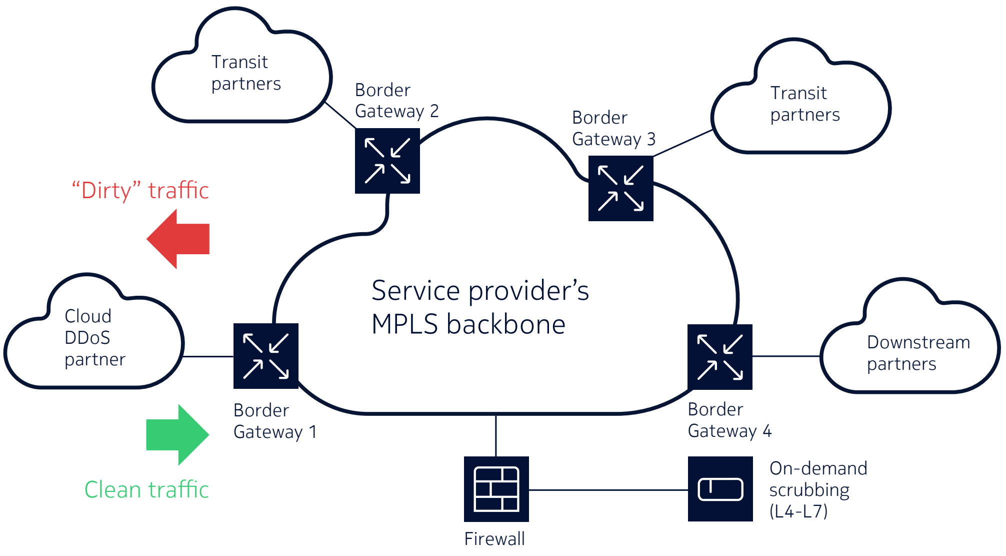
European ISP deploys next-generation DDoS security solution using Nokia Deepfield Defender and Service Routers

Use case

A European internet service provider (ISP) was looking for better DDoS protection. Its initial approach was to use a cloud-based DDoS service from one of their transit partners, and this approach worked effectively - for a while.

Figure 1. Using external cloud-based DDoS protection from a cloud DDoS security provider



Challenge

The ISP was looking for a long-term solution to obtain better protection against current and new DDoS threats; perform well under multiple concurrent attacks; scale and break the linear dependency of the price of mitigation on traffic volume (cost per gigabit cleansed), which drove exorbitant costs with the growing traffic volumes.

Several options were examined:

- Using the existing partner for cloud-based protection (i.e., continuing with the current approach);
- Using a new partner for cloud-based protection;
- Deploying their own scrubbing center;
- Deploying inline mitigation using advanced routers they have in the network (aka, using network-based protection).

The new DDoS solution needed to strike a balance between several important considerations:

- Be able to mitigate any size of DDoS attack (and handle multiple concurrent attacks)
- Eliminate network-level traffic shifts, which introduce latency and additional transport costs
- Allow scalable DDoS protection for more customers and downstream service providers
- Own security instead of relying on a black-box cloud service that gives them limited visibility and control
- Contain continuously growing costs as bandwidth and attack sizes grow.

Additional and equally important considerations were to gain more control over DDoS security and the ability to automate security responses, mitigation actions, and detailed reporting to protected enterprise customers.

Solution

The ISP has advanced, programmable routers (Nokia FP4-based Service Routers) in their network, and they have been confident in the Nokia 7750 SR routers' performance and scalability. Service Routers enable transit connectivity and private network interconnections (PNI) to the internet over multiple 100 Gigabit Ethernet links. One of the key advantages gained by using the same routing platform for network-based mitigation was obtaining the highest levels of DDoS protection while ensuring the highest performance and scalability.

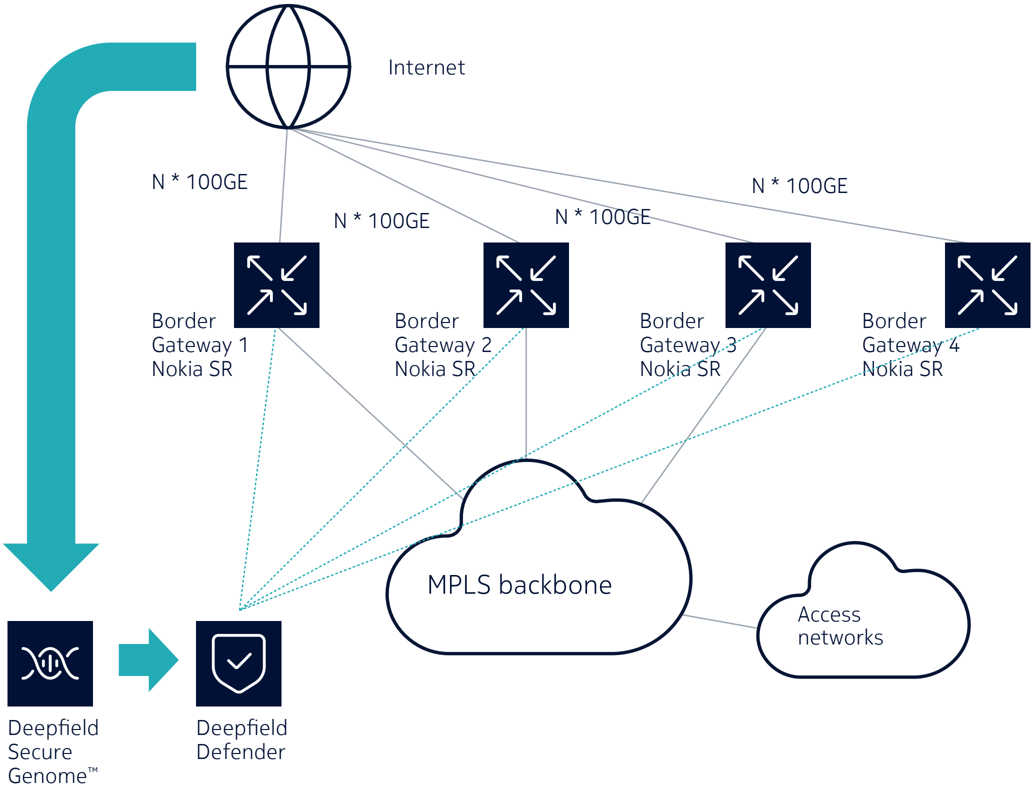
The novel approach to DDoS security, pioneered by Nokia, combines big data analytics for network-wide DDoS detection and sophisticated routers for granular, large-scale mitigation.

The solution allows the ISP to gain more control over DDoS security, detect DDoS faster and more accurately, and achieve granular and scalable mitigation using their routers - without the need for additional hardware or added layers of security equipment.

Deepfield Defender is a software-only system (no hardware probes), allowing a short time for the solution to be set and become operational.

Next-generation DDoS protection with big data analytics-based DDoS detection, and router-based mitigation

Figure 2. Nokia DDoS security solution with Deepfield Defender and Service Routers (SR)



Solution elements

Nokia Deepfield's approach uses big data IP analytics, combining network data (telemetry, DNS, BGP, etc.) with Nokia's patented Deepfield Secure Genome™. Secure Genome is a cloud-based, up-to-date data feed that tracks the security context of the internet. With detailed visibility into over 5 billion IPv4 and IPv6 addresses, tracking internet traffic over 30 categories and deploying more than 100 Machine Learning rules for automatic classification and precise allocation of applications and flows into security-related traffic types and categories, Secure Genome "knows" intricate security details of the internet (e.g., details about prior attacks, insecure servers, and compromised IoT devices that can be used for DDoS attacks).

When this information is correlated with the information from the network, it allows Deepfield Defender – a software-only based system - to detect DDoS faster and more accurately and drive agile network-based mitigation using advanced IP routers (in this case, using Nokia 7750 SR routers). Using advanced AI/ML algorithms, Deepfield Defender calculates the optimal mitigation strategy for a particular DDoS attack (or multiple concurrent attacks) and, using NETCONF protocol, sends a list of filters to Service Routers which are then applied to neutralize DDoS attacks.

Deepfield Defender became a cornerstone for the next-generation DDoS detection and mitigation solution to be deployed by the ISP. Leveraging rich telemetry and programmability of the IP network itself, Deepfield Defender delivered significant benefits over legacy (appliance-based or DPI-based) approaches: better scalability, improved detection (with lower false positives) and cost efficiency, and full traffic visibility, delivering holistic, 360-degree DDoS security required for the era of the cloud, IoT and 5G.

A holistic, 360-degree DDoS security solution

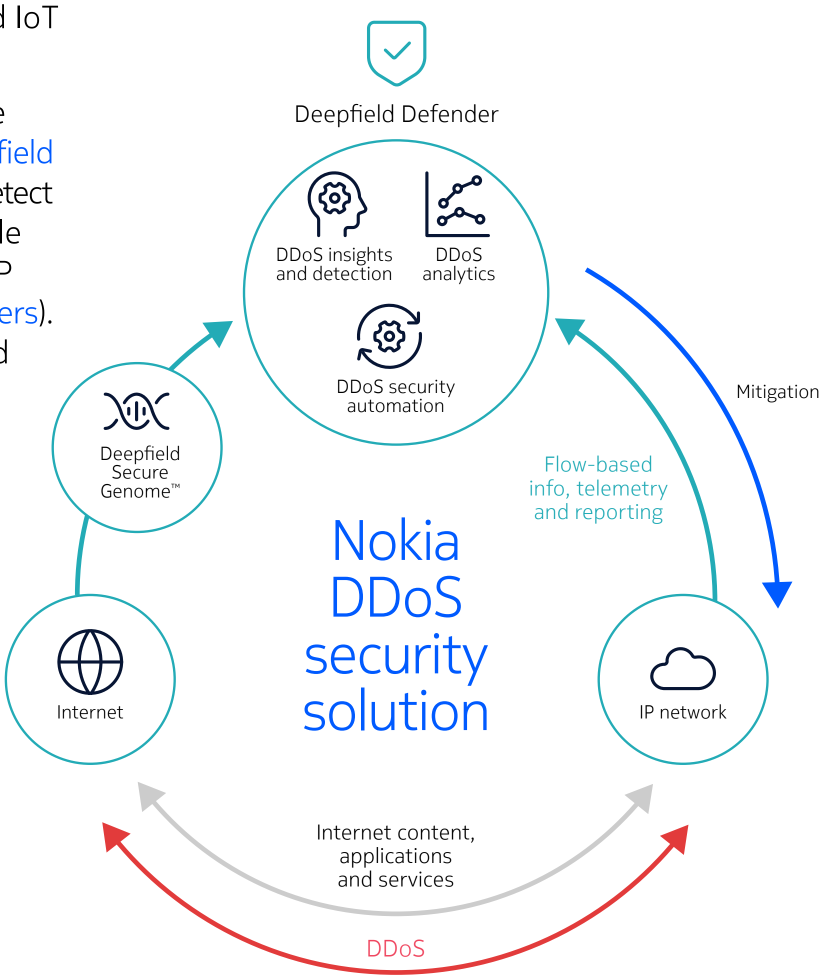

Deepfield Defender
DDoS insights and detection
DDoS analytics
DDoS security automation
Deepfield Secure Genome™
Mitigation
Flow-based info, telemetry and reporting
Nokia DDoS security solution
Internet
IP network
Internet content, applications and services
DDoS

Figure 3. Nokia DDoS security solution

Benefits

With the Nokia DDoS security solution, the ISP was able to realize its security ambitions to:

- Provide real-time DDoS detection with better accuracy
- Deliver cost-effective, agile, terabit-level mitigation, which scales to the peering capacity without additional hardware costs (which is a problem for scrubber-based solutions)
- Protect their infrastructure and customers and provide DDoS protection to downstream partners
- Automate mitigation of complex security policies to drive real-time surgical removal of DDoS threats and attacks
- Using fine-grained network telemetry and detailed reporting on mitigation, establish a closed-loop DDoS security environment for continuous monitoring and improvement.

The deployed Nokia DDoS security solution using big data IP network analytics (Deepfield) and advanced, programmable routers (Nokia Service Routers) is a cost-effective and efficient way to block existing DDoS attacks. Based on advanced technologies, it delivers capabilities and flexibility to detect new and emerging threats as they develop and evolve.

Expanding DDoS protection to all users and services with fast and accurate detection and network-wide mitigation

Using advanced, programmable routers such as Nokia FP4- and FP5-powered Service Routers for agile and scalable mitigation enabled this service provider to implement the concept of a “self-defending network,” delivering a major leap in efficacy and cost-efficiency of network-wide DDoS mitigation.

Learn more about Nokia Deepfield

About Nokia

At Nokia, we create technology that helps the world act together.

As a B2B technology innovation leader, we are pioneering networks that sense, think and act by leveraging our work across mobile, fixed and cloud networks. In addition, we create value with intellectual property and long-term research, led by the award-winning Nokia Bell Labs.

Service providers, enterprises and partners worldwide trust Nokia to deliver secure, reliable and sustainable networks today – and work with us to create the digital services and applications of the future.

Nokia OYJ
Karakaari 7
02610 Espoo
Finland
Tel. +358 (0) 10 44 88 000

Document code: CID212626 (May)