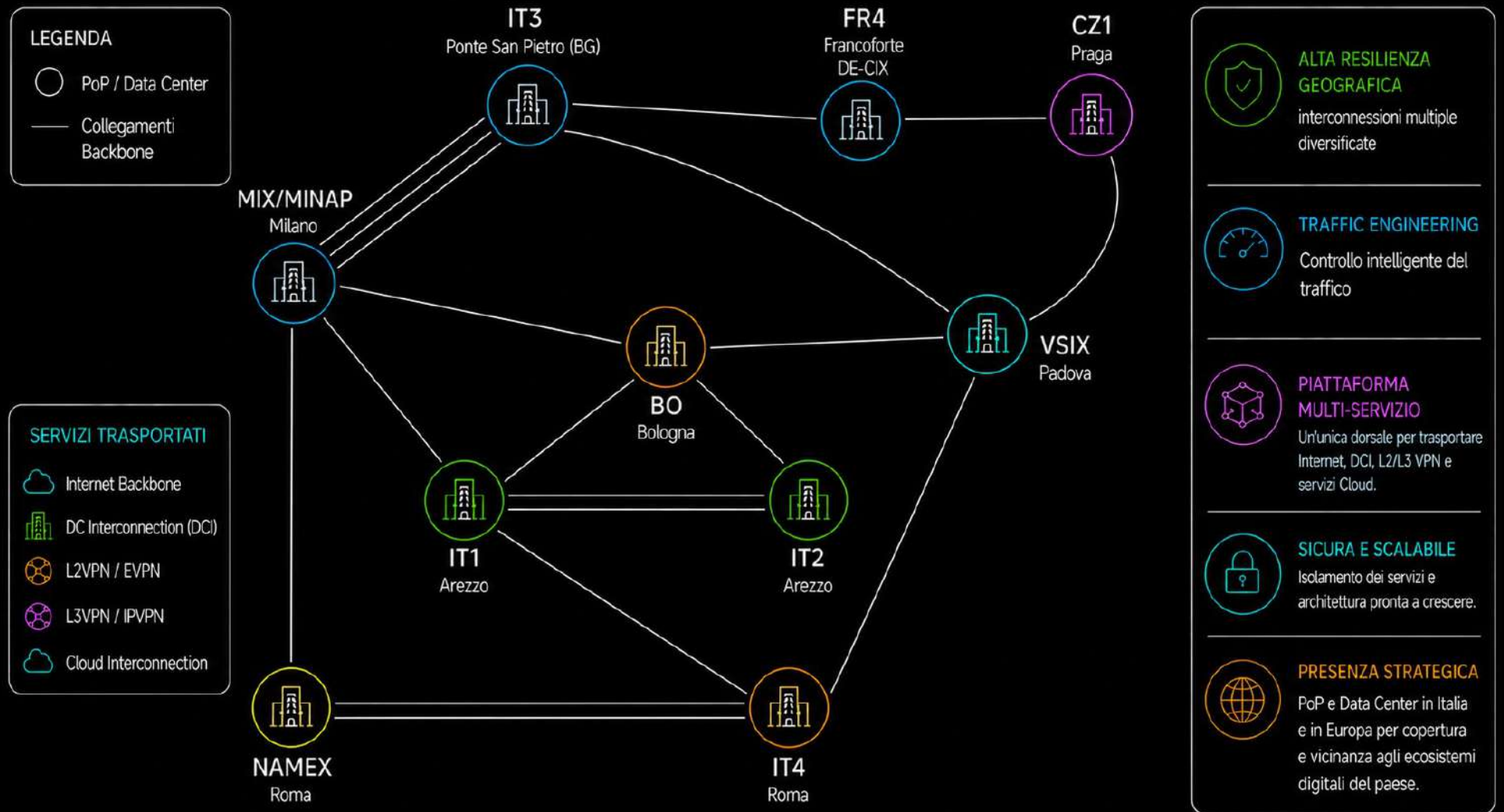
Integrazione con orchestrator e controller. Mobilità dei workload tra host e tra data center in modo trasparente.

5. IL RUOLO DI EVPN

EVPN è il control-plane moderno che distribuisce le informazioni di reachability in modo efficiente, evitando i limiti dei meccanismi flood-and-learn delle reti L2 tradizionali.

Transport Backbone

TRANSPORT BACKBONE: INTERCONNETTERE DATA CENTER, POP E INTERNET EXCHANGE



ALTA RESILIENZA GEOGRAFICA
interconnessioni multiple diversificate

TRAFFIC ENGINEERING
Controllo intelligente del traffico

PIATTAFORMA MULTI-SERVIZIO
Un'unica dorsale per trasportare Internet, DCI, L2/L3 VPN e servizi Cloud.

SICURA E SCALABILE
Isolamento dei servizi e architettura pronta a crescere.

PRESENZA STRATEGICA
PoP e Data Center in Italia e in Europa per copertura e vicinanza agli ecosistemi digitali del paese.

APPROFONDIMENTO: VXLAN vs SR-MPLS

1. ORIGINE E FILOSOFIA

- VXLAN: nato nel data center per superare i limiti delle VLAN e supportare ambienti multi-tenant cloud.
- SR-MPLS: evoluzione di MPLS/LDP per WAN carrier-grade e traffic engineering deterministico.

2. DATA PLANE: ENCAPSULATION VS LABEL STACK

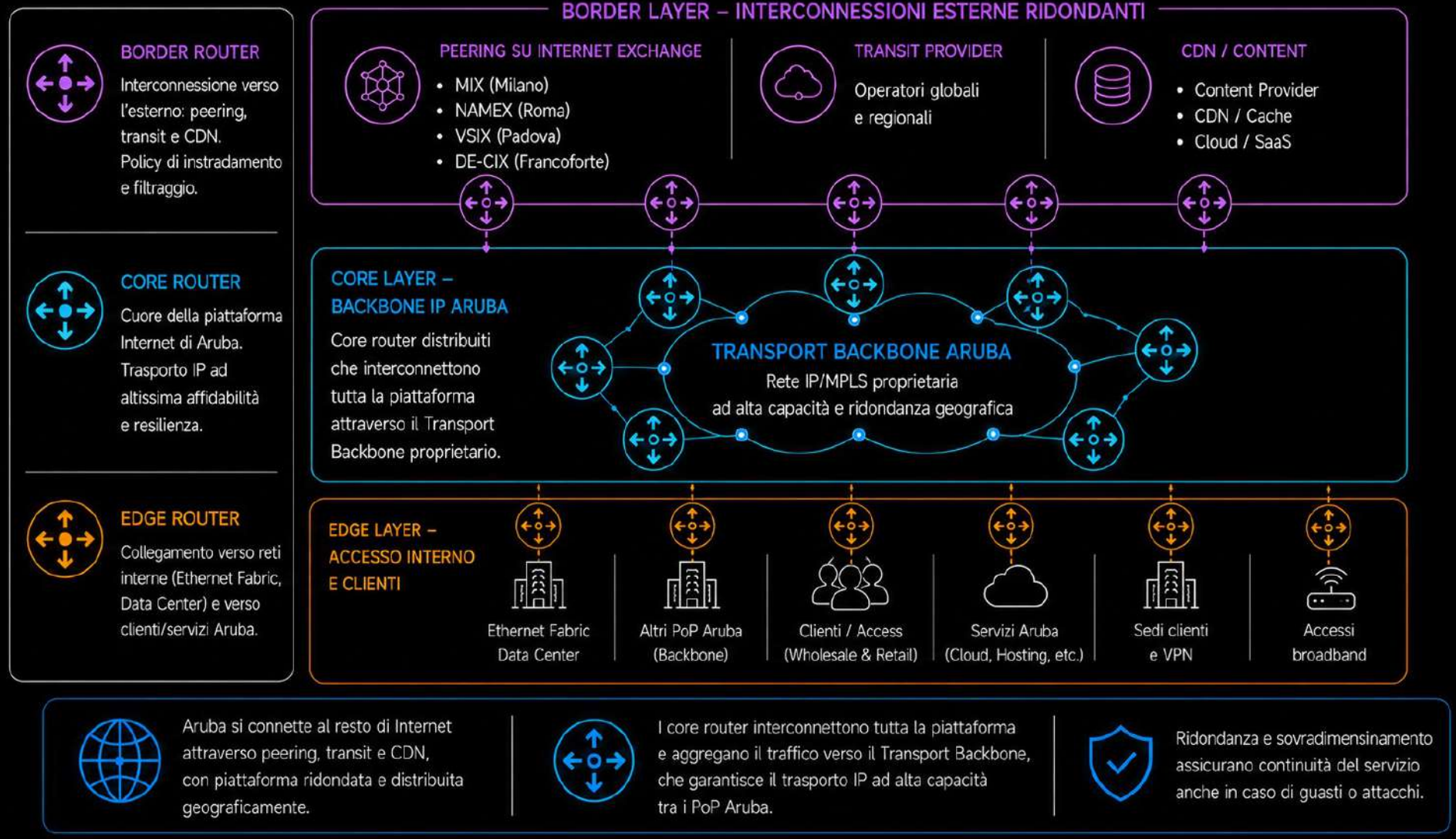
- VXLAN: incapsula L2 in UDP/IP. Non controlla direttamente il percorso.
- SR-MPLS: aggiunge uno stack di label MPLS davanti al pacchetto. Overhead minimo e ogni label rappresenta una "istruzione di percorso» o una astrazione di rete/servizio.

3. CONTROLLO DEL PERCORSO

- VXLAN: non permette source routing arbitrario; il percorso è quello che decide l'underlay routing (ECMP).
- SR-MPLS: source routing nativo. Il nodo di ingresso può dire "vai prima a A, poi a B, poi a C". Supporta protezioni dei percorsi con riconvergenza sub-50ms (TI-LFA).

Internet Backbone

INTERNET BACKBONE: PEERING, TRANSIT E CONTENT DELIVERY



DDoS Defence

DDoS: TREND E NUOVE FORME DI ATTACCO

DDoS: CHE COS'È?

Un attacco DDoS (Distributed Denial of Service) ha l'obiettivo di rendere indisponibile un servizio legittimo saturando risorse di rete, apparati, applicazioni o sistemi di mitigazione attraverso traffico o richieste generate da molte sorgenti distribuite.

COSA PUÒ COLPIRE

- BANDA
- RETI E APPARATI
- SERVER E APPLICAZIONI
- DNS / API E SERVIZI

GLI ATTACCHI DDoS SONO IN FORTE CRESCITA

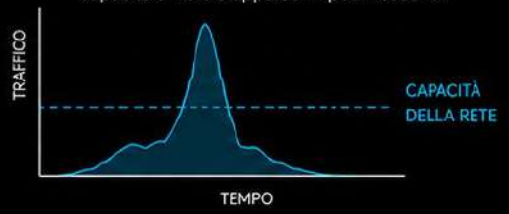
- 47,1 milioni di attacchi DDoS mitigati nel 2025, oltre il doppio rispetto al 2024.
- Attacchi iper-volumetrici fino a 31,4 Tbps registrati nel Q4 2025.

Fonte: Cloudflare DDoS Threat Report 2025

LE PRINCIPALI TENDENZE DEGLI ATTACCHI DDoS

1 IPER-VOLUMETRICI

Picchi di traffico estremamente elevati, spesso di breve durata, in grado di saturare capacità di rete e apparati in pochi secondi.



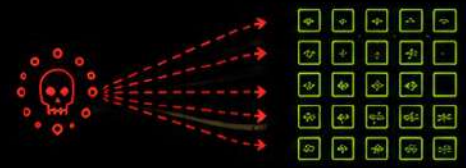
2 MULTI-VECTOR

Gli attaccanti combinano più tecniche (es. volumetriche, protocol based e applicative) o le alternano in sequenza per eludere le difese e aumentare l'impatto.

VOLUMETRICI (UDP, ICMP, ...) + PROTOCOL BASED (SYN, ACK, ...) + APPLICATIVI (HTTP, DNS, ...) ...

3 CARPET BOMBING

Il traffico viene distribuito su molti IP/prefissi (intere subnet) anziché su un singolo target, rendendo l'attacco meno visibile e più efficace nel causare congestione e degrado.



TREND IN FORTE CRESCITA:
Nel 1° semestre 2024 il 75% degli attacchi osservati usava tecniche di carpet bombing.

Fonte: Vercara (DigiCert) DDoS Threat Intelligence 2024

PERCHÉ SERVE UNA DIFESA MULTILIVELLO

Gli attacchi moderni sono rapidi, massivi, distribuiti e automatizzati.
Serve un'architettura di difesa a più livelli per garantire la continuità dei servizi.

ASSORBIRE IL PRIMO IMPATTO
Una rete sovradimensionata fornisce headroom per assorbire i picchi iniziali.

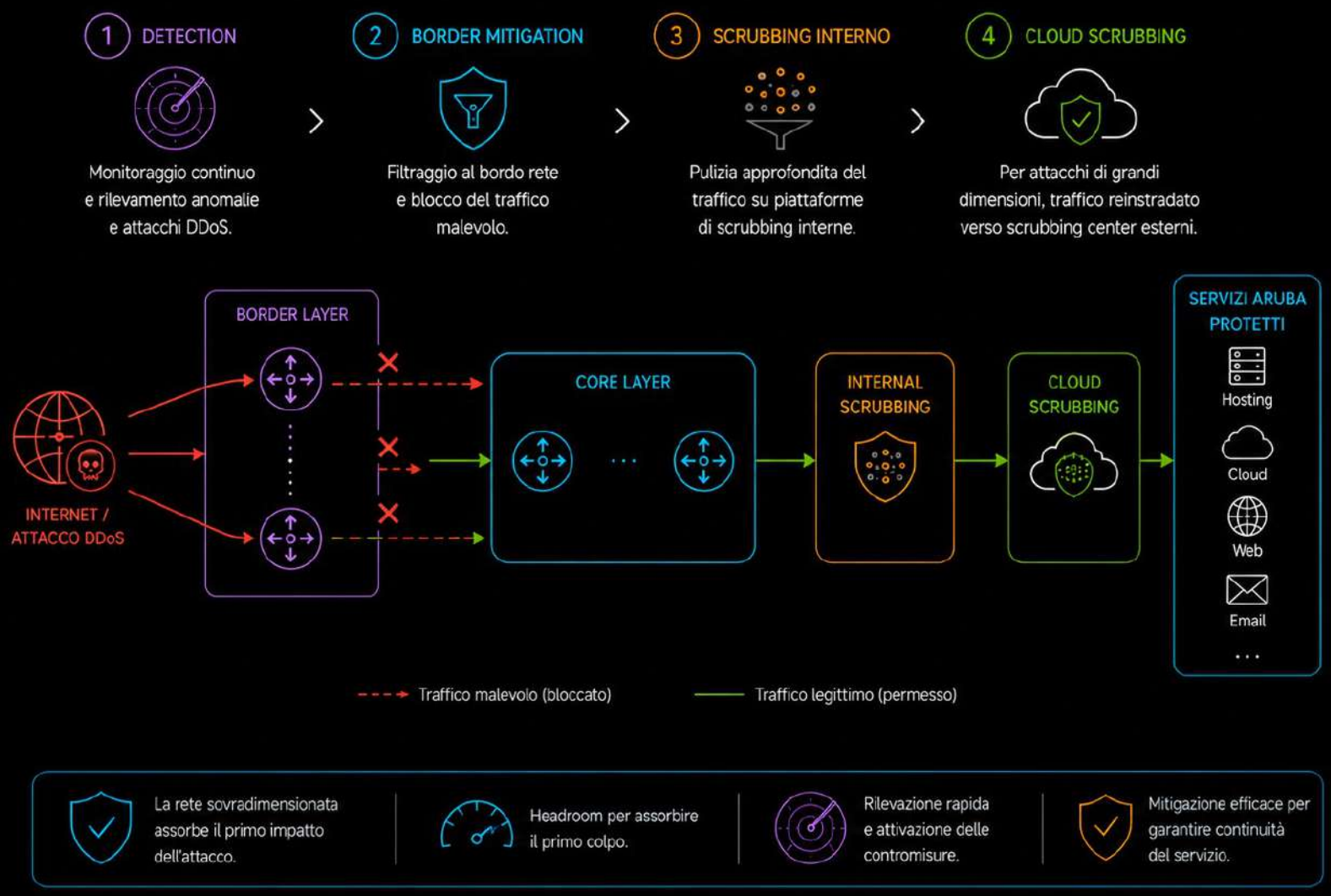
RILEVAZIONE RAPIDA
Monitoraggio continuo e analisi comportamentale per identificare l'attacco.

FILTRAGGIO AL BORDO
Policy e filtri al bordo rete (es. FlowSpec) per bloccare il traffico malevolo.

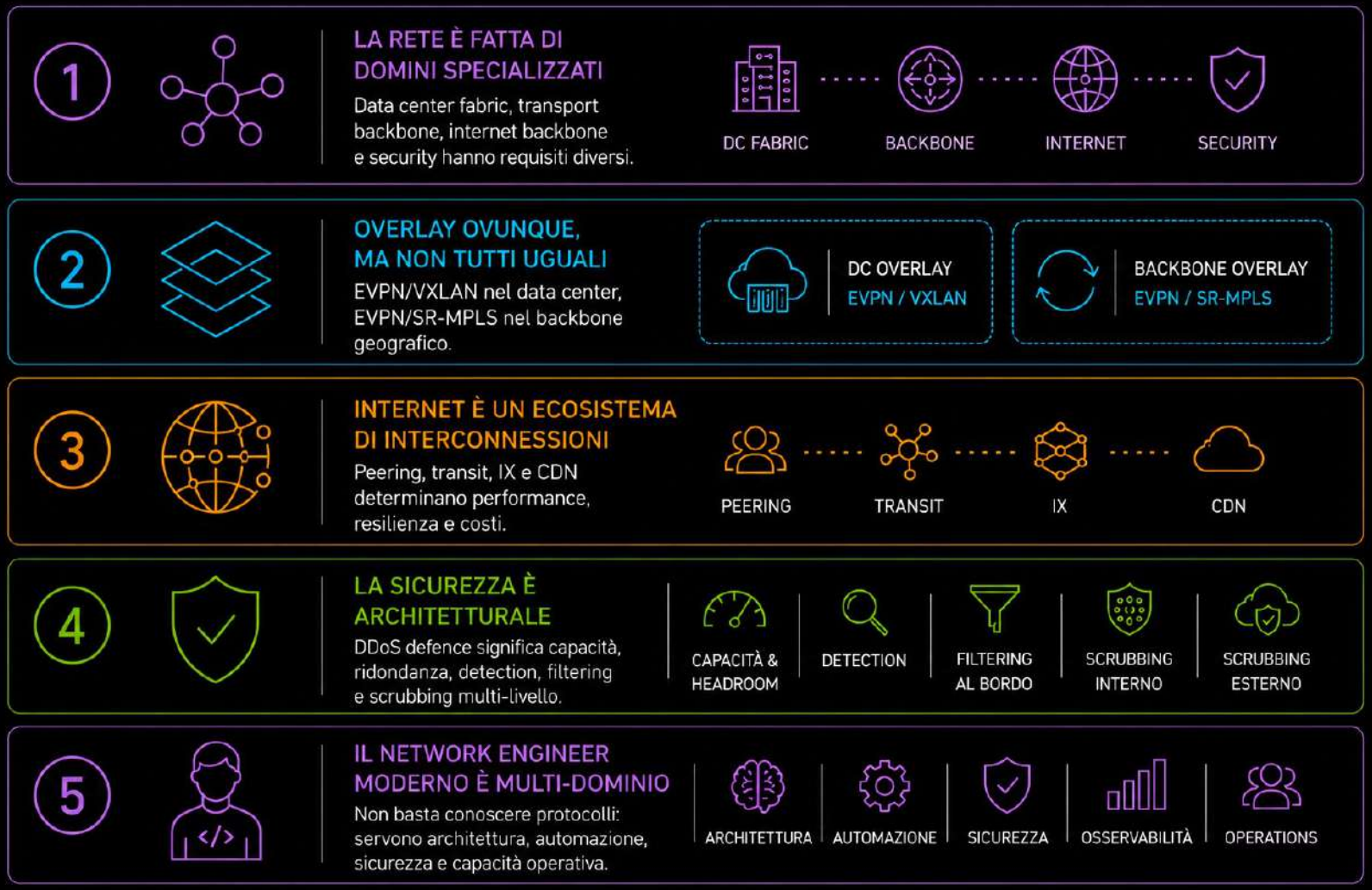
SCRUBBING INTERNO
Pulizia approfondita del traffico su piattaforme di scrubbing interne.

SCRUBBING ESTERNO
Per attacchi di grandi dimensioni, il traffico viene reindirizzato verso scrubbing center esterni.

DDoS DEFENCE: DAL PRIMO IMPATTO ALLA MITIGAZIONE



TAKEAWAYS


1
LA RETE È FATTA DI DOMINI SPECIALIZZATI
Data center fabric, transport backbone, internet backbone e security hanno requisiti diversi.
DC FABRIC
BACKBONE
INTERNET
SECURITY
2
OVERLAY OVUNQUE, MA NON TUTTI UGUALI
EVPN/VXLAN nel data center, EVPN/SR-MPLS nel backbone geografico.
DC OVERLAY
EVPN / VXLAN
BACKBONE OVERLAY
EVPN / SR-MPLS
3
INTERNET È UN ECOSISTEMA DI INTERCONNESSIONI
Peering, transit, IX e CDN determinano performance, resilienza e costi.
PEERING
TRANSIT
IX
CDN
4
LA SICUREZZA È ARCHITETTURALE
DDoS defence significa capacità, ridondanza, detection, filtering e scrubbing multi-livello.
CAPACITÀ & HEADROOM
DETECTION
FILTERING AL BORDO
SCRUBBING INTERNO
SCRUBBING ESTERNO
5
IL NETWORK ENGINEER MODERNO È MULTI-DOMINIO
Non basta conoscere protocolli: servono architettura, automazione, sicurezza e capacità operativa.
ARCHITETTURA
AUTOMAZIONE
SICUREZZA
OSSERVABILITÀ
OPERATIONS

neacademy

DATAFEST

Andrea Colangelo

Network Infrastructure Director @ Aruba

THANKYOU!

andrea.colangelo@staff.aruba.it
https://linkedin.com/in/acolangelo