CASE STUDY

Securing the crossroads of the Iberian internet: DDoS protection with sovereignty built in

ESpanix delivers automated, network-based DDoS protection to more than 200 connected networks using Nokia Deepfield Defender



NOKIA | ESpanix

ESpanix, the largest internet exchange point (IXP) in Spain and Portugal, has deployed Nokia Deepfield Defender to protect its exchange platform and the more than 200 national and international networks that connect to it against distributed denial-of-service (DDoS) attacks.

By combining AI-driven big data analytics from Deepfield Defender with mitigation performed directly on the Nokia IP routers that already carry its traffic, ESpanix detects and removes attack traffic in seconds. Removal occurs at the exchange, before traffic reaches member ports and their end customers, without diverting internet traffic to scrubbing centers outside its network or outside the borders of Portugal and Spain.

The deployment allows ESpanix to offer an optional value-added DDoS protection service to its connected networks, which together serve the majority of internet end users across Spain and Portugal. It extends a partnership that in 2025 made ESpanix the first IXP in Spain to offer 400G connectivity, built on Nokia IP routing and optical transport.

This case study describes how ESpanix turned the central crossroads of the Iberian internet into the smartest place to stop DDoS attacks. With Deepfield Defender, ESpanix makes the national internet more resilient, keeps traffic and security protection within its own borders, and adds a new dimension to the services it offers its members.



“This protection is delivered entirely within our network, across the datacenters in Madrid, Barcelona and Lisbon where we connect with our members. This ensures that local traffic remains local.”

Javier Achirica

CTO, ESpanix

ESpanix: Where the Iberian internet comes together

ESpanix is the leading IP traffic exchange in Portugal and Spain and one of the main IP interconnection points in southern Europe. It has carried internet traffic across the Iberian Peninsula for more than 25 years, growing into a neutral hub where access operators from both countries meet the world's largest cloud, content and carrier networks. The company's motto captures its place in the national internet: "Si pasa en Internet, pasa por ESpanix," which translates to "if it happens on the internet, it passes through ESpanix."

The ESpanix Node connects more than 200 customer networks across six points of presence in the metropolitan areas of Barcelona, Lisbon and Madrid. This includes most national internet service providers (ISPs), content and cloud providers, and national and international carriers. The Node switches more than 2 Tb/s of traffic on 260 Tb/s of installed capacity. A single connection unlocks access to most networks operating across the peninsula, without the burden of running cross-contracts with each individual operator.

Neutral by design

ESpanix is governed by a non-profit association that draws its board of directors from the organizations that connect to it, including leading national and international operators. Sociedad Gestora del Nodo Neutro Espanix manages the day-to-day operation of the exchange's services and infrastructure. The company operates across three business areas: interconnection, datacenters and value-added services. ESpanix Datacenter, located in the Calle Mesena building in Madrid, is a Tier IV-compliant facility that provides direct connections to all major national and international fiber and capacity providers.

Security and quality built into the organization

ESpanix holds ISO 27001 and ISO 9001 certifications and is certified at the "High" level of Spain's National Security Scheme (Esquema Nacional de Seguridad, ENS). These credentials matter to the public-sector, enterprise and operator networks that depend on ESpanix.



A brief history of ESpanix: From national peering point to southern Europe's digital hub

ESpanix was established in 1997 as the neutral exchange point for Spanish IP traffic. It is the oldest internet exchange in Spain. From the beginning, its purpose has been to enable the country's networks to exchange traffic directly—with the lowest latency, highest capacity and full resilience.

From a national peering perspective, ESpanix has grown into a digital hub that operates across three business areas: interconnection, datacenters and value-added services. Services such as ESpanix Time, which provides redundant stratum 1 time synchronization with the highest precision available in the region, and tailored projects that combine connectivity and datacenters showed the company's readiness to go beyond peering. Its network is designed for extreme redundancy, with separate low and high LANs. In January 2025, the company worked with Nokia to upgrade each of its points of presence.

Geography now works in ESpanix's favor. The Iberian Peninsula is becoming the nerve center of the region's telecommunications, connecting continental Europe with the Middle East, Asia, Africa and the Americas through subsea cables landing in Barcelona, Valencia, Almería, Lisbon and Bilbao. ESpanix is expanding accordingly with POPs in Lisbon, Madrid and Barcelona. In January 2026, it signed a general action protocol with the Government of Aragón to establish an IXP in Zaragoza. In June 2026, it formed a strategic alliance with Epsilon Telecommunications to position the peninsula as a low-latency hub for AI and cloud services.

The traffic tells the same story. In 2026, ESpanix recorded growth of more than 12 percent, with peaks above 2 Tb/s becoming increasingly frequent. This growth is driven by everything from video calls and remote work to gaming, AI applications and low Earth orbit satellite constellations, all of which depend on the lowest possible latency.

> "For any player in the market, the decision is clear: Connecting with ESpanix means connecting with the complete ecosystem where neutrality, scale and physical proximity guarantee the performance that digital operations demand."

AMEDEO BECK PECCOZ,
HEAD OF STRATEGY, ESPANIX



How Nokia helped ESpanix evolve its network

To keep pace with the demand for high-capacity, sustainable interconnection among its then 200-plus connected networks, ESpanix selected Nokia in 2025 to deliver Spain's first 400G connectivity for IXP customers.

The upgrade uses Nokia 7250 Interconnect Routers (IXRs) to offer native 400GE ports, a more efficient and sustainable alternative to bonding multiple 100GE connections. This approach reduces complexity, power consumption and operating costs for ESpanix and its customers. Nokia 7750 Service Routers (SRs) provide edge routing, and the Nokia 1830 Photonic Service Switch (PSS) optimizes bandwidth across ESpanix's optical transport network, allowing the exchange to select the best solution for each customer's needs. Across its network, ESpanix relies on Nokia technology for edge routing, datacenter interconnect, metro links and customer-facing switches.

All ESpanix points of presence were upgraded to 400G and operational in January 2025. The layered network approach ensures scalability for larger customers and supports ESpanix's goals of expanding its footprint and evolving its infrastructure.

The upgrade added capacity and placed a programmable Nokia IP routing fabric with built-in security capabilities at every ESpanix point of presence. This created a foundation that enabled the next step for ESpanix: DDoS protection performed by the very routers that forward member traffic, without adding appliances, detours or latency.





“Our customers demand technology that is reliable and future-proof. Nokia’s solutions deliver the capacity and scalability we need to meet growing demand, enabling us to offer 400G connectivity to our members. With the support of Nokia, we not only become the most advanced IXP in the South Europe region, but our work together also aligns with our commitment to sustainability by reducing power consumption compared to traditional solutions.”

AMEDEO BECK PECCOZ,
HEAD OF STRATEGY, ESPANIX

For ESpanix, DDoS security is a service, not an afterthought

DDoS attacks continue to grow in size, frequency and complexity. Massive botnets of compromised IoT devices and weaponized residential proxies are driving hyper-volumetric and application-layer attacks against networks, services and end users. As ESpanix's CTO puts it, "DDoS attacks remain a primary threat to our connected networks daily."

As the central crossroads of the Iberian internet, the ESpanix Node plays a key strategic role in DDoS security. By stopping malicious traffic at the exchange, the Node prevents it from reaching the networks, businesses, public services and consumers behind its ports.

For an exchange, the traditional approach to DDoS security has been to stay neutral: Forward every packet, legitimate or malicious, and leave protection to each connected network. This leaves members to source DDoS protection individually, often from external scrubbing providers beyond national borders. Traffic is diverted away from the exchange, latency and costs rise, and responsibility for securing domestic traffic shifts outside the region.

ESpanix wanted a different answer. Consistent with its commitment to maximizing security across its service portfolio, it set out to integrate detection and mitigation directly into its own infrastructure and offer the result to its members as a service.

> "DDoS attacks remain a primary threat to our connected networks daily."
>
> **JAVIER ACHIRICA, CTO, ESPANIX**

It needed a solution that would:

- **Detect and mitigate** all types of DDoS attacks in seconds, in the network, before malicious DDoS attack traffic reaches member ports.
- **Isolate and remove** only unwanted traffic with the granularity to keep legitimate packets flowing.
- Cover all of its points of presence while keeping local traffic local, with no detours through third-party scrubbing infrastructure and strict data sovereignty.
- **Unify detection and mitigation** so that the service is simple to implement and operate and requires no specific technical expertise from members and their end users.
- Run on the Nokia routing fabric ESpanix already operates, without adding appliances or layers to the data path.
- **Increase the value** of connecting to the ESpanix Node and add a new dimension to the ESpanix service portfolio.

How Nokia helped ESpanix strengthen DDoS security

ESpanix selected and deployed Nokia Deepfield Defender to protect its exchange platform and connected networks. Deployment was completed across the ESpanix Node in 2026, and the new DDoS protection service was introduced to the ESpanix community and the wider industry in September 2026. Several factors drove the decision:

Exceptional detection granularity: Deepfield Defender isolates and removes only unwanted traffic, so ESpanix can substantially reduce the impact of DDoS events on its members without affecting legitimate packets that use the same ports.

Unified detection and mitigation: One system detects attacks, calculates the optimal mitigation strategy and instructs the routers to act. Unifying these capabilities makes DDoS protection far simpler to implement and operate for ESpanix and its members.

Security built into existing routers: Mitigation is performed by the Nokia IP routers that already forward member traffic at every point of presence. No additional appliance sits in the path, and no attack traffic is backhauled across the network.

Sovereignty by architecture: Because detection and mitigation occur within ESpanix's network, local traffic remains local. There is no detour through third-party scrubbing infrastructure, a strong point against alternative service offerings that route customer traffic through external providers.

A proven model for internet exchanges: With Deepfield Defender, ESpanix joins a growing group of leading European internet exchanges that use Nokia Deepfield to protect their members and build new security services on top of their interconnection platforms.

> "DDoS attacks remain a primary threat to our connected networks daily. Integrating a proactive detection and mitigation solution into our infrastructure represents a significant step forward in ESpanix's ongoing commitment to maximizing security across our service portfolio. Leveraging the exceptional detection granularity of Nokia Deepfield, we can substantially reduce the impact of DDoS events by isolating and removing only unwanted traffic."
>
> **JAVIER ACHIRICA, CTO, ESPANIX**

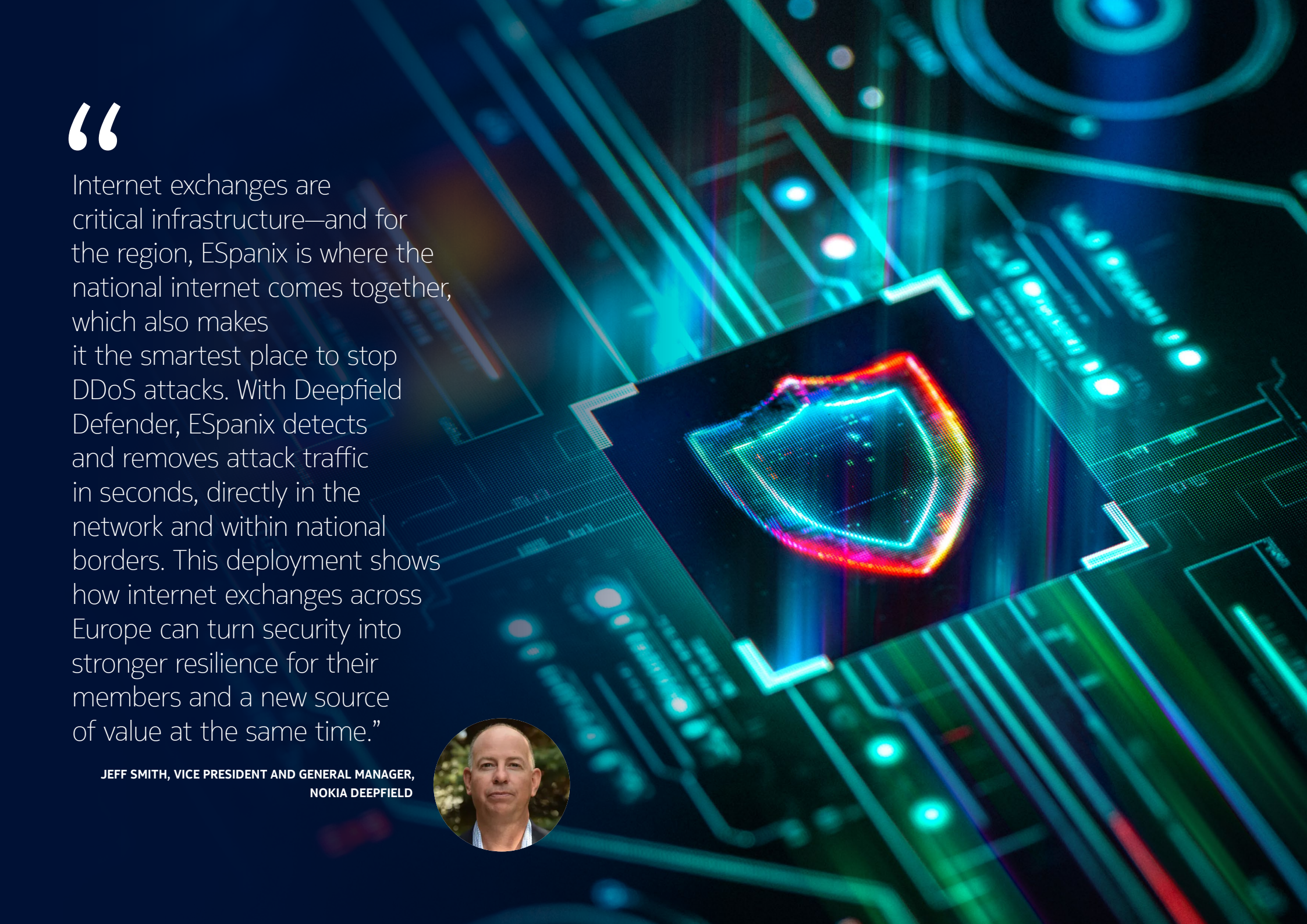
One deployment, many beneficiaries: DDoS protection as a new ESpanix service

With Deepfield Defender in place, ESpanix now offers DDoS protection as an optional value-added service to any of the more than 200 networks connected to the ESpanix Node. Subscribing members are protected at the exchange, before attack traffic reaches their ports. As the ESpanix CTO notes, “Our end users need no specific technical expertise to enjoy robust, seamless defense.”

For an internet exchange, the model has a multiplier effect: A single deployment extends protection to every network that chooses to connect through it, along with the businesses, public services and consumers they serve. One deployment has many beneficiaries.

What the service delivers

- **For members:** Fewer and shorter outages and service degradations, protection delivered where they already connect, local traffic that remains local and a new reason to connect to the ESpanix Node.
- **For ESpanix:** Security becomes a service line within its value-added services business area. As the company’s CTO describes it, this turns a defensive necessity into “a new dimension to the services we offer our members.”
- **For both countries:** Greater resilience of the shared national internet, with attacks that cross the region’s central exchange stopped centrally, and protection delivered within national borders in line with European digital-sovereignty expectations.



“Internet exchanges are critical infrastructure—and for the region, ESpanix is where the national internet comes together, which also makes it the smartest place to stop DDoS attacks. With Deepfield Defender, ESpanix detects and removes attack traffic in seconds, directly in the network and within national borders. This deployment shows how internet exchanges across Europe can turn security into stronger resilience for their members and a new source of value at the same time.”

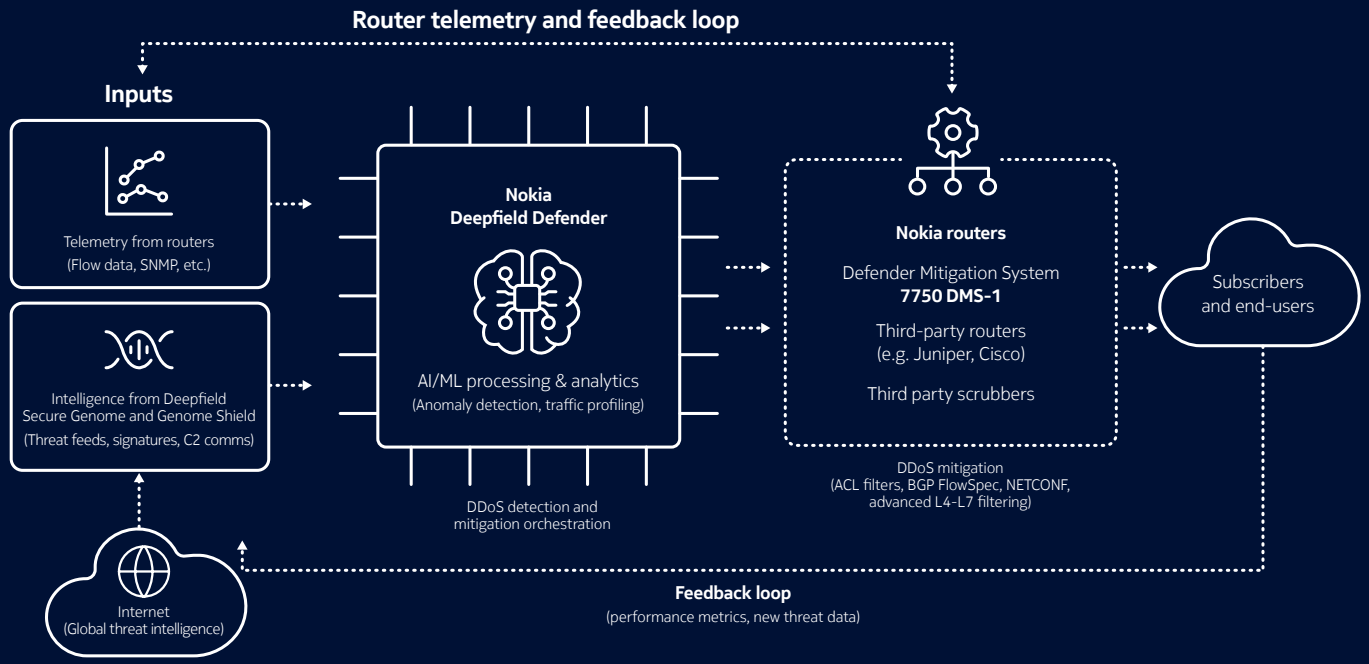
JEFF SMITH, VICE PRESIDENT AND GENERAL MANAGER, NOKIA DEEPFIELD

ESpanix's next-generation anti-DDoS solution

The Nokia DDoS security solution enables ESpanix to defend against DDoS attacks with accuracy, speed, scale, efficiency and cost-effectiveness—directly at the network edge, at every point of presence. At ESpanix, the solution comprises:

- Nokia Deepfield Defender, an AI-driven big data analytics software application that provides fast and accurate DDoS detection and facilitates agile mitigation of all types of DDoS attacks.
- Nokia Deepfield Secure Genome®, a patented, cloud-based data feed that continuously tracks the security context of the internet.
- Nokia IP routers from the 7750 SR family, which are already deployed across ESpanix network and provide built-in security capabilities that do not hinder routing performance.

Nokia Deepfield DDoS security solution



Holistic, 360-degree DDoS protection with Deepfield Defender

Deepfield Defender combines network data—including flow telemetry, DNS and BGP—with Secure Genome, which has detailed visibility into more than five billion IPv4 and IPv6 addresses, tracks more than 30 categories of internet traffic and applies more than 100 machine learning (ML) rules to classify applications and flows into security-related categories. It "knows" the security details of the internet, including prior attacks, insecure servers and compromised IoT devices that can be used for DDoS attacks.



AI-driven DDoS detection and mitigation orchestration

Correlating this knowledge with what it sees in the ESpanix network, Defender detects all types of DDoS attacks in seconds and, using advanced AI and ML algorithms, calculates the optimal mitigation strategy for each attack, or concurrent attacks, in real time. It then instructs the routers to apply precise filters that surgically remove only unwanted traffic while allowing legitimate packets to keep flowing.

Network-based mitigation with Nokia IP routers

The solution performs mitigation through Nokia routers that forward ESpanix's traffic and are powered by Nokia FP network processors. These routers deliver scalable, agile and granular DDoS mitigation at line rate, removing only DDoS traffic while ensuring predictable IP routing and high performance.

Expert DDoS support by Deepfield ERTS

Deepfield Defender is complemented by the Deepfield Emergency Response Team Support (ERTS) service: Nokia security experts, available 24/7, who further empower ESpanix's network engineering and operations teams to stop DDoS attacks.

Summary

ESpanix has placed automated, network-based DDoS security at the central exchange of the Iberian internet and turned it into a service. With Nokia Deepfield Defender, ESpanix can:

- Detect and mitigate in-network DDoS traffic in seconds, before it reaches member ports.
- Rely on exceptional granularity to remove only unwanted traffic and let legitimate packets keep flowing.
- Keep local internet traffic and security local, with no detours through third-party scrubbing infrastructure.
- Ensure that members and their end users can benefit from a unified solution that is simple to implement and operate and requires no specific technical expertise.
- Make an optional value-added service available to more than 200 connected networks, which increases the value of connecting to the ESpanix Node.
- Continue to deepen its partnership with Nokia, which enabled it to launch Spain's first 400G IXP network in 2025 and sovereign, in-network DDoS protection in 2026.

Nokia Deepfield is more than an advanced network analytics and security solution. It is a foundational enhancement that transforms the IP network into an intelligent, resilient and highly optimized asset. For ESpanix, it enables a single deployment to protect an entire national ecosystem of networks and turns security into a source of value rather than a cost.

Find out more

Visit our website to learn more about how Deepfield Defender, the Nokia 7750 Service Router and 7250 Interconnect Router families and Nokia support services can help you defend your network and your customers against DDoS attacks with unprecedented scale, effectiveness and cost-efficiency. Stop DDoS traffic before it affects your customers and services.

- Deepfield Defender nokia.com/ip-networks/deepfield/defender/
- Nokia Deepfield nokia.com/ip-networks/deepfield/
- Nokia 7750 Service Router nokia.com/ip-networks/7750-service-router/
- Nokia 7250 Interconnect Router and FP technology nokia.com/ip-networks/
- ESpanix — espanix.net

Nokia OYJ
Karakaari 7
02610 Espoo
Finland

Tel. +358 (0) 10 44 88 000

CID: 215576 (November)

nokia.com



About Nokia

Nokia is a global leader in connectivity for the AI era. With expertise across fixed, mobile and transport networks, we're advancing connectivity to secure a brighter world.

Nokia is a registered trademark of Nokia Corporation. Other product and company names mentioned herein may be trademarks or trade names of their respective owners.

© 2026 Nokia