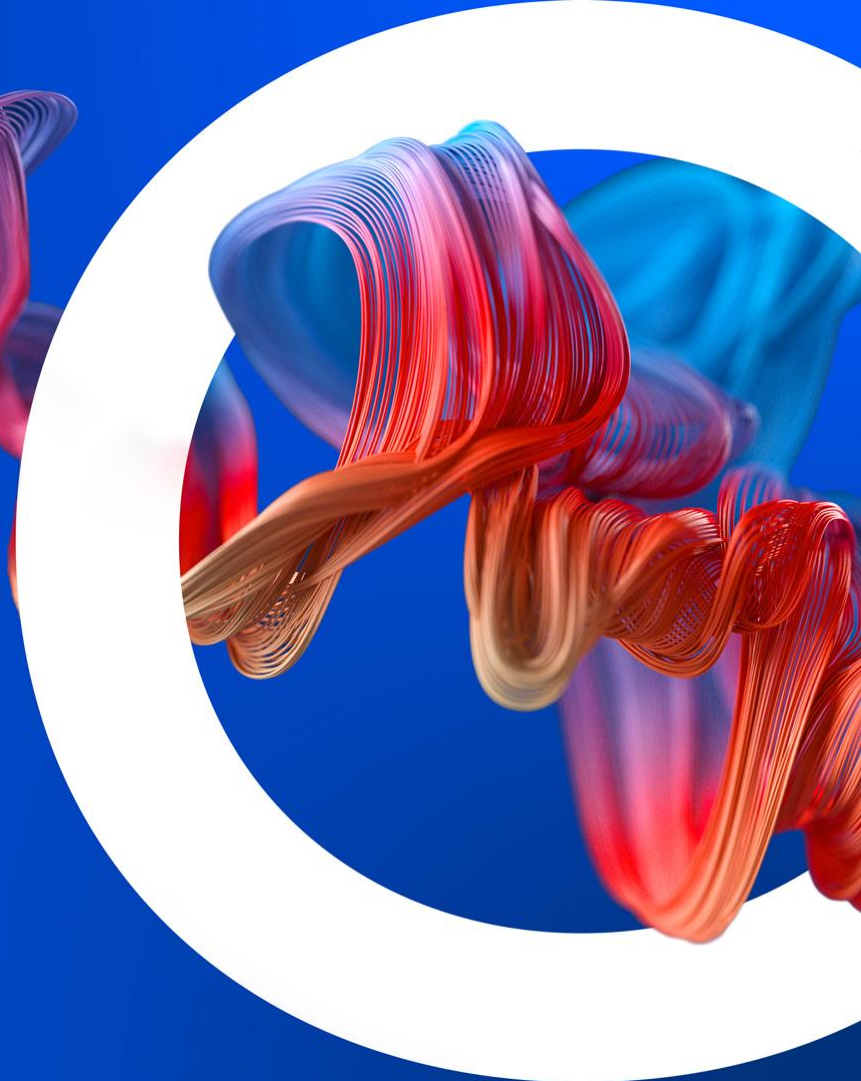
Securing IXP Fabrics

Alessandro Bulletti

IP Consulting Engineer, EMEA

Peering Days, Bologna, March 23 -25th 2026



IXP challenges

A big L2 switch, but not only..

A stable, secure IXP Fabric

- Only BGP route exchanges and Data traffic is desired
- Noise (unwanted protocols, BUM, etc.) can be extremely intrusive and must be avoided
- Fast convergence and redundancy needed in case of failure
- Multi-homing with loop prevention

An IXP Fabric to offer anti-DDoS services

- Enhance network availability against DDoS attacks directed to customers
- Secure by-design approach
- Maintain low latency and data privacy
- Sustainable operations
- Unlock opportunities for protection as a Service
- Seamless integration in network operations

IXP Secure Fabric – Inherent protection

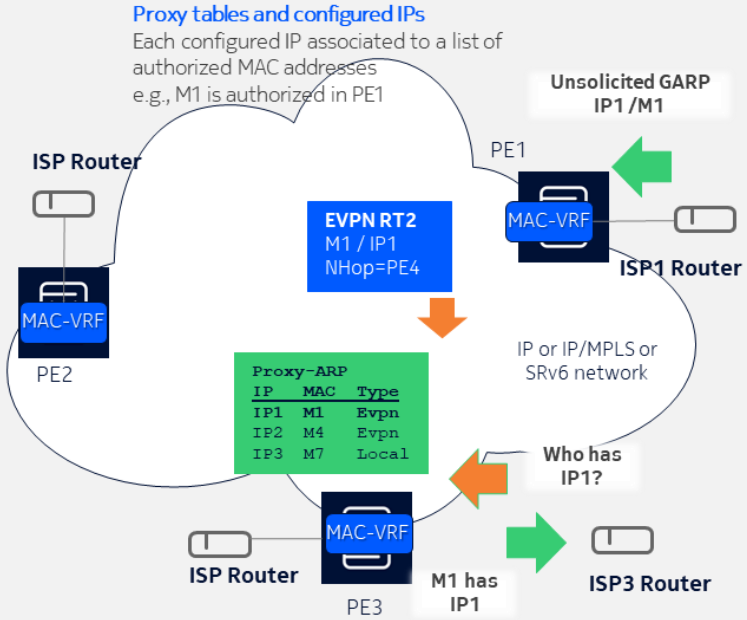
EVPN with Proxy-ARP/ND

The challenge

- Protect from ARP/ND floods
- Protect from unplanned loops in customer's networks
- Address port instability and MAC duplication
- Police and filter ingress traffic
- Secure the control plane

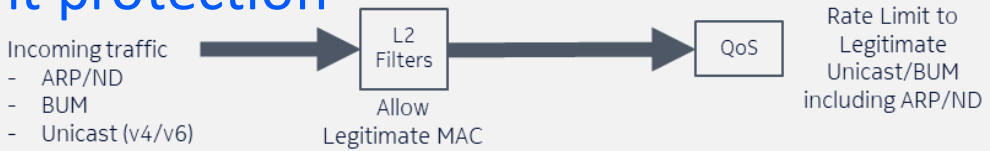
The solution – EVPN

- Enable EVPN with Proxy-ARP/ND
- Service isolation and load-balancing, secure Fabric access
- Reduce Floods
- HA with Multi-Homing
- ECMP across the MPLS-SR Fabric
- Future proof with automation capabilities



IXP Secure Fabric – Inherent protection

Gated lines of defense



First line of defense

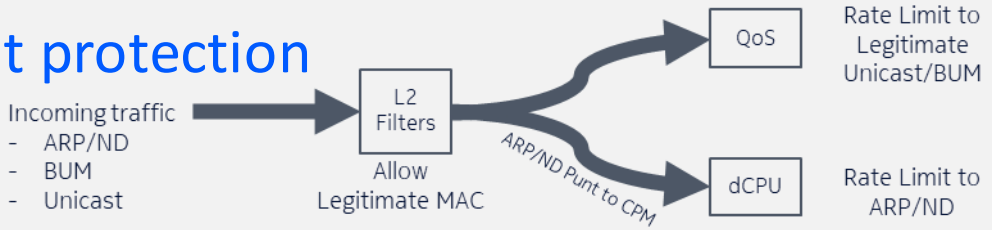
- One Static MAC entry on customer logical interface
- VPLS FDB static mac association to logical interface
- ACL filter list to block traffic at IPv4/6 and MAC layer
- Block unknown multicast and broadcast traffic, only allow ARP
- Benefit: control which MAC/IPv4/6 sends traffic into the Fabric, and which traffic

Second line of defense

- QoS ingress police BUM traffic
- Allow for further ingress Policer per traffic class and per customer logical interface
- Police ARP ingress traffic
- Benefit: rate-limit ingress BUM traffic and rate limit ARP
- Implement ARP policer/rate limiters in hardware
- Benefit: MAC address authorized is learned in the EVPN infrastructure, and its traffic is rate-limited with CPU load under control

IXP Secure Fabric – Inherent protection

Gated lines of defense



Third line of defense

- Proxy-ARP/ND specific protection
- Flooding control over the EVPN infrastructure
- BGP EVPN MAC Duplication detection
- Static ARP/ND entries
- Dynamic proxy ARP with MAC list
- Duplicated MAC-IP Detection under EVPN Proxy-ARP
- Attention: when Proxy ARP is enabled, ARP/ND are punted to CPM: distributed CPU protection allows handling ARP requests in hardware

Benefits

- Significantly reduce, or even eliminate, broadcast traffic from ARP/ND resolution
- Enforce strict control, ensuring that customers can only advertise and use IP addresses assigned to them
- To achieve this, only valid customer IP addresses and their corresponding MAC addresses should be installed in the Proxy ARP/ND table
- dCPU protection to rate-limit unexpected floods in hardware

IXP challenges

A big L2 switch, but not only..

A stable, secure IXP Fabric

- Only BGP route exchanges and Data traffic is desired
- Noise (unwanted protocols, BUM, etc.) can be extremely intrusive and must be avoided
- Fast convergence and redundancy needed in case of failure
- Multi-homing with loop prevention

An IXP Fabric to offer anti-DDoS services

- Enhance network availability against DDoS attacks directed to customers
- Secure by-design approach
- Maintain low latency and data privacy
- Sustainable operations
- Unlock opportunities for protection as a Service
- Seamless integration in network operations

IXP Fabric and anti-DDoS Services – External protection

State of the art – The challenge with botnet and AI driven DDoS

Botnets & AI circumvent traditional anti-DDoS systems

- Real devices with real TCP stack able to respond to TCP/app challenges
- Real traffic, often encrypted → header/payload pattern matching fails
- Increasing DDoS attack variability

For Botnet/AI DDoS:

- it's no longer about looking what's **inside** the packet
- instead, it's about
  - understanding who/what is sending the packet
  - fast detection and mitigation

Solution:

use AI powered engine for more reliable fast detection and protection

IXP Fabric and anti-DDoS Services – External protection

State of the art – Nokia Threat Intelligence Report 2025

Terabit tsunamis

Terabit-level attacks are a daily reality for many service providers, not sporadic events.
Many terabit peaks are reached under 1 minute.

Carpet bombing

52% of attacks target multiple hosts/systems (IP addresses)

Snooze & lose

78% of attacks were completed within five minutes (compared to 44% in 2024); 37% ended within two minutes

100 Tbps, when?

Between September and October 2025, within a month, attacks over ~~10~~ / ~~20~~ /40 Tbps* were recorded.

Battle for bots

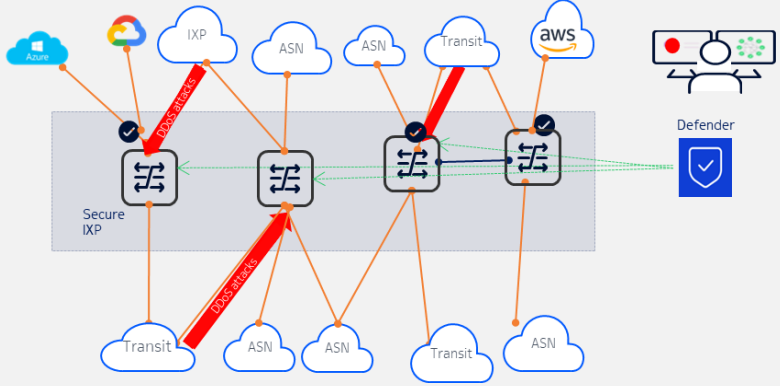
Residential proxies evolved into a complex ecosystem; malicious players fighting to hijack and control bots

AI vs. AI

Algorithmic orchestration driving attack automation; quick switching of techniques, tactics and vectors

IXP Fabric and anti-DDoS Services – External protection

Turn the problem into a resource



DDoS attacks and IXP

- DDoS protection has mainly 2 drivers, such as protecting the "providers" infrastructure from attack and their customers from DDoS attacks as Value-add service
- Historically, IXPs act as neutral network intermediary, also transporting DDoS traffic
- DDoS mitigation takes a different approach as it requires active intervention by identifying and dropping packets associated with malicious attack traffic

The solution

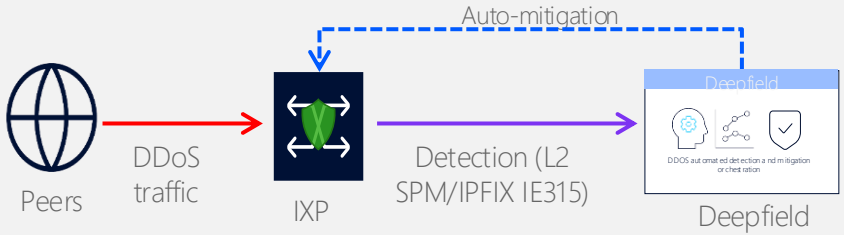
- Mitigate risks to network stability and business operations
- Offer DDoS protection as a Service: integrate into its core infrastructure
- Keep Service and SLA as contracted, enable seamless DDoS protection on IXP platforms, no rerouting to scrubbing center needs
- Sustainable: save power and operations complexity, leverage built-in security on routers
- Maintain low latency and data privacy

IXP Fabric and anti-DDoS Services – External protection

Turn the problem into a resource

Solution details

- Network-based intelligence to drive security policies on routers for edge mitigation
- DDoS protection for the IXP Fabric, also expandable to other services like Internet transit
- Example: IXP Detection on L2 interfaces, with SPM or IPFIX IE315 with detection based on dst MAC@ of peering partner
- IXP Mitigation: IP-filters on L2 interfaces



Benefits

- Target zero downtime for IXP customers and enterprises
- No change in infrastructure when routers are capable of high scale and performance filter application and reporting
- May integrate with API into Service Portal for Policy configuration and Reporting
- May add scrubber for Application layer security
- Orchestrate 3 layers of security:
  - Detection-only
  - Detection and mitigation in Fabric
  - Detection and redirection to local or 3rd party's Scrubbing Service

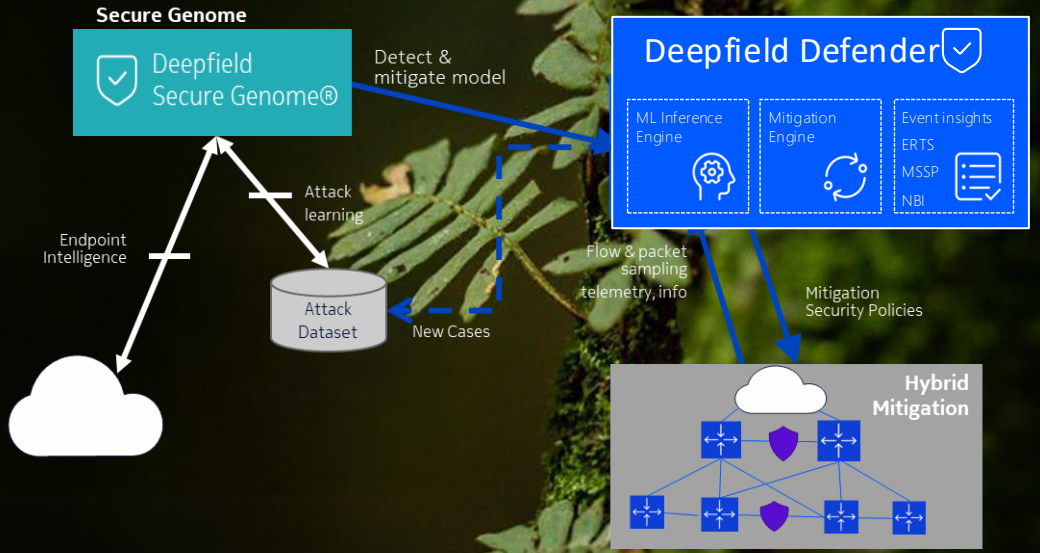
IXP Fabric and anti-DDoS Services – External protection

Next Generation Architecture

Reliable, faster DDOS detection with Secure Genome context

"zero-touch" detection and auto-mitigation

Scalable mitigation at Edge and complete with scrubbing for App layer mitigation



- Security model trained on attack data, scanning the internet, intelligence on endpoints and reputation
- Machine Learning Engine to identify dynamically attacks in real time
- AI Mitigation Controller to push security policies to the network
- Hybrid Mitigation at peering routers and/or dedicated high scale scrubber

References of Secure IXP Fabric and IXP/Hosting DDoS offering

A Secure (EVPN SR-based) IXP fabric

https://blog.apnic.net/2023/08/16/peering-lan-2-0-introduction-of-evpn-at-de-cix/

https://blog.lacnic.net/en/ix-br-promotes-the-use-of-segment-routing-v6-vpn

DDoS protection at IXP

https://www.nl-ix.net/articles-events/article/beyond-peering-our-vision-on-anti-ddos/

DDoS protection at Hosting

https://www.worldstream.com/en/about-worldstream/ddos-protection/


NOKIA

Copyright and confidentiality