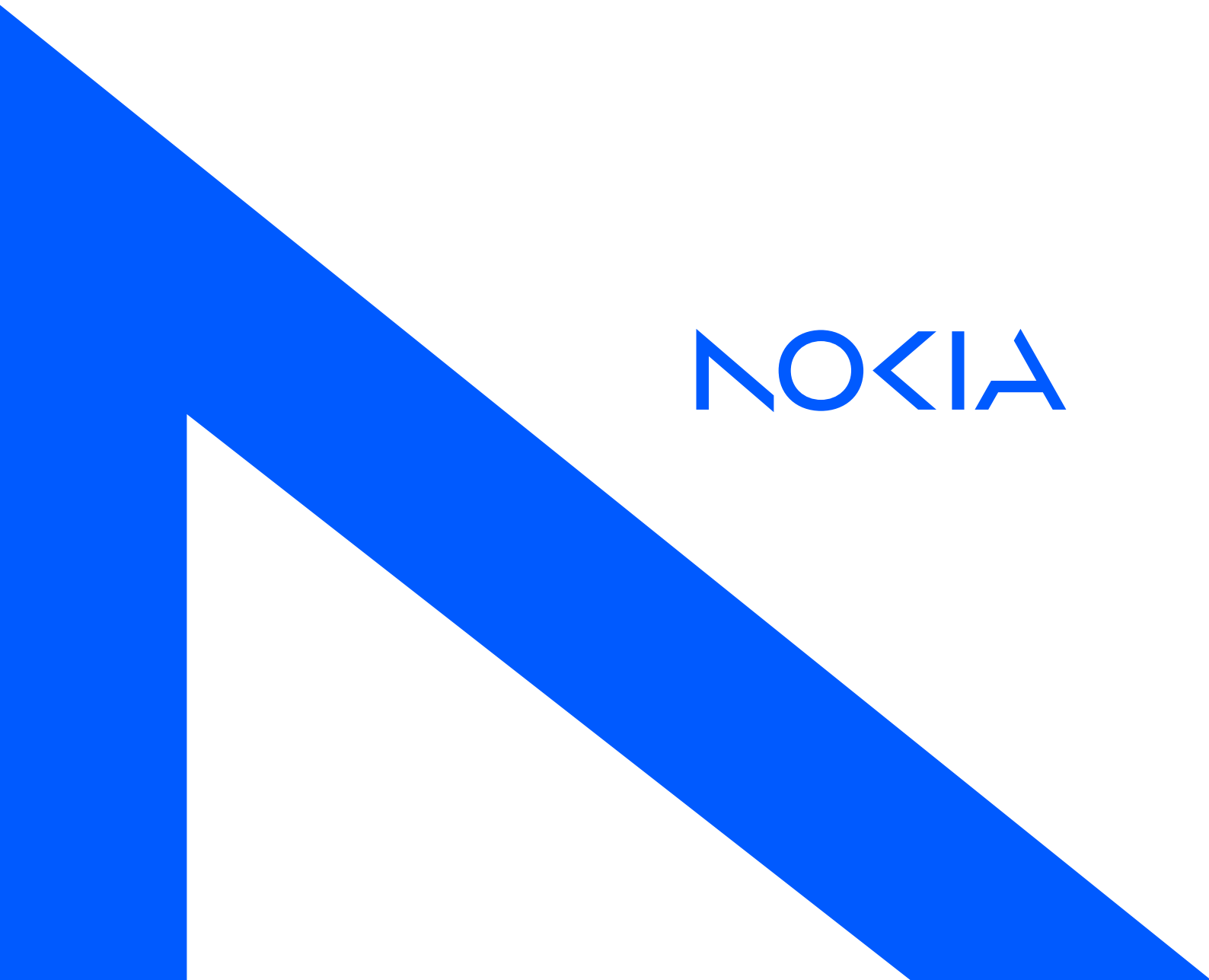
A multi-layer embedded approach to IP network security

A strategy to safeguard business continuity against IP network threats

Application note



Abstract

With digital transformation, AI adoption and the alarming growth in cyberthreats, our networks and data have never been at such risk of exploitation. Prioritizing security in the design and support of the many systems the IP network comprises—especially as the policy and regulatory environment continues to evolve—is at the heart of Nokia's multi-layer embedded approach to IP network security. By melding together high-performance IP silicon with platform-level security, breakthrough apps and tools within the Network Operating System (NOS), AI-driven big data security analytics and quantum-safe cryptography innovation, network operators will be equipped to identify and mitigate against the most egregious of modern and future threats.

Contents

Introduction

In the history of computing, our networks and data have never been more at risk. Most of the world's content and economy is digitalizing, causing corporate, government and personal data to traverse the world's public and private internets in petabyte volumes. The steady growth in Artificial Intelligence (AI) further compounds liability, widening the cyberthreat landscape in potentially alarming ways.

The telecommunications network underpins this superfluidity, ensuring the continuity of our business and social needs. Yet, as increasingly more sophisticated and devastating cyberattacks loom, such digital hyperconnectivity requires hyperprotection of both the active inflight data and the network.

Prioritizing security in the design and support of the many systems the network comprises—especially as the policy and regulatory environment continues to evolve—is at the heart of Nokia's multi-layer embedded approach to IP network security.

At Nokia, we have a deep history in IP networking, security and telecommunications innovation. We have leveraged this to identify the vector points most fundamental to IP network security, melding together high-performance IP silicon with platform-level security, breakthrough apps and tools within the Network Operating System (NOS), and AI-driven big data security analytics. As well, we help prepare today for the coming quantum paradigm shift, leveraging in-house Nokia Bell Labs quantum computing innovation to shield against future threats.

Nokia's IP network security approach yields numerous benefits for IP network operators. Security at scale and enhanced trust in our communications systems, along with the security intelligence, analytics and automation to detect and mitigate distributed denial-of-service (DDoS) attacks in our evolving AI-driven big data environment.

Figure 1. Our multi-layered embedded approach to IP network security

IP silicon

IP network silicon is vital to IP network security, and the Nokia FP chipset is engineered to safeguard business continuity against the most malicious threats. This is where Nokia's multi-layer embedded approach to IP network security begins, with efficient and high-performance security features prioritized in the IP network infrastructure itself.

Integrated line-rate MACsec and ANYsec network encryption, secured with AES-256 network encryption, delivers highly scalable multi-terabit secure and trusted network connectivity.

Figure 2. Integrating security right down to the silicon level

- Line-rate network encryption
- Highly scalable ACL filtering with no performance penalty
- DDoS attack mitigation

Nokia FP silicon provides the filtering scale and performance headroom necessary to be a highly precise attack sensor and mitigation element. Even with the application of hundreds of thousands of ACL filters in the FP-based routing platforms, there is no performance impact.

The mitigation aspect of the Nokia DDoS security solution combines packet forwarding capacity and performance with the enhanced packet intelligence and control capabilities of Nokia FP4, FP5 and FPcx-based routers and an FP5-based dedicated mitigation platform—the 7750 Defender Mitigation System (DMS) —with advanced DDoS countermeasures. Nokia Deepfield Defender acts as a security analytics, detection and mitigation control platform, driving granular, scalable and cost-effective mitigation of all types of DDoS either on the network edge (FP-based routers) or on the 7750 DMS.

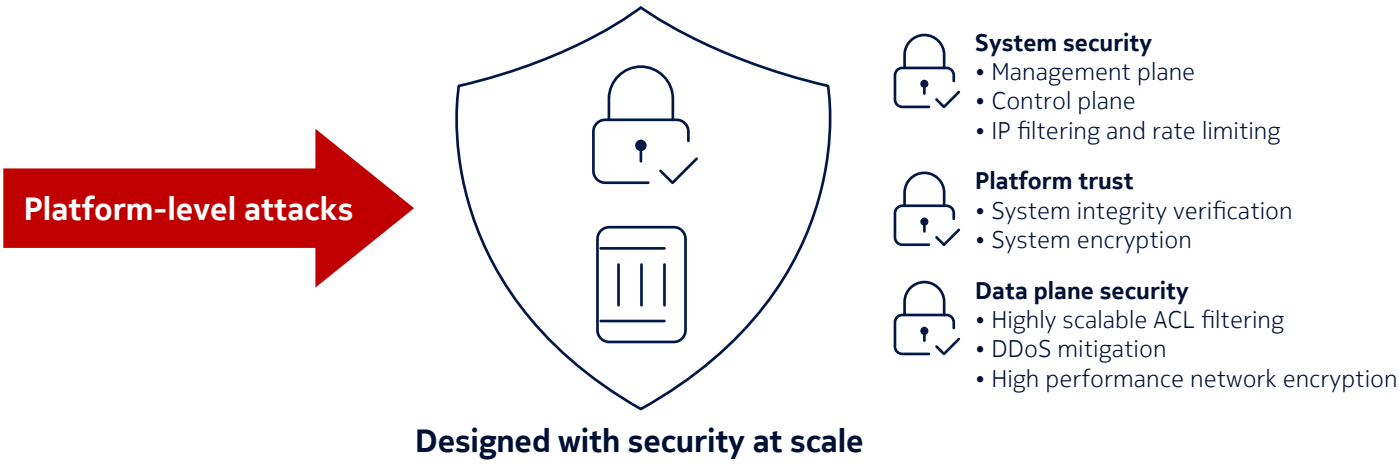
To ensure deterministic network performance and service quality, both mitigation and detection can be used at line rate without impacting the performance of other services running on the same chipset.

IP Trusted systems

When an attack strikes at the platform level, Nokia's approach to prioritizing security and trust means that the management, control and data planes are designed with the capabilities and considerations required to both anticipate and withstand these threats.

System security

Figure 3. System security and platform trust



At the management plane, security includes defense against unauthorized access through capabilities such as flexible user Authentication, Authorization and Accounting (AAA); login control; event logging and encrypted management protocols. For the control plane we implement multiple security controls for routing protocols such as:

- Authentication (including keys)
- Key chaining
- Database limiting
- Time-to-live (TTL) security
- Prefix limiting
- Origin validation
- Route filtering
- Policies management
- Neighbor disablement

To mitigate a flood of traffic reaching the system control and management planes we implement multiple levels of queuing, policing and filtering in both distributed and centralized architectures.

Platform trust

Nokia's platform trust is anchored in the pillars of system integrity verification and system encryption. We implement Secure Boot, which provides a foundation for other platform trust capabilities. Secure Boot ensures that the software executed by the system originated from Nokia and is trusted.

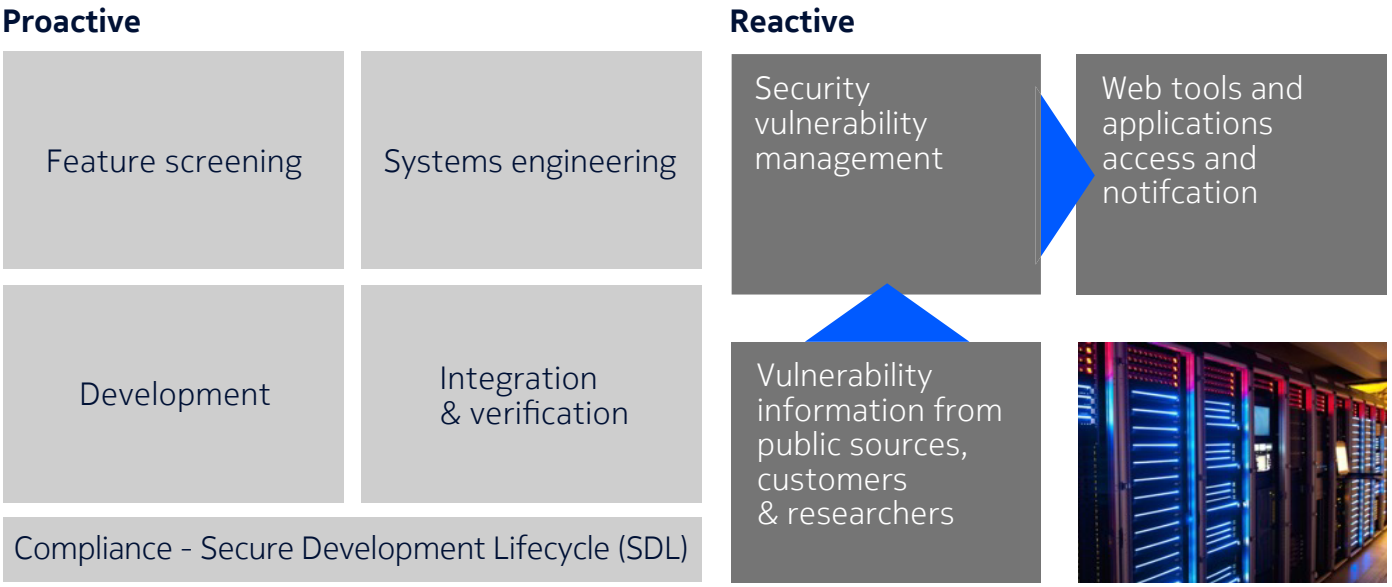
Building on IEEE 802.1AR requirements for device identity keys, the Nokia approach implements Trusted Computing Group (TCG) compliant Trusted Platform Module (TPM) 2.0 Keys for Device Identity and Attestation. This identity key and certificate are then used in software features to provide cryptographic evidence that the system used by the customer is manufactured by Nokia. One example is secure boot-strapping of the system using the Secure Zero Trust Provisioning (SZTP —as defined in RFC 8572—and "Bootz".

TPM 2.0 also provides the hardware root of trust for measurement and attestation as well as secure storage for disk cryptographic keys. Measured Boot complements Secure Boot by providing cryptographic evidence that each piece of the system boot chain uses the software version allowed by a customer.

Secure product lifecycle

Nokia approached planning for security management from both a proactive and reactive point of view. Proactively, Nokia focused on key elements in the building, coding and testing of our products. Given security events can happen in the field, after products have been deployed in customer environments, the process also identifies and mitigates these risks reactively throughout the secure product lifecycle.

Figure 4. Key components of the security management process



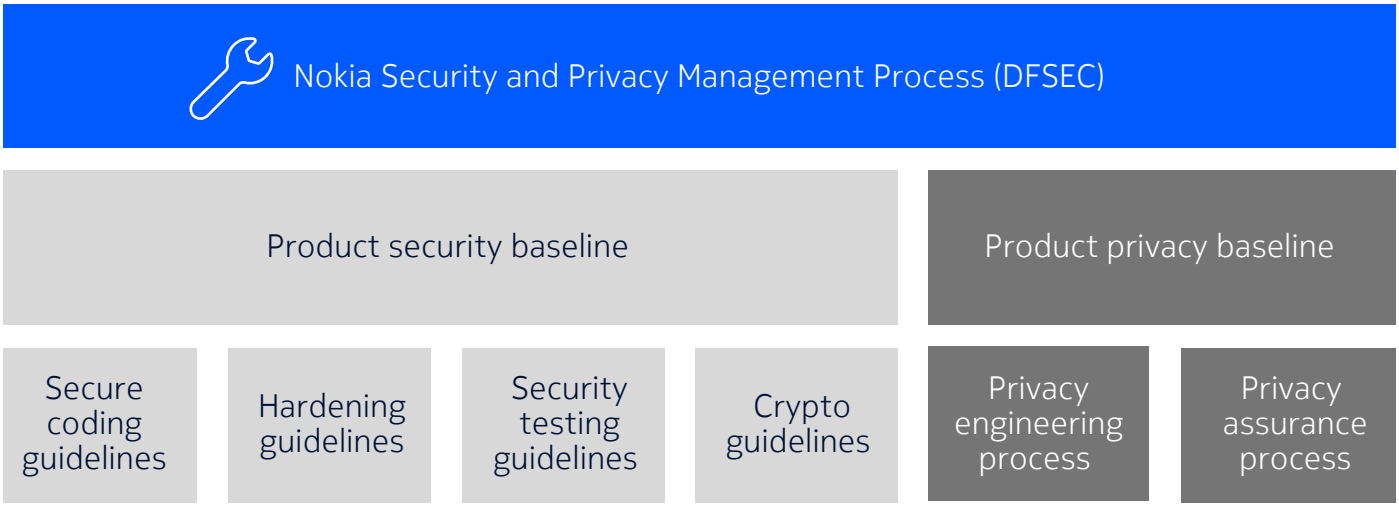
Key components of the security management process

With a focus on the continuous integration and assimilation of the industry's best practices, standards and regulations, the combination of proactive and reactive Nokia IP network security management involves:

- **Proactive measures**: Feature screening, systems engineering, secure coding, integration and verification and compliance to measure against our Secure Development Lifecycle (SDL) process.
- **Reactive measures**: Vulnerability information from a range of inputs including Computer Emergency Response Team (CERT), assessments and tools, technical alerts and customer communications.

Our SDL supports our security by design culture, continuously assimilating and integrating security best practices, in-house requirements and industry-sourced specifications into both product security and product privacy baselines.

Figure 5. Secure Development Lifecycle



The product security baseline is tied to process elements and core activities that are undertaken within the SDL, including:

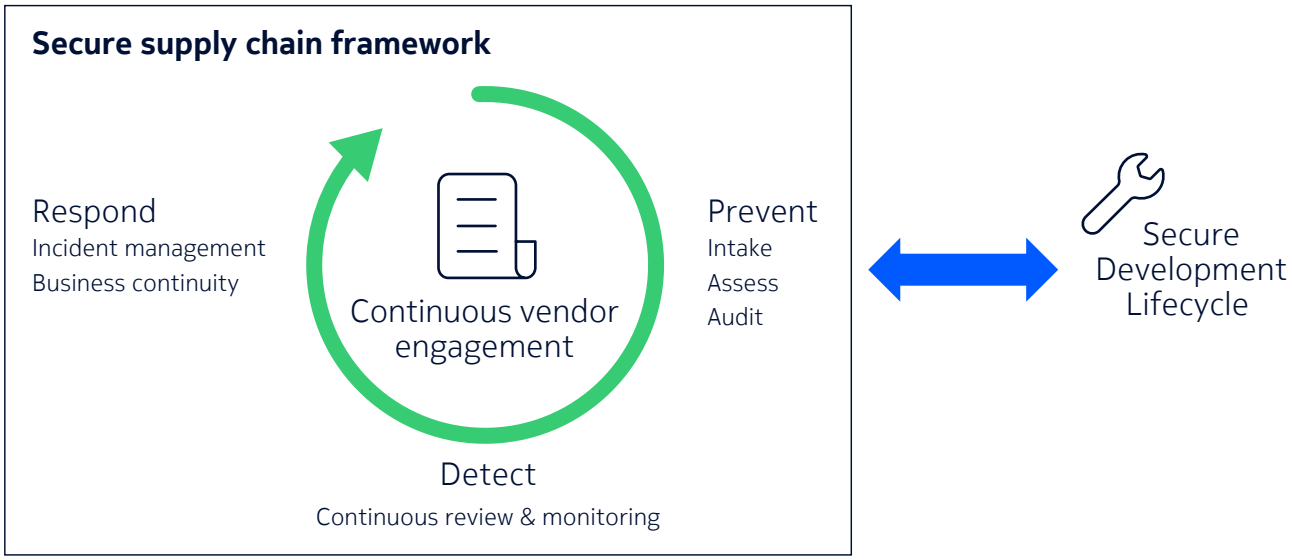
- **Secure coding** guidelines that help developers write secure code in the languages Nokia utilizes in product building
- **Product hardening** to ensure that customers do not have to do extra work to make them secure
- **Rigorous security testing** using optimized tools and manual methods to identify product vulnerabilities
- **Crypto guidelines** drawn from industry cybersecurity standards and certifications such as Federal Information Processing Standards (FIPS) and National Information Assurance Partnership (NIAP)

The product privacy baseline is founded on the concept that our products and software are designed to favor privacy, including securely encrypting collected and stored data.

Secure supply chain

Establishing trusted systems requires that the supply chain from which hardware and software components are sourced is secure as well. Nokia has adopted a strategy of prevention, detection and response to ensure this security is maintained at every point in the relationship.

Figure 6. Secure supply chain framework



Nokia strictly adheres to a set of oversight and risk management principles. This includes first identifying what needs protection, establishing clear minimum-security requirements, then understanding supplier security postures, and assessing supplier risks.

Security is embedded in the contracting process and upheld by both Nokia and our suppliers.

Raising awareness and training within the supply chain is also critical. New suppliers undergo a comprehensive onboarding process that clearly stipulates Nokia's security requirements around vendor contracts. This is followed by security and privacy vendor risk assessments and training on Nokia processes. Once established as a supplier, Nokia conducts regular supplier reviews and continuous monitoring with a focus on ensuring business continuity.

Being prepared to support suppliers during security incidents is crucial as well. An established incident response process is triggered in the event of an issue, with the goal of fast response and resolution.

This structured approach and eye on continuous improvement ensures that we maintain a resilient and trustworthy supply chain allowing Nokia to build trusted and secure products.

Supplier components are selected for use in our products and further secured through the Nokia SDL and DFSEC processes.

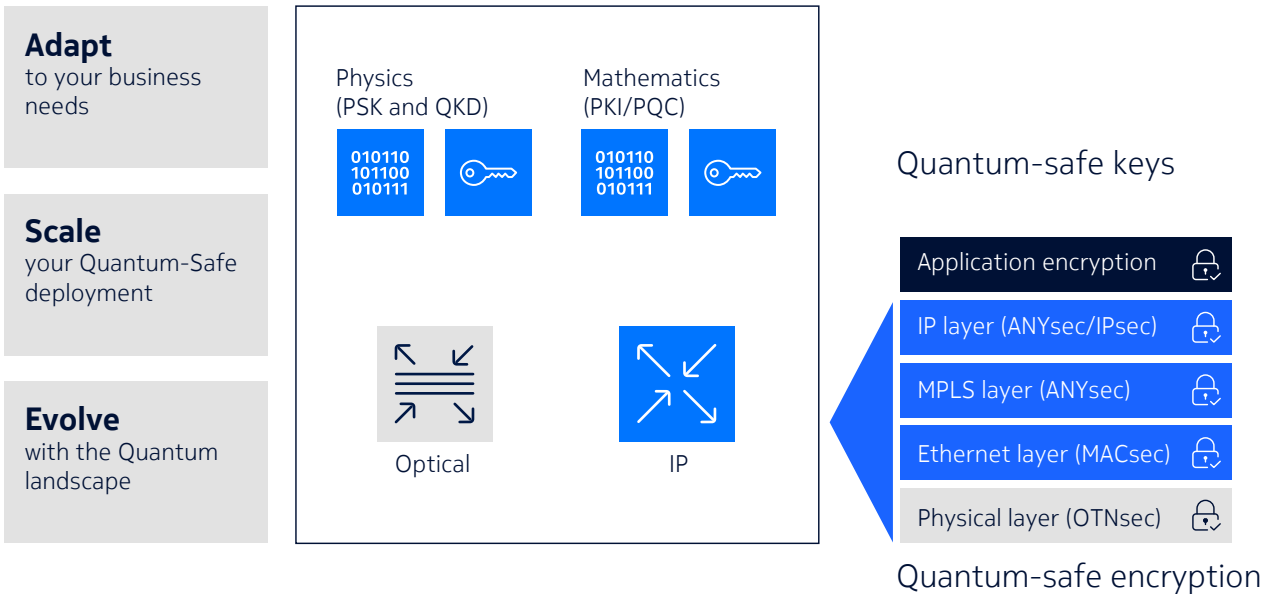
Quantum-safe networks

As our reliance on safe and trusted connectivity increases, it is essential that we act now to shield against the quantum migration challenge. While the timeline for a cryptographically relevant quantum computer (CRQC) is uncertain, the cybersecurity migration needed to counter this threat is the largest the Information and Communication Technology (ICT) industry has faced and will require considerable time and effort.

The Nokia IP network security approach is focused on maintaining a digital communications infrastructure that remains secure, reliable and trustworthy for consumers, enterprises, mission critical infrastructure builders and Communications Service Providers.

Called Quantum-Safe Networks (QSN), Nokia's quantum-safe solutions are proven and ready for immediate implementation. At the same time, Nokia Bell Labs is driving continued innovation with key academic and technology partners that will shape the future of quantum-safe network solutions.

Figure 7. Nokia Quantum-Safe Networks

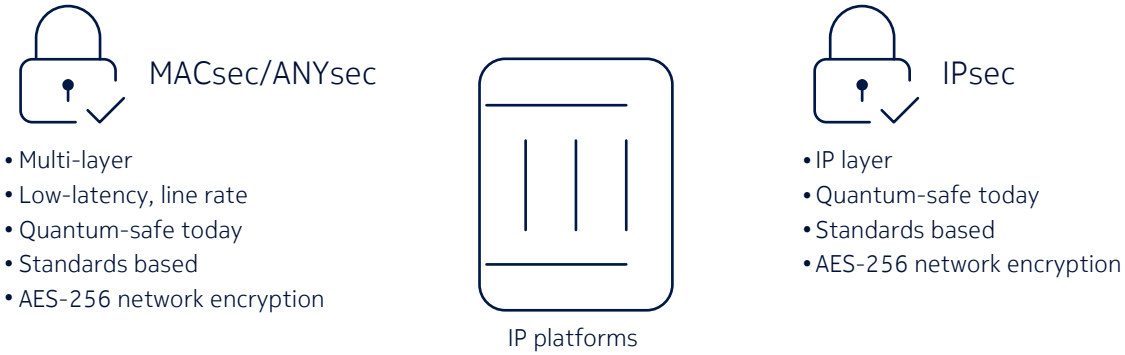


A defense-in-depth approach can deliver quantum-safe security through the appropriate application of quantum-safe IP or optical cryptography. With Nokia QSN, a quantum-safe outcome can be achieved today with the application of one of our quantum-safe IP network cryptography technologies - MACsec, ANYsec or IPsec. Or a customer may choose to deploy multiple quantum-safe network cryptographic technologies in a multi-layer approach.

This approach is complementary and helps to manage the risk in the evolution of application layer cryptography. The approach can be adapted to a customer's business and use case needs, delivers confidence to scale network deployments and supports strategy modifications as the quantum threat evolves.

By combining crypto-agility and crypto-resiliency in a defense-in-depth approach, we create a comprehensive and proactive security posture that can withstand current and future threats, ensuring the security, trust and resilience of our digital infrastructure.

Figure 8. Quantum-safe IP cryptographic technologies



Deployed globally on field-proven IP portfolio

Support for multiple IP cryptographic technologies forms part of our multi-layer defense-in-depth IP cryptography:

- Silicon-based line rate 802.1AE MACsec and 802.1X MACsec Key Agreement (MKA) protocol combined with quantum-safe symmetric cryptographic keys to deliver secure and trusted quantum-safe Ethernet network connectivity.
- Enhanced 802.1AE/802.1X MKA protocol combined with quantum-safe symmetric cryptographic keys to deliver what we call ANYsec. With flexible granularity, multi-layer end-to-end or hop-by-hop high scale, granular secure and trusted services can be deployed transparently to the existing Ethernet, MPLS and IP network infrastructure, speeding the velocity of deployment and delivering quantum-safe network connectivity today.
- IPsec capabilities that enable trusted and secure quantum-safe network connectivity, with industry leading scale, capacity and resiliency to address a range of network and market applications including mobile RAN, core and transport networks and secure enterprise access. Standards-based, Nokia IPsec capabilities include support for transport and tunnel modes, along with both public and private services. Quantum-safe today through the support of RFC 8784, the Nokia IPsec cryptographic solution will evolve to incorporate the new post-quantum cryptography (PQC) mathematical algorithms in alignment with the industry.
- Nokia MACsec/ANYsec and IPsec cryptographic technologies are underpinned by quantum-safe AES-256 block cipher datapath network encryption.

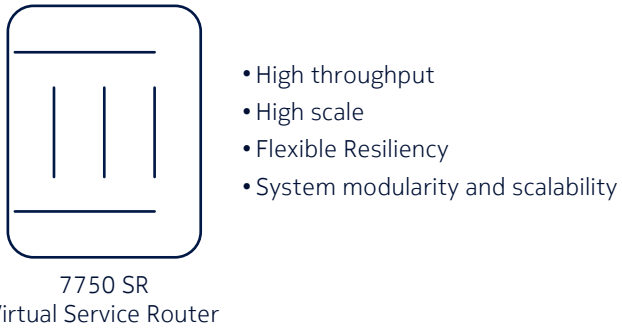
Router NOS applications and tools

As data volumes explode and the number of connected devices proliferates, the urgency around protecting against cyberthreats grows. The Nokia IP Network security approach includes several robust options within the Router NOS apps and tools layer that scale and evolve with the threat landscape while safeguarding the high performance and reliability of the network infrastructure.

IPsec Security Gateway

Nokia's carrier grade router-based IPsec Security Gateway solution inherits the scale, resiliency and security of the 7750 SR infrastructure. A single Nokia Secure Gateway can support up to 32,000 macro base stations or 500,000 small/femto cells, and up to 3.2Tbps of encrypted traffic.

Figure 9. IP security gateway



Distributed architecture to deliver industry leading IPsec performance

The solution delivers flexible resiliency, supporting inter-chassis 1:1 or N:M stateful redundancy models and combining system modularity with scalability and a single system IP address to help simplify operational deployment.

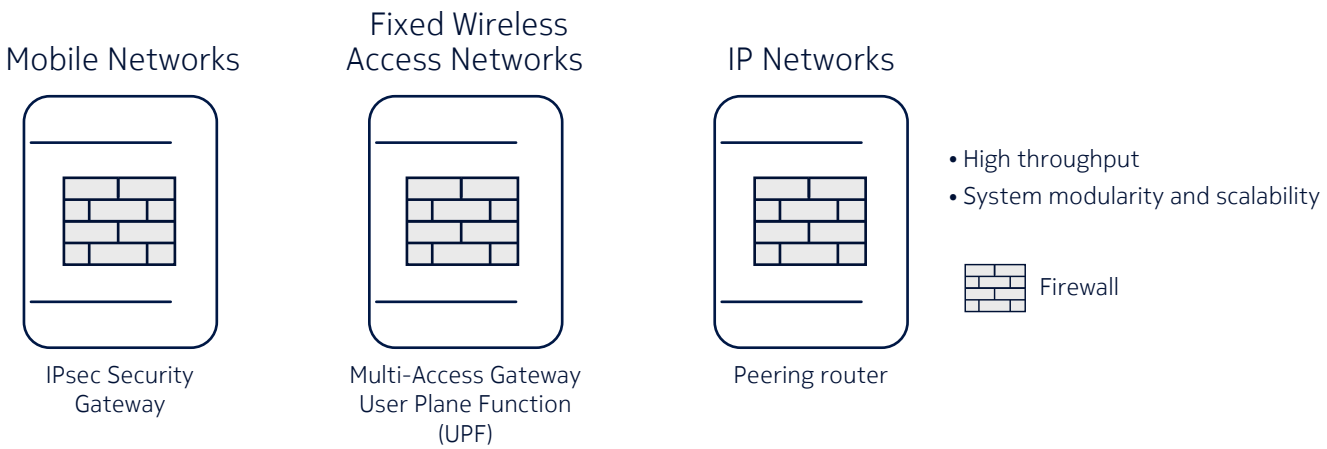
A distributed architecture allows for greater scale, redundancy and flexibility in securing IP networks. The IPsec Security Gateway distributes both the Internet Key Exchange (IKE) control plane traffic and the data plane traffic across the system. As well, multi-core processors for the IKE process greatly enhance tunnel setup and distribution of data plane traffic across multiple cores, which can increase overall IPsec performance.

The IPsec Security Gateway function can be deployed on the 7750 SR Extended Service Appliance (ESA), 7705 Service Aggregation Router (SAR) and Virtualized Service Router (VSR).

Integrated firewalls

Designed to perform stateful, in-line packet inspection to stop unsolicited traffic from breaching the many secure zones required by today's open, distributed network architectures, Nokia SR OS firewalls play a central role in Nokia's IP multi-layer network defense strategy.

Figure 10. Integrated firewalls



Nokia SR OS-based integrated firewalls sit in-line with traffic and track all sessions flowing into or out of the zone they protect. Flows solicited by legitimate users or applications pass through with rate limiting where required, while traffic not on a firewall's list of solicited flows is blocked. In addition, pinholes can be selectively enabled for trusted unsolicited traffic.

The stateful firewall supports all protocols including Transmission Control Protocol (TCP) and GPRS Tunneling Protocol (GTP) to discard packets that violate protocol rules and to neutralize the more complex attacks targeting the control, user and management planes of network functions and applications.

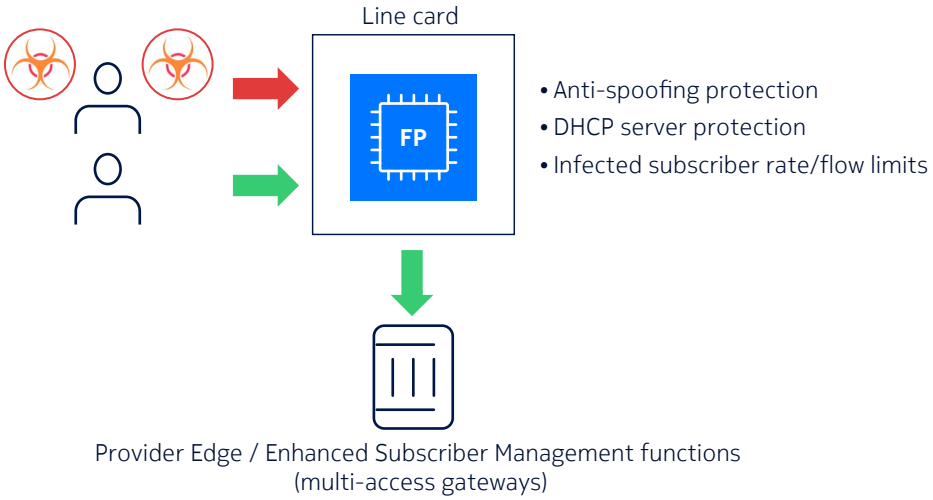
With high throughput and system modularity and scalability, Nokia SR OS firewalls are well-suited to particular points in the network, including:

- Integrated in the IPsec gateway to perform GTP and Stream Control Transmission Protocol (SCTP) checks and allow Operations, Administration and Maintenance (OAM) traffic through
- Integrated with the Multi-Access Gateway User Plane Function to perform TCP and User Datagram Protocol (UDP) traffic checks
- Integrated with peering routers on partner and roaming links to provide secure zones between a network operator and its partners

The integrated firewall function can be deployed on the 7750 SR ESA and VSR.

Enhanced subscriber management

Figure 11. Enhanced subscriber management



Attacks can also target network-resident services, such as a Broadband Network Gateway (BNG), by pretending to be valid subscribers or users. The Nokia SR OS monitors protocols such as Address Resolution Protocol (ARP) and Dynamic Host Configuration Protocol (DHCP) to identify and discard invalid requests that try to bond to the network or that seek to exhaust finite resources such as DHCP sessions.

Integrated Unicast Reverse Path Forwarding (uRPF) protection helps mitigate problems caused by the introduction of malformed or forged (spoofed) IP source addresses into the network.

As well, should a provider's subscribers and IoT devices be hijacked and turned against them, FP-equipped routers and gateways have the granularity and power to deflect and control individual subscribers with minimal impact or performance degradation.

AI-driven big data security analytics

As shorter, distributed, more sophisticated and more impactful DDoS attacks continue to ramp up, security is becoming a paramount concern across the industry.

Nokia's approach to DDoS security blends petabyte-scale big data IP analytics with the power of advanced network routers and next-generation DDoS mitigation systems to fight DDoS with unprecedented scale, efficiency and cost-efficiency.

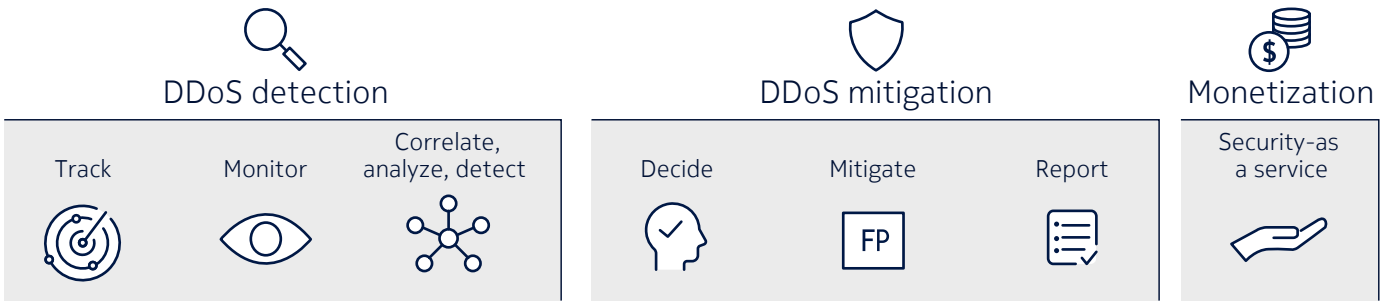
The Nokia IP network security solution combines:

- Deepfield Defender, an AI/ML-driven DDoS security platform
- Sophisticated, FP processor-based Nokia routers or 7750 Defender Mitigation System
- Deepfield Secure Genome®, a patented proprietary cloud-based data feed that tracks the internet's global security context and feeds this information to Deepfield Defender in real time

These capabilities empower providers to improve protection while lowering costs, removing human errors and improving the overall scale of security and automation.

Nokia's advanced, high-performance DDoS security solution detects all types of DDoS quickly and accurately and drives agile, network-based mitigation on the existing Nokia routers or a dedicated mitigation platform, with minimal or no impact on customer traffic. This advanced DDoS security solution allows network owners and operators to stay ahead of the latest generation of threats, scaling protection and adding security-enhanced service offerings to enterprises, especially those operating in critical industry segments.

Figure 12. Stopping DDoS in seconds



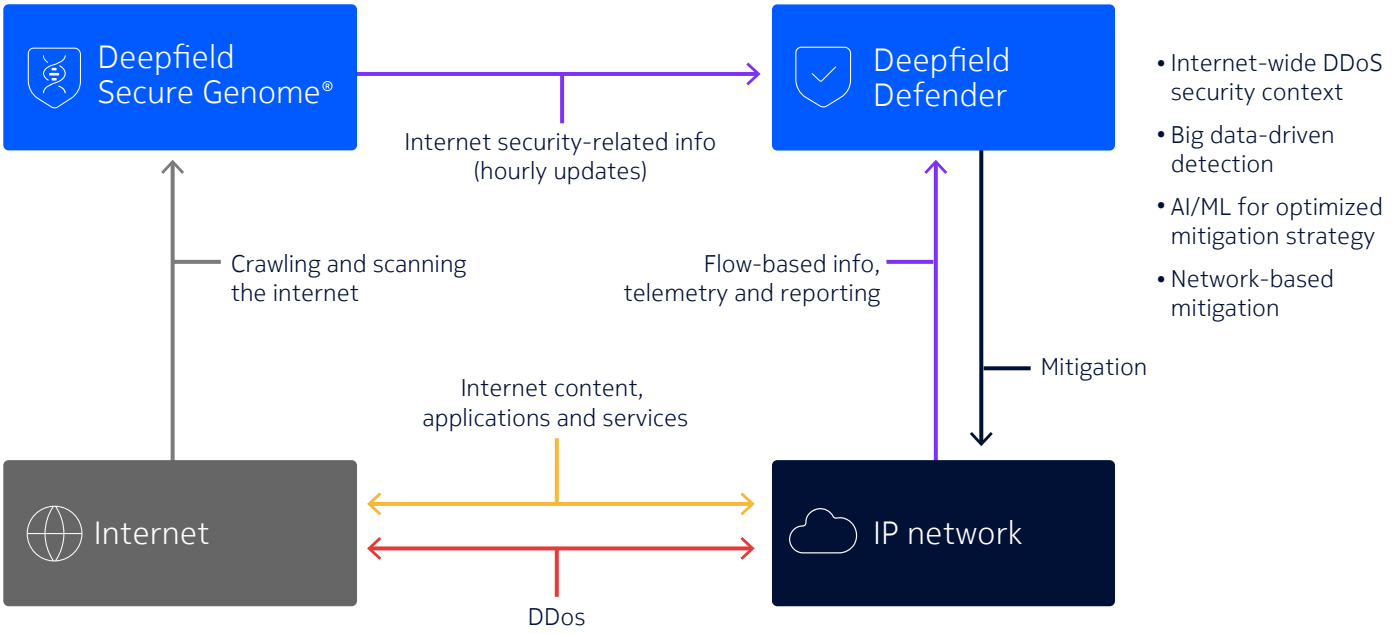
AI-driven big data analytics combined with advanced IP network capabilities

DDoS attackers now operate industrial-scale botnets with valid IP addresses and legitimate traffic characteristics, making traditional detection methods ineffective. To counter these threats, Nokia Deepfield Defender uses AI and ML to deliver adaptive, automated and extensible DDoS protection, such as:

- **DDoS detection**: Called a "security map of the internet," Nokia's unique cloud-based global database, Deepfield Secure Genome® identifies potential threats in real time, with hourly updates and visibility into over 5 billion IPv4 and IPv6 addresses. Flow-based telemetry information from the IP network and sampled port mirroring (SPM) are correlated with the information from Secure Genome to deliver DDoS detection within seconds and with much improved accuracy.

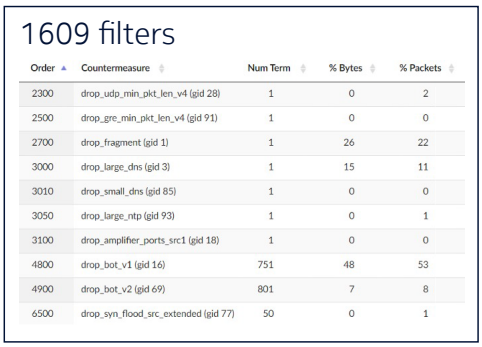
- **DDoS mitigation**: Deepfield Defender considers the availability of the network's actual mitigation capabilities (mitigation instruments and scrubbing systems) and, using AI-based decision trees and deep learning models, creates in seconds the most optimal strategy to combat a DDoS attack or many concurrent DDoS attacks. Precise filtering and mitigation strategies can be applied to mitigation systems such as programmable routers like the Nokia FP4/FP5-based IP routers, or Nokia's dedicated next-generation scrubber, 7750 Defender Mitigation System, which provides massive-scale IP filtering and application-layer attack mitigation.
- **Security monetization**: Service providers can also create new revenue streams while optimizing their network security by providing premium DDoS protection services to their customers. A DDoS Protection as a Service (DDoS-PaaS) option allows for customizable, tiered security services while offering detailed insights and reporting to premium customers via tailored user interfaces.

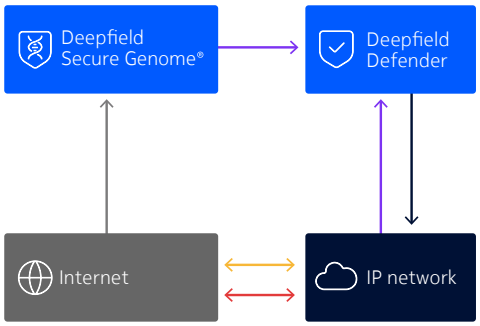
Figure 13. DDoS security solution

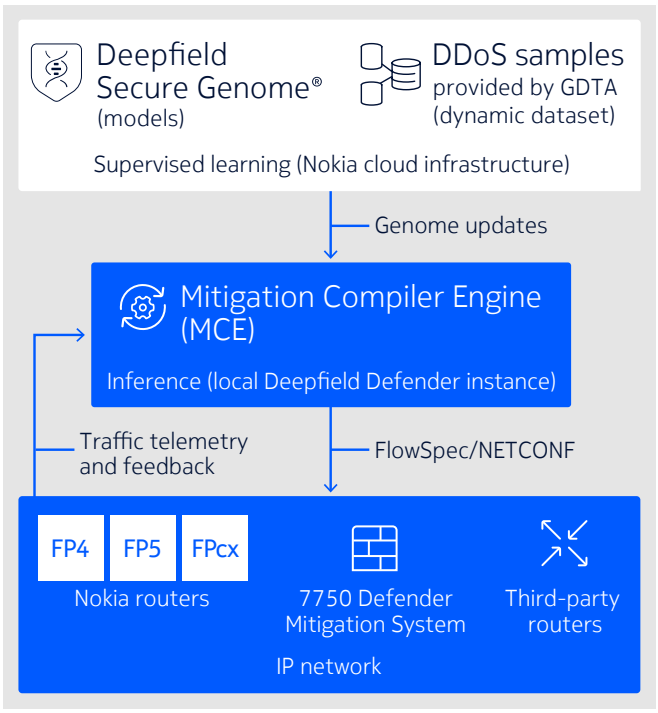


Leveraging the rich telemetry and programmability of the IP network itself, the Deepfield Defender-based DDoS security solution outperforms legacy (appliance- or DPI-based) approaches, resulting in improved accuracy of DDoS detection (with fewer false positives) and more rapid, scalable and cost-efficient DDoS mitigation.

Figure 14. Network-optimized mitigation







Mitigation Compiler Engine (MCE)

- Inference from Deepfield Secure Genome ML models (trained on 10K+ real-world attack samples)
- Generates optimized mitigation strategies for complex DDoS attacks
- Effective against known DDoS and emerging vectors

Deepfield Defender uses AI/ML technology to detect and mitigate DDoS attacks with high accuracy and speed, while also providing customizable security policies and real-time mitigation capabilities.

- **ML algorithms** are trained on a large dataset of DDoS attacks to identify patterns and anomalies in network traffic. The ML models are used to detect and classify DDoS attacks in real time.
- **DDoS samples** from the Deepfield DDoS Library, which contains more than 10,000 real-world samples, are used to train our detection models. This optimizes the false positive/negative efficiency of DDoS detection and improves mitigation as fewer filters are required to neutralize DDoS attacks.
- **Deepfield Model Language** (DML) uses complex security policies defined and implemented across a wide range of DDoS filtering appliances and NETCONF/BGP Flowspec/Remotely Triggered Black Hole (RTBH) routers. Filters and mitigation policies can be created and tailored to specific network environments.
- **Deepfield Secure Genome® data feed** is used to build allow-lists and block-lists to filter out malicious traffic.
- **Supervised learning** of ML models on a large dataset of labeled DDoS attacks allows the system to learn from known attacks and improve detection accuracy.
- **Unsupervised learning** is used to identify unknown or zero-day attacks, empowering the system to detect anomalies in network traffic that may previously have been missed.

Summary

With the world's networks and data more at risk than ever before, a comprehensive strategy is required. Adopting Nokia's multi-layer embedded approach to IP network security can protect both IP network infrastructure and content, ensuring:

- Cost-effective protection for all network elements, all customers and all data traversing a mission-critical network.
- Trusted systems designed with security at scale.
- Trusted communications with high IP network/service performance and quantum-safe dataflow confidentiality, integrity and availability.
- Security intelligence and automation for AI-driven big data security analytics as well as quantum-safe key generation, distribution and orchestration.

By prioritizing security in the design and support of the many systems the network comprises, the Nokia IP network security approach ensures network operators maintain a digital communications infrastructure that is secure, reliable and trustworthy for consumers, enterprises, mission critical infrastructure builders and Communications Service Providers.

Abbreviations

AAA	Authentication, Authorization and Accounting
ARP	Address Resolution Protocol
AI	Artificial Intelligence
BGP	Border Gateway Protocol
BNG	Broadband network gateway
CERT	Computer Emergency Response Team
CRQC	Cryptographically relevant quantum computer
DDoS	Distributed denial of service
DDoS-PaaS	DDoS Protection as a Service
DHCP	Dynamic Host Configuration Protocol
ESA	Extended Services Appliance
FIPS	Federal Information Processing Standards
GTP	GPRS Tunneling Protocol
IS-IS	Intermediate System to Intermediate System
ICMP	Internet Control Message Protocol
IKE	Internet Key Exchange
ML	Machine Learning
MKA	MACsec Key Agreement

NIAP	National Information Assurance Partnership
NETCONF	Network Configuration Protocol
NOS	Network Operating System
OSPF	Open Shortest Path First
OAM	Operations, Administration and Maintenance
PQC	Post-quantum cryptography
QSN	Quantum-Safe Networks
RTBH	Remotely Triggered Black Hole
SPM	Sampled port mirroring
SDL	Secure Development Lifecycle
SCTP	Stream Control Transmission Protocol
SZTP	Secure Zero Trust Provisioning
TTL	Time-to-live
TCP	Transmission Control Protocol
TCG	Trusted Computing Group
TPM	Trusted Platform Module
RPF	Reverse Path Forwarding
uRPF	Unicast Reverse Path Forwarding
UDP	User Datagram Protocol
VSR	Virtual Service Router

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, which is celebrating 100 years of innovation.

With truly open architectures that seamlessly integrate into any ecosystem, our high-performance networks create new opportunities for monetization and scale. 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: (June) CID214929