Build a self-defending IP network

Multilayer embedded IP network security is a new imperitive in the evolution of mission-critical networks

NOKIA

IP networks face new security threats

IP networks have become mission critical. Every organization – from manufacturing, to commerce, to entertainment – now depends on Communications Service Provider (CSP) IP networks for connectivity. Everyone expects real-time responsiveness, secure connectivity and 100 percent reliability in exchange for their fees.

To ensure the high performance, confidentiality and integrity now demanded of them, IP networks must overcome a new generation of network-level security threats. Distributed Denial of Service (DDoS) traffic has more than doubled since the COVID-19 pandemic began. Peak rates have surged beyond the terabit mark and have the capacity to reach the 15 Tb/s range over the next few years. New devices – including billions of Internet of Things (IoT) devices and high-bandwidth servers – are open to being hijacked and used in conjunction with reflection, amplification and carpet-bombing techniques to launch increasingly sophisticated attacks. These attacks make it harder to engineer predictably high network performance.

Some of the threats arise from how the network architecture and delivery model are changing. Network functions are being split up and distributed across the network, opening many new attack surfaces. CSPs are also using public networks to extend or complement their private networks, exposing IP traffic to the risk of theft and manipulation. The economic and political fallout from such man-in-the-middle and data breach attacks is escalating. Enterprises embracing digitalization are concerned about loss of revenue and customer dissatisfaction. Government is concerned at the growing disruption of critical infrastructure and services. CSPs looking to secure new revenue from the digitalization and network transformation of critical industries must be able to demonstrate that customer data flows are impervious to theft or manipulation. Any breach can cause serious damage to both reputations.

Current IP network security solutions lack scale and functionality

Most IP network security models are based on appliances and servers that do not scale cost-effectively for broad deployment. They leave CSP networks and many customers exposed. Vulnerabilities buried deep in router operating systems and silicon are largely unaddressed and continue to pose a significant threat.

As a result, CSPs face escalating costs fighting DDoS attacks and other security threats. Customers experience increasingly variable service quality and unease about the confidentiality and integrity of data that flows through CSP networks. CSP profitability and brand are both affected.

A multilayered approach to IP network security

To provide at-scale protection of IP networks, IP network security must be like packet forwarding – a high-performance, highly scalable capability of the network itself.

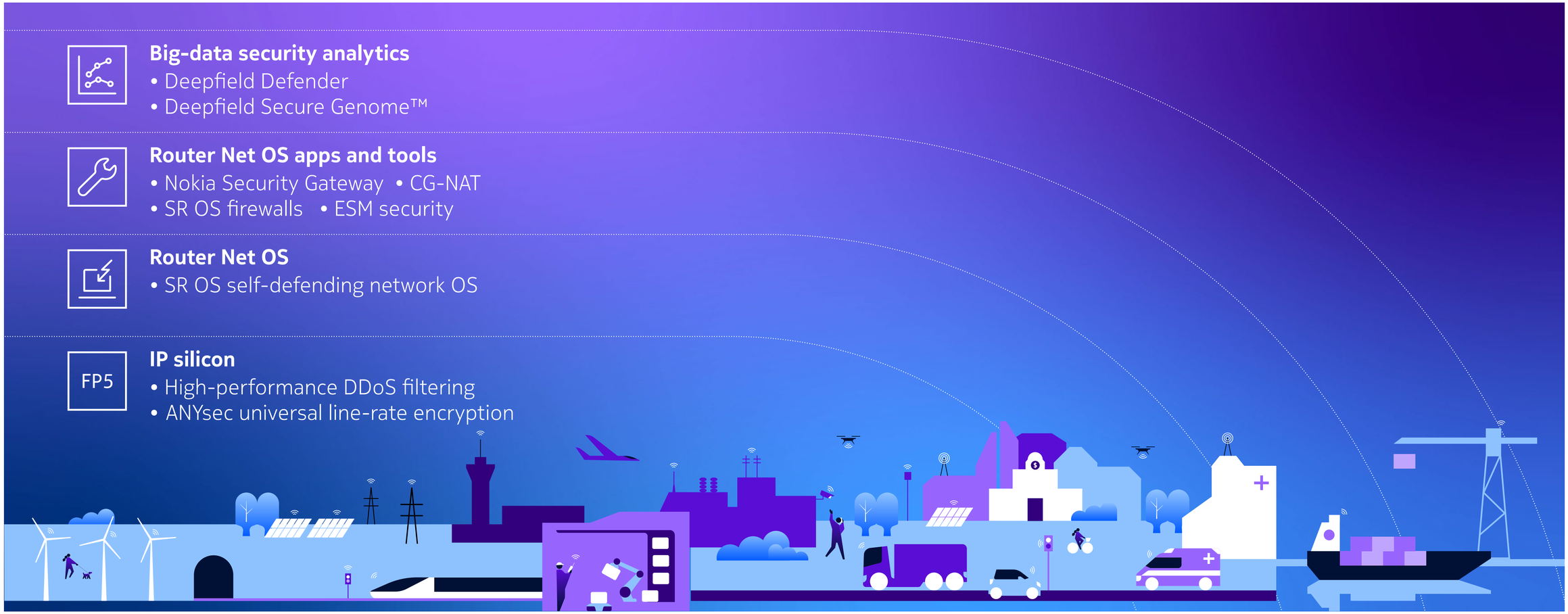
Security capabilities must be built into every layer of the network infrastructure:

- **IP silicon** must endure the heaviest DDoS attacks without impacting services. It must provide the filtering scale, flexibility and speed to be a highly precise DDoS attack sensor and mitigation device. It must provide built-in encryption to protect all data that flows through it. And it must do this all at line rate - without impacting the performance of any service running on the same chipset.
- The **network operating system (netOS)** must be impervious to attacks that try to violate its integrity, consume its resources, or sabotage its ability to view or control the network.
- **Security tools and gateways** must be embedded within networks to take advantage of the high performance, scale, and reliability of network infrastructure.
- **Next-generation intelligence and analytics tools** must be able to detect today's sophisticated DDoS attacks and automate the network's response against them – quickly and with precise accuracy.

We secure IP networks from within

To provide at-scale protection of IP networks, IP network security must be like packet forwarding - a high performance, highly scalable capability of the IP network itself. Nokia has pioneered this approach by embedding security into the DNA of every layer of our IP network infrastructure, providing high-performance, fully featured and at scale protection for your mission-critical networks.

Nokia is the first to deliver this multilayer, embedded approach to IP network security with our secure IP network portfolio. Security is built into every layer of our Nokia 7750 Service Router (SR) and 7950 XRS series of routers.



FP5 self-defending IP network silicon

FP5-equipped routers and gateways offer effective protection against network-level threats.

FP5-equipped routers and gateways allow CSPs to respond to attacks quickly and more effectively than ever before. With FP5, tens of thousands of hardware-based filters and queues can be applied almost instantly to identify and stop attacks with unparalleled precision and speed. This is achieved without impacting legitimate traffic, or the performance of other services running on the same chipset.

ANYsec encryption extends the low latency and simplicity of MACsec to MPLS, Segment Routing and IP networks. It provides CSPs with the freedom to transform IP-based services into secure IP based services on demand. Instead of treating encryption as an expensive, complex and limited capability that requires significant advanced planning, CSPs can flip a switch to turn on encryption whenever and wherever it is required – no matter what service or network transport is being used. And because it is silicon-based, turning on ANYsec will have no performance impact on any other service or function running on the router, no matter what percentage of traffic is encrypted.

Our FP5 network silicon protects the 7750 SR control plane, the internal software that controls the router and all its interactions with the network. That's because FP5 isolates all control plane traffic coming from partner routers and assigns each interaction its own fair-share slice of the control plane processor. This high-resolution approach to sharing control plane cycles limits the damage one attack can cause – without interfering with the thousands of legitimate control plane interactions that keep networks stable.

SR OS self-defending network operating system

Every feature in our SR OS network operating system undergoes rigorous testing to expose and correct potential vulnerabilities. Automated source code inspection and code analysis tools look for errors that can lead to security breaches. External agencies examine object code from the outside in, looking for any vulnerabilities that could be exploited. The development process itself – from coding to the build process to software delivery – is based on security best practices. These have earned SR OS and the 7750 SR and 7950 XRS accreditation from key security agencies.

Network-level security tools and gateways

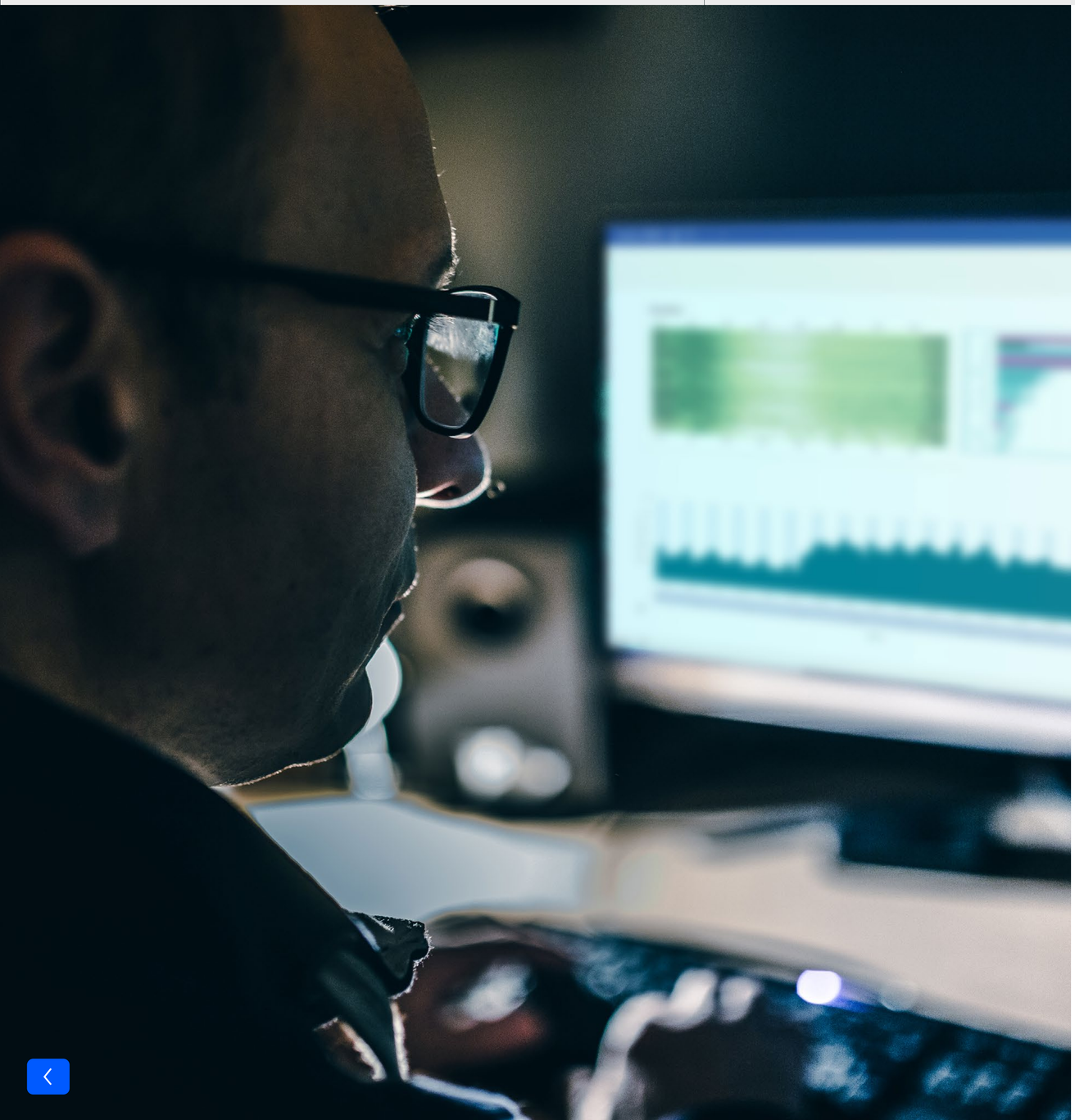
Nokia network-level security tools and gateways are built on Nokia's highly-secure and carrier-grade 7750 SR and SR OS platforms. This allows the IPsec gateway (Nokia Secure Gateway) to support an industry-leading 32,000 IPsec connections and 960 GB/s of encrypted traffic from just one chassis. It also leverages other carrier-class attributes including:

- Fully redundant hardware;
- High availability across control modules;
- Non-stop routing and services;
- Load balancing across ports, tunnels, and cards; and
- Fully-transparent multi-chassis redundancy.

The Nokia SR OS Firewall uses the protective cocoon of SR OS to create secure zones in mobile networks. Nokia SR OS firewalls can share a platform with other SR OS systems. This helps to optimize performance, minimize costs, and reduce overheads because the systems can be managed as a single node.

SR OS also defends subscriber management functions such as Nokia's Broadband Network Gateway (BNG). It does this by monitoring network interactions and discarding any unauthorized attempts to bond with the network, exhaust finite resources, or spoof IP addresses.

FP5-equipped 7750 SR routers and gateways can also control traffic from infected subscribers and IoT devices, without impact to performance.



Deepfield Defender: Big data-driven DDoS intelligence and analytics

Nokia Deepfield Defender works with FP5-equipped 7750 SR routers and gateways to provide more effective protection against DDoS attacks, even as they increase in scale, sophistication, and frequency.

In the past, peering routers were forced to send all suspected DDoS traffic to centralized scrubbing centers containing mitigation appliances. This approach relied on manual processes, was prone to false positives and negatives, and came at a considerable cost in licenses and backhaul bandwidth.

Deepfield Defender changes this model with unique situational intelligence and automation. It uses the high-scale, high-resolution filtering and reporting capabilities of 7750 SR and 7950 XRS networks for faster and more accurate DDoS identification and mitigation.

The process starts with Deepfield Secure Genome which provides visibility into more than 95 percent of internet traffic, with a level of intelligence that was previously unavailable to CSPs. Deepfield Defender's multidimensional analytics combine Secure Genome with a CSP's network data to provide an instant and precise snapshot of traffic flowing anywhere in the network. Automated mitigation workflows can set up tens of thousands of high-resolution filters on the 7750 SR or 7950 XRS in seconds. These filters can provide visibility into potential attacks, or discard, rate-limit, or forward packets for additional analysis – all without impacting performance.

Achieve universal DDoS protection

This new breed of network-based identification and mitigation is far more accurate and cost-effective at eliminating volumetric DDoS attacks, compared to the appliance-based scrubbing center model.

It allows CSPs to turn on volumetric DDoS protection everywhere in their network, including in the services, data center, and peering edge. It extends protection to all customers, not just the top 5 to 10 percent, which increases customer satisfaction. At the same time, it eliminates the impact of customer-targeted DDoS traffic on a CSP's service quality and bandwidth consumption.

To find out more, visit: Nokia IP Network Security web page

Nokia OYJ
Karakaari 7
02610 Espoo
Finland

Tel. +358 (0) 10 44 88 000

CID: 210518 (May)

nokia.com

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.