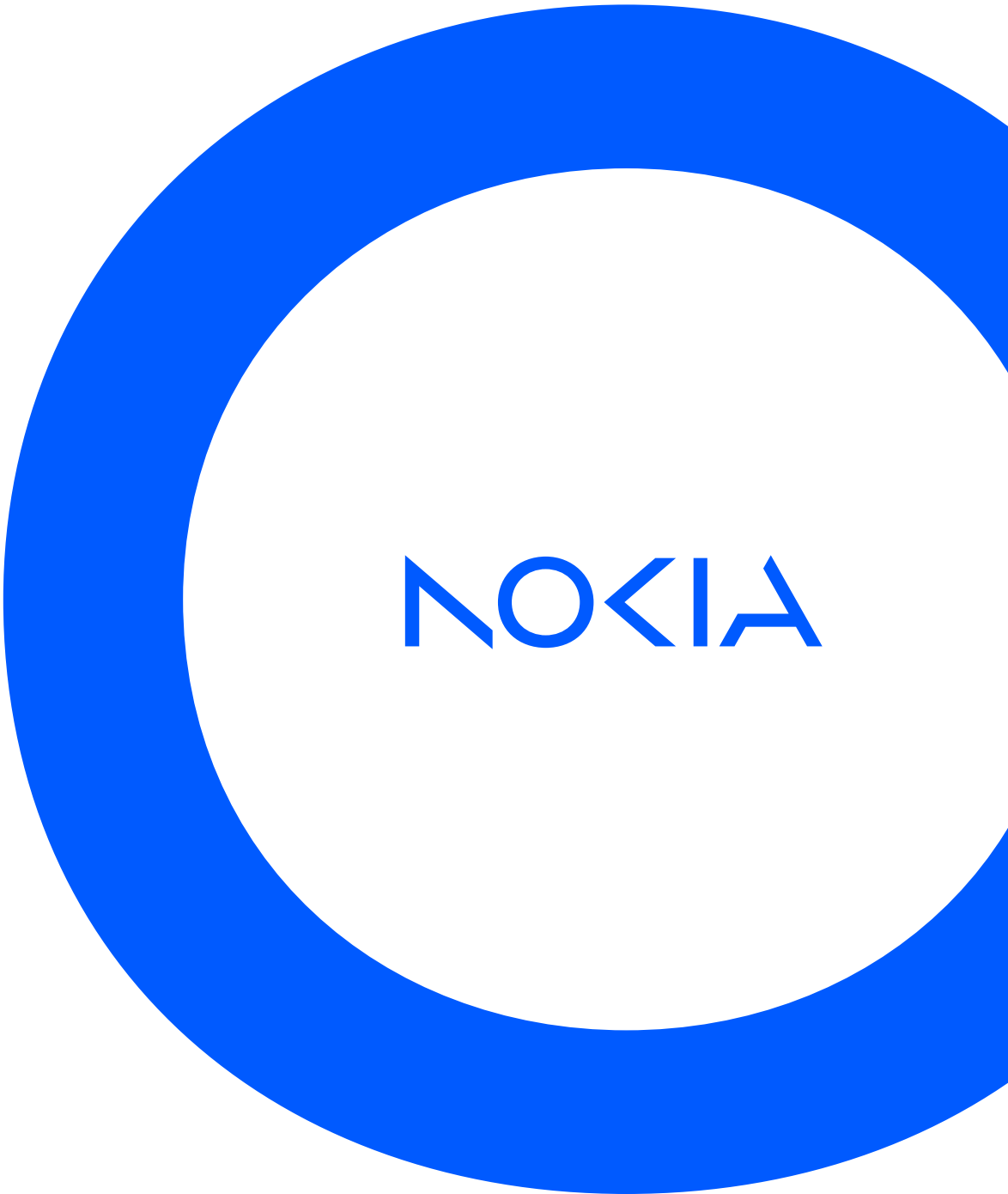
Nokia Secure IP Networks

A multilayer, embedded approach to IP network security

Application note



Abstract

To support new, mission-critical applications associated with cloud architectures, 5G and Industry 4.0, IP networks must be trusted to provide guaranteed high-performance and secure connectivity. Achieving this is increasingly difficult due to growing threats from network-level attacks and security breaches and to the limited scalability, functionality and cost-effectiveness of IP network security solutions based on appliances and servers.

As a service provider, you know you need to find new approaches to address the escalating threat landscape before it impacts your brand reputation and profitability.

The solution lies in making IP network security just like packet forwarding — a high-performance, highly scalable capability of the IP network itself. Nokia has pioneered this approach by embedding security into every layer of the IP network infrastructure. IP silicon innovation, a self-defending network operating system (netOS) and multiple security tools work together to provide:

- Universal, cost-effective protection for all network elements, all customers and all data traversing a service provider's network.
- Predictably high IP network/service performance and dataflow confidentiality/integrity
- Faster identification and mitigation of distributed denial of service (DDoS) attacks with minimal false positives and false negatives

This application note explains how Nokia's IP network security architecture enables you to deliver on these promises.

Contents

Introduction

The internet has evolved from a best-effort IP network for email and browsing to a network at the center of a digital revolution in the way we live, work and play. Every sector — from industry and commerce to entertainment and energy — now relies on IP networks for connectivity, and everyone expects real-time responsiveness, secure connectivity and 100 percent reliability in exchange for their fees.

This new reality has never been more apparent than during the COVID-19 pandemic, when we all became dependent (to some degree) on IP networks to keep us going. As critical infrastructure and services moved online, our tolerance for security vulnerabilities and variable service quality all but disappeared.

But as IP networks and the data flows they carried became increasingly important in our daily lives, they also became increasingly attractive to attackers wanting to wreak havoc of a political or economic nature, or for financial gain.

DDoS and its impact on mission critical IP networks

Distributed denial of service (DDoS) traffic grew 40 percent during just the first month of the pandemic, and peak daily DDoS traffic rates more than doubled from February to September of 2020, to reach terabit speeds[1]. Nokia Deepfield research suggests volumetric DDoS attack rates could reach the 15 Tb/s range over the next few years as DDoS becomes the fastest growing category of traffic — faster than even gaming or video.

New devices, including billions of internet of things (IoT) devices and high-bandwidth servers, are hijacked and used in conjunction with reflection, amplification and carpet-bombing techniques to launch increasingly sophisticated attacks that reduce service quality and service access. New short-burst DDoS attack vectors cause disruptions that are far more difficult to identify and mitigate than previous attacks.

Service providers are also impacted by DDoS traffic that does not target them specifically but flows through their networks to reach their customers. This comes at a time when they are already facing the challenges of engineering mission-critical networks dominated by bursty traffic coming from cloud and enterprise services. Random surges of DDoS traffic make ensuring consistent service quality much more difficult.

The confidentiality and integrity of customer data flows

At the same time, service providers are embracing third-party transport options, open network architectures and globalization. This has the potential to make their IP networks more porous and vulnerable to attacks that can impact the confidentiality and integrity of customer data flows.

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 reputation. According to IBM[2], it takes 280 days for most enterprise victims of a breach to discover and contain it, with most small business going bankrupt within six months. Government is concerned at the growing disruption of critical infrastructure and services, seemingly by state players. HP[3]-sponsored research estimates that cybercrime activity conducted by nation-state players has increased two-fold from 2017-2020. In the first half of 2021 alone, breaches led to 25 percent of U.S. beef operations, gas supply to most of the eastern U.S. seaboard shut down, a major financial company being locked out of their network and tampering with the public water supply at a major treatment plant.

1 Nokia Deepfield Network Intelligence Report, Executive Summary, Page 4.

2 Cost of a Data Breach Report, IBM, 2021.

3 Nation States, Cyberconflict and the Web of Profit, Dr. Michael McGuire, University of Surrey, 2021.

Service providers 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 the reputations of both provider and customer.

The integrity of IP networks themselves

Service providers must also contend with the integrity and confidentiality of their own data flows. According to OMDIA[4], approximately one quarter of all servers sold by 2024 will go to edge data centers, which translates to more service provider data in flight, and greater vulnerability to breach.

Many of the desired benefits of cloudification and architectural evolution such as control plane and user plane separation (CUPS) can also increase the security risks for IP networks. Network and service functions can now be disaggregated, distributed and deployed anywhere they need to go to optimize capacity, latency, reliability and service experience. This open, disaggregated and distributed design introduces many new surfaces that attackers can exploit. Any potential breaches can quickly become service-impacting events.

Attackers can also exploit weaknesses in network operating systems and in a network's control, data and management planes to disrupt service quality or gain unlawful entry.

Issues with current IP network security models

Today's IP network security models are based on specialized, limited-scale appliances for DDoS scrubbing, encryption and firewalls that solve only a fraction of these problems. They lack the cost-effective scalability required for broad deployment, and because of their overlay design, are unable to address most vulnerabilities buried in network operating systems and silicon. They focus on protecting a small portion of the network or on attacks targeting the most valuable and demanding customers.

Given the scale of what must be protected, the expansion of what is considered mission-critical and the escalating impact of attacks on OPEX and customer churn, service providers know they need to find a better way to address the growing threat landscape before it impacts their brand and profitability.

IP network security must come from the network itself

The solution lies in harnessing IP network infrastructure to play a larger role in protecting the network, its services and therefore customers' service experience. To provide the scalability and functionality required to protect large, mission-critical networks, IP network security must become like packet forwarding: a high-performance, highly scalable function of routers and switches.

Security must be built into the DNA of each and every layer of the IP network.

The IP silicon must be designed to sustain bursty or constant bit-rate attacks without service disruptions. It must deliver the filtering speed, precision and scale required to be a highly precise DDoS attack sensor and mitigation device, and it must provide built-in encryption to protect all the 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 purpose built to be secure, robust and work with the IP silicon to mitigate all attacks that attempt to consume its resources, hijack its processes or sabotage its control plane.

4 The profile of organizations deploying edge is more traditional than you might think, OMDIA, 17 Dec 2020.

This protective shield of purpose-built silicon and netOS becomes an ideal base on which to layer additional security tools and functions such as DDoS defense, encryption, firewalls and carrier-grade network address translation (NAT).

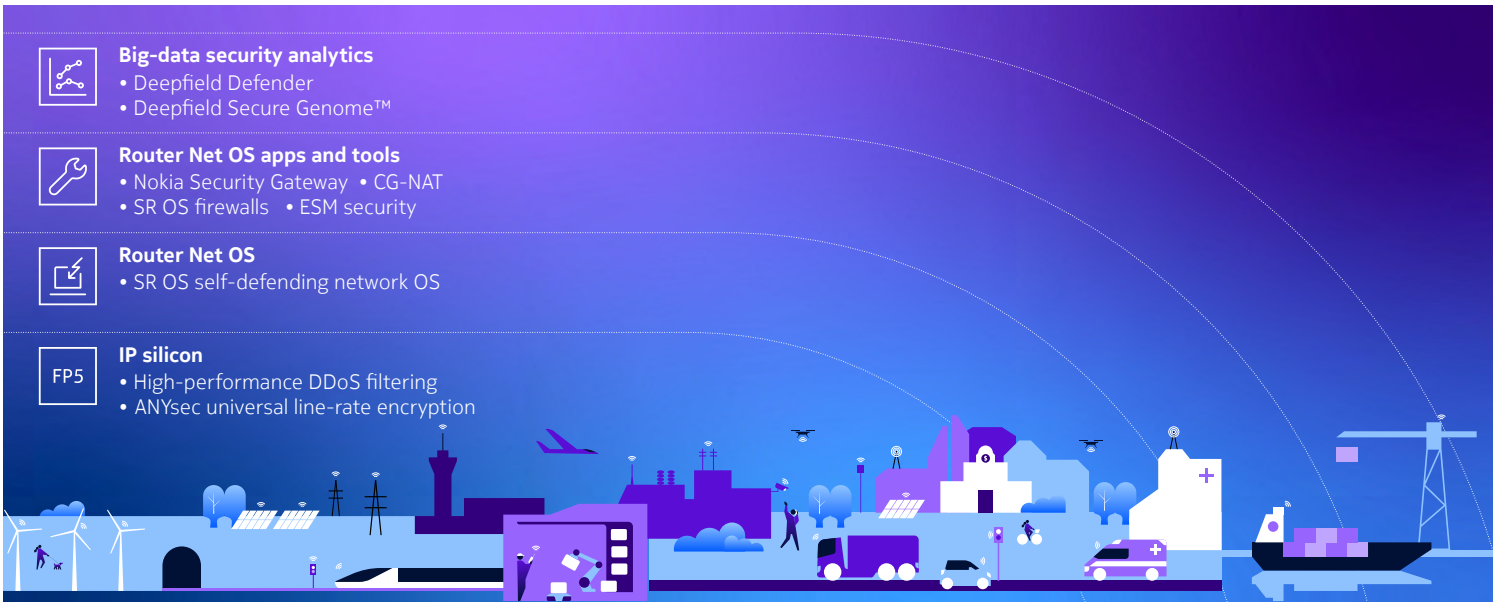
A big-data security analytics component contains the broad situational intelligence and multidimensional analytics required to detect today's sophisticated DDoS attacks with minimal false positives and false negatives, and it automates the network's response to attacks to minimize the impact on a service provider and its subscribers.

Nokia IP network security

Nokia has been the first to deliver a multilayer, embedded approach to IP network security (see Figure 1) that includes:

- FP4/FP5 silicon-based protection in the Nokia 7750 Service Router (SR) and the Nokia 7950 Extensible Routing System (XRS)
- Nokia Service Router Operating System (SR OS), a self-defending netOS
- IPsec, firewall, NAT and subscriber security tools and functions
- Nokia Deepfield Defender multidimensional intelligence, analytics and automation.

Figure 1. Nokia IP network security architecture



This unique, network-embedded approach to IP network security provides service providers with:

- Universal, cost-effective protection for all network elements, all customers and all data traversing a service provider's network.
- Predictably high IP network/service performance and dataflow confidentiality/integrity
- Faster identification and mitigation of DDoS attacks with minimal false positives and false negatives

The remainder of this application note summarizes the roles and functions of each layer in the Nokia IP network security framework.

FP4/FP5-based DDoS filtering: Industry-leading scale, precision and speed

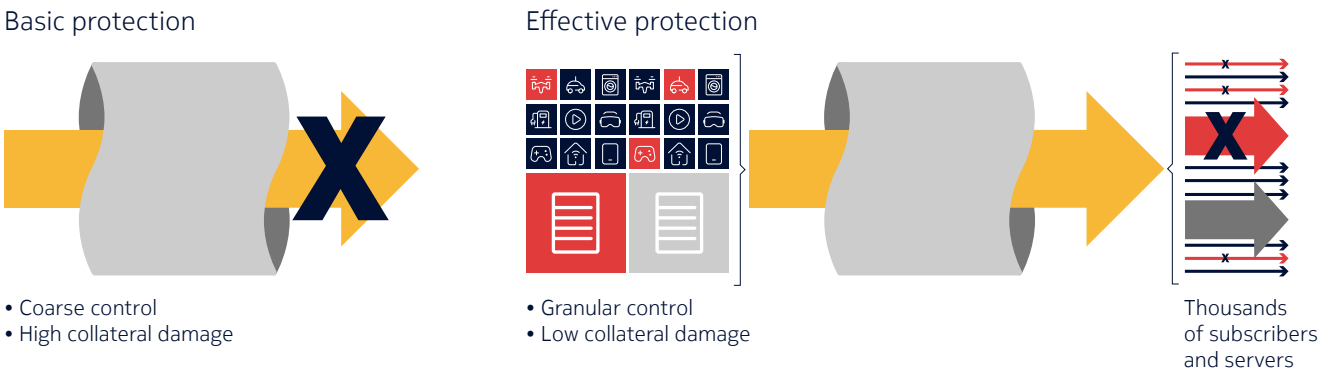
IP network silicon designed for IP network security must provide not just basic protection, but effective protection.

Basic protection is brute force. When traffic from a specific peering partner or tunnel creates a problem, the security device simply drops traffic from the offending partner or tunnel. Unfortunately, this can make the attack far more effective than the attacker could have ever wished for because valid traffic is swept away along with attack traffic.

Effective protection means having the ability to distinguish and control good and bad with great precision, minimizing collateral damage.

As shown in Figure 2, it means being able to see the hijacked server and IoT devices responsible for the attack and being able to stop or rate limit traffic from these sources without impacting any other traffic sharing that tunnel.

Figure 2. Basic protection vs. effective protection



To accomplish this task requires monitoring and controlling tens of thousands of sources, which in turn requires tens of thousands of filters and queues that can be set up without impacting performance, even when links are fully saturated.

This is exactly what the FP4/FP5-equipped 7750 SR and the 7950 XRS deliver to protect the network's user and control planes. Each of these routers has the scalability and performance required to be a highly precise attack sensor and mitigation element without compromising other services running on the same router or gateway.

Each FP4/FP5 complex on a line card can handle bidirectional traffic at wire rate with industry leading filter scale. These filters, called access control lists (ACLs), perform traditional IP header inspection as well as signature-based inspection to identify and mitigate more sophisticated attacks.

The speed of ACL deployment is just as important as ACL density in minimizing impacts. Typical router platforms can take minutes or hours to deploy tens of thousands of ACLs. By contrast, ACLs can be configured on a single FP4/FP5 in a 7750 SR/7950 XRS in mere seconds to screen or mitigate an amplified SYN attack.

FP5-based universal line rate encryption: ANYsec

Service providers can help ensure the confidentiality and integrity of all dataflows traversing their networks through network level encryption. A universal encryption technology optimized for service provider environments must have the following attributes:

- **Low latency:** to support time sensitive applications and services
- **Simple, low cost:** to enable mass-scale deployment
- **Flexibility:** to support all service provider network protocols
- **Highly secure:** based on stringent 256-bit encryption standards

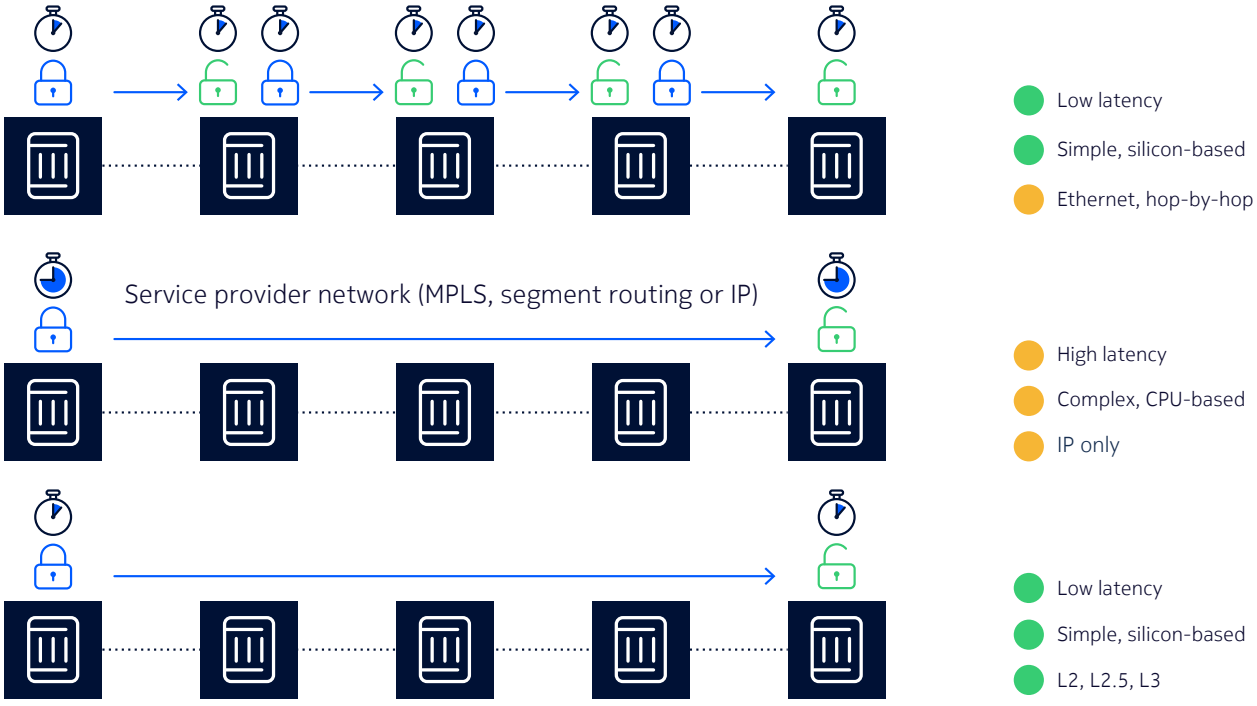
Up to now, service providers have tried to fulfill this role with limited deployments of MACsec, IPsec or proprietary technologies. None of them have fulfilled more than one or two of the requirements listed above.

MACsec is silicon-based, allowing it to deliver the nano-second latencies required for time sensitive networking. Because it is Ethernet-based, it must be implemented hop-by-hop in MPLS, segment routing or IP networks. This means frames must be un-encrypted at every hop, increasing security risks and operational complexity and adding to overall latency.

IPsec was designed for single hop encryption across IP networks. But it is complex and must be implemented in central processing unit (CPU) platforms, significantly increasing costs. This also means IPsec latencies are much higher, making IPsec unsuitable for time-sensitive networking. Finally, neither option supports native encryption of individually engineered tunnels, flows and slices based on MPLS and segment routing.

To address these gaps, Nokia has delivered ANYsec encryption on the 7750 SR series of routers.

Figure 3: Comparing ANYsec with traditional network encryption options



Based on MACsec standards, ANYsec extends its capabilities beyond Ethernet and VLANs to include native encryption across MPLS, segment routing or IP networks. Service providers can leverage ANYsec to encrypt individually engineered tunnels/flows/slices at network ingress, switch or route them natively across any MPLS/segment routing network, and de-encrypt them when the tunnel/flow/slice is terminated on the other side.

To provide the latency, performances and universal network capability required, ANYsec is implemented in silicon within the FP5 chipset. Best-of-breed network technology is fused with best-of-breed encryption to make secure networking (just like packet forwarding) a high-performance, universal capability of the network itself.

ANYsec provides service providers 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 advance planning, service providers can flip a switch to turn on encryption whenever and wherever it is required regardless of the service or network transport being used. 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.

Nokia SR OS: A self-defending netOS

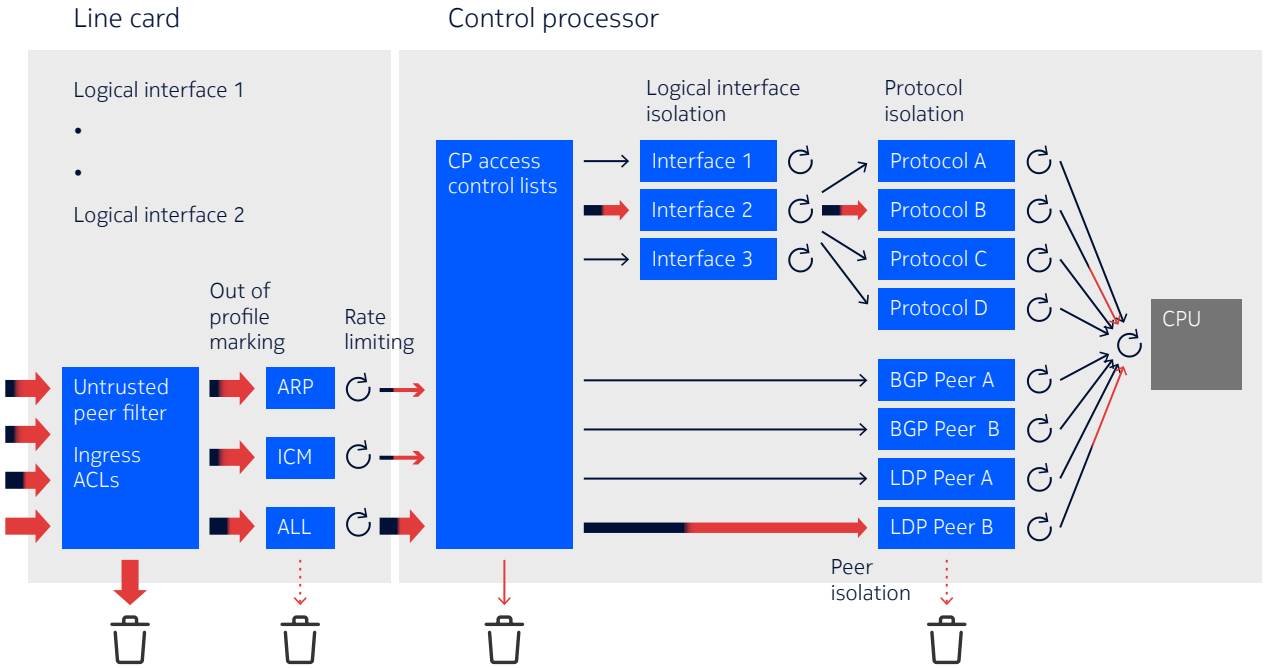
Every feature in Nokia's IP network operating system, the SR OS, undergoes rigorous testing with special emphasis on security capabilities to eliminate the potential for breaches. Vulnerabilities are identified and addressed on multiple levels.

Automated source code inspection and static code analysis tools look for errors that can lead to compromising situations. External agencies examine object code from the outside in, looking for vulnerabilities they can exploit. The development process itself, from coding to the build process to software delivery, is based on security best practices that earn our products accreditation from key security agencies.

The Nokia SR OS also leverages FP4/FP5 complexes on the 7750 SR/7950 XRS control process card and all ingress line cards to filter out attacks targeting the control plane. This unique capability prevents the central CPU from becoming overwhelmed, which would impact control plane performance. This capability also frees the CPU to support other SR OS security capabilities, such as out-of-band management, role-based access control and login protection.

This silicon-assisted control plane defense is shown in Figure 4. Blue represents FP4/FP5 elements in the ingress line card and in the control processor. The gray CPU on the control processor is where the routing control plane resides. Traffic entering the line card on the left is mostly red, indicating there is a fair amount of malicious traffic attempting to attack the control plane.

Figure 4. SR OS and FP4/FP5 protection of the routing control plane



The SR OS begins its control-plane defense on a 7750 SR/7950 XRS by using FP4/FP5 hardware filters to identify and discard traffic from untrusted peers or packets identified as part of an ongoing attack. Address Resolution Protocol (ARP) and Internet Control Message Protocol (ICMP) packets commonly used in attacks are monitored. Whenever they cross a dynamic threshold, they are rate limited or marked for discard as appropriate.

By the time packets leave the line card and enter the control processer, much of the attack traffic has already been rate limited or discarded.

The FP4/FP5 silicon in the 7750 SR/7950 XRS control processor complex augments the defense process by removing malformed or protocol-violation packets that would interfere with control plane logic. Traffic is then isolated into thousands of queues that are accessed by the CPU in a scheduled fashion.

Each protocol within each virtual interface gets a queue, as does every Border Gateway Protocol (BGP) or Label Distribution Protocol (LDP) peer the control plane interacts with. This isolation ensures total fairness so that malicious players are never able to block well-behaving ones.

In Figure 4, even though malicious packets from LDP Peer B and from Protocol B/Interface 2 make up the bulk of traffic transiting to the control plane, isolation in their own queues limits them to just their one slice of CPU cycles.

The SR OS leverages FP4/FP5 to ensure that even when service providers are unaware that a massive attack against the control plane has started, the impacts to the CPU and to the thousands of control plane interactions are already controlled and minimized.

Attacks also target network-resident services, such as a broadband network gateway (BNG), by pretending they are subscribers or valid users. The SR OS monitors protocols such as 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 is used to ensure that IP addresses are who they state they are. Finally, as a provider's subscribers and IoT devices are hijacked and turned against them, FP4/FP5-equipped 7750 SR/7950 XRS routers and gateways have the granularity and power to deflect and control individual subscribers with minimal impact or performance degradation.

Nokia Network Security Gateway: High-scale IPsec tunnel termination

Nokia's Network Security Gateway (NSG) allows service providers to terminate IPsec tunnels required by radio access networks (RANs) or other network equipment to secure transport over potentially insecure IP networks. From its highly protected shell within SR OS and 7750 SR routers, the NSG is able to deliver high-performance IPsec capacity and termination. A single 7750 SR chassis can support up to 32,000 eNBs or gNBs and up to 960 GB/s of encrypted traffic.

Integration in carrier-grade network infrastructure extends high availability attributes to the NSG, including:

- Fully redundant hardware
- High availability across control modules
- Nonstop routing and services
- Load balancing across ports/tunnels/cards
- Fast convergence across multiple technologies:
  - Bidirectional forwarding detection (BFD)
  - MPLS Virtual Router Redundancy Protocol (MPLS VRRP)
  - Interior Gateway Protocol (IGP)
  - Border Gateway Protocol (BGP)

The NSG leverages multi-chassis redundancy to synchronize IPsec tunnels between two chassis so that any failover is fully transparent, and there is no need to reset connections. This improved resiliency and hitless recovery allows service providers to achieve far greater tunnel scale by eliminating the need for a 1:1 active/standby configuration of IPsec tunnels.

Deepfield Defender: Network-integrated DDoS defense

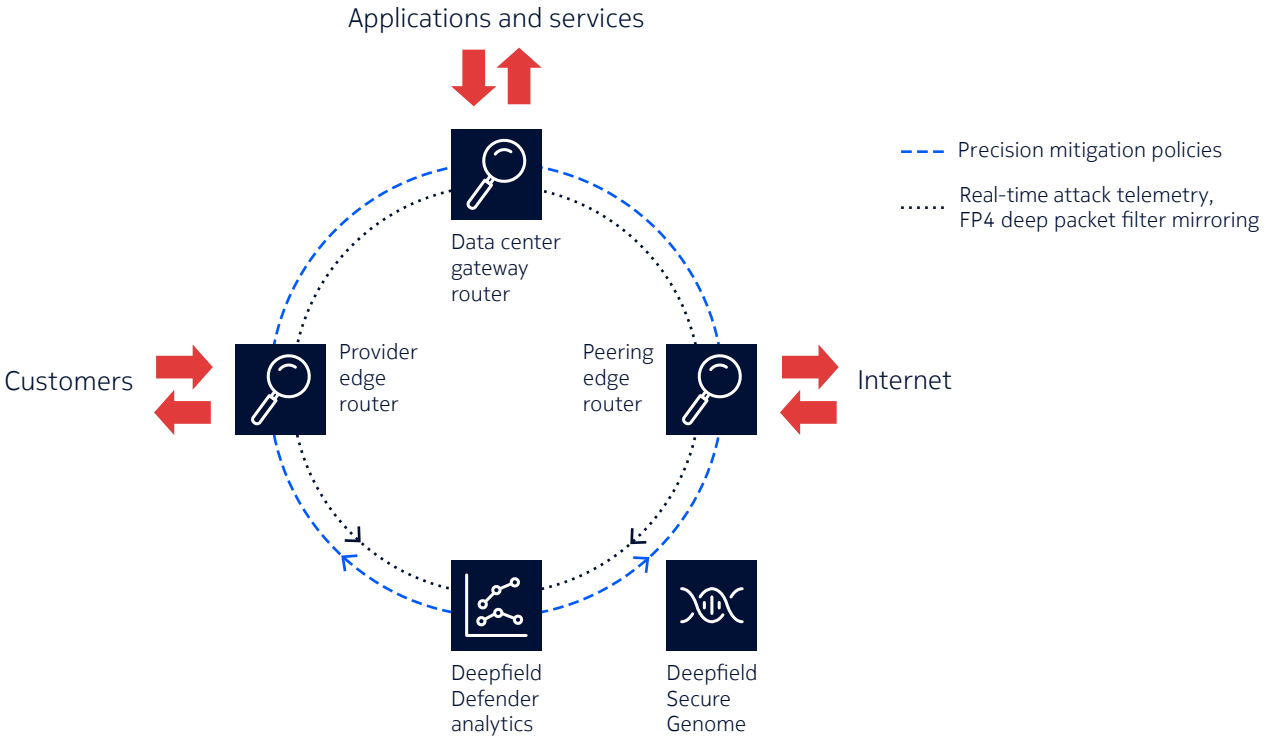
Big data analytics tools such as Nokia Deepfield Defender can be combined with FP4/FP5-equipped 7750 SR/7950 XRS routers and gateways to provide a more effective response to DDoS attacks as they increase in scale, sophistication and frequency.

In the past, peering routers were forced to send all traffic suspected of carrying volumetric or application-level DDoS to centralized scrubbing centers stacked with DDoS mitigation appliances. Security analysts did their best to clean suspicious traffic through manual analysis, but this came at considerable cost in DDoS appliance licenses and backhaul bandwidth. Manual analysis was also prone to false positives and false negatives.

Nokia Deepfield changes this model with unique situational intelligence and automation and by leveraging the network infrastructure itself to identify and mitigate the volumetric attacks that make up almost all DDoS traffic.

The process starts with Deepfield Secure Genome (see Figure 5), which provides visibility into almost all internet traffic through a patented process. Secure Genome provides a level of intelligence that was previously unavailable to service providers to help minimize false positives and negatives.

Figure 5. Deepfield Defender DDoS identification and mitigation



For example, Secure Genome can quickly identify that a suspicious surge in traffic is a file transfer from Amazon that should not be mitigated. Or Secure Genome can provide the IP addresses of an IoT device class that has been hijacked en masse, minimizing the wider impact of a more indiscriminate mitigation response.

The multidimensional analytics of Deepfield Defender combine Secure Genome with a service provider's own network data to provide an instant and precise snapshot of what is flowing through the network.

Defender tracks thousands of IP sources, setting baselines and performing additional analytics whenever thresholds are crossed to determine if the attack is real before taking action. These analytics include domain name system (DNS) analysis, IP flow analysis and packet ratio analysis.

Defender automated workflows can set up thousands of 5-tuple or signature-based filters on the rate-limiting or forwarding packets to stateful firewalls for additional analysis. Defender does all this without impact to performance.

This new breed of network-based identification/mitigation is far more cost-effective and scalable for eliminating volumetric DDoS compared to appliance-based scrubbing center models, allowing service providers to provide volumetric DDoS protection for all customers, not just a small number of the most demanding customers.

Universal customer protection allows providers to improve customer satisfaction and eliminate the impact of customer-targeted DDoS traffic on service quality and bandwidth consumption.

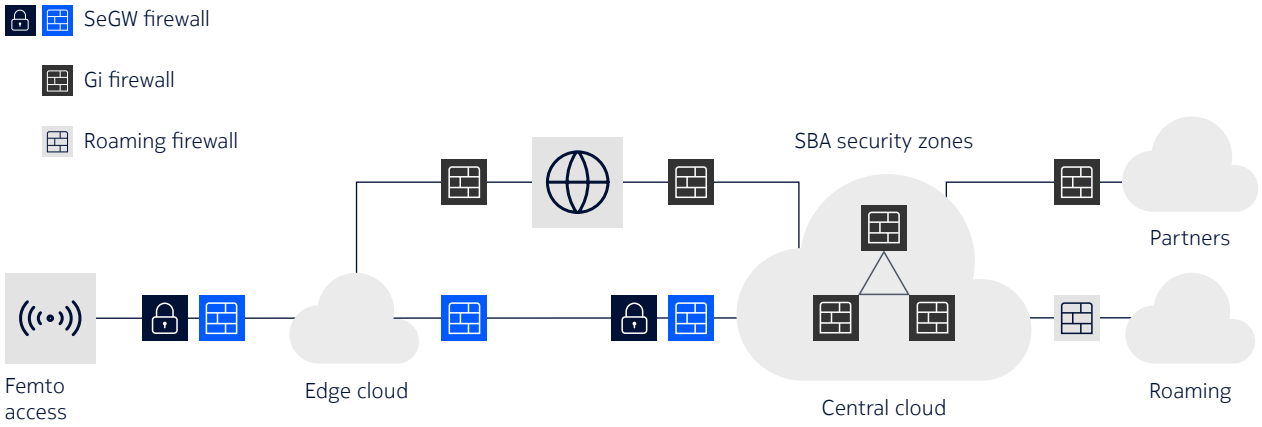
Only the 5 percent of DDoS traffic related to application-level attacks needs to be forwarded to centralized scrubbers for deeper analysis, a function that can be part of a more comprehensive security service that could be offered as part of a tiered security offering.

Firewall protection

The last line of IP network defense is the firewall, a product that does stateful, inline packet inspection to stop unsolicited traffic from breaching the many secure zones required by today's open, distributed network architectures.

Nokia SR OS-based firewalls sit in-line with traffic and keep track of all sessions flowing in or out of the zone they protect (see Figure 6). They selectively open pinholes so flows that have been solicited by legitimate users or applications can pass through while traffic not on a firewall's list of solicited flows is blocked.

Figure 6. Nokia SR OS firewall applications in 4G/5G networks



Nokia SR OS firewalls extend this capability beyond application flows, opening up pinholes for control, data and management plane flows so they can pass in and out of secure zones.

Nokia SR OS firewalls keep track of Transmission Control Protocol (TCP), GPRS Tunneling Protocol (GTP) and other protocols to discard packets that violate these protocols and to neutralize the more complex attacks targeting the control, user and management planes of network functions and applications.

Nokia SR OS firewalls can sit at many points in the network:

- Inside the edge and central cloud sites to create security zones between different functional areas to limit damage in case of breach
- Behind the IPsec gateway to perform GTP checks and let operations, administration and maintenance (OAM) traffic through
- Inside the mobile gateway (PGW/UPF/PGW-U) to provide DDoS protection against amplification attacks, anomalies attacks and bot/infected server attacks that specifically target mobile subscribers and RAN resources
- In front of partner and roaming links to provide secure zones between a service provider and its partners

Nokia SR OS firewalls leverage the self-defending and secure control plane of the SR OS to ensure they themselves do not fall victim to attacks as they defend other elements. They share the same physical platform as Nokia's IP gateways plus NAT and IP routing/forwarding functions.

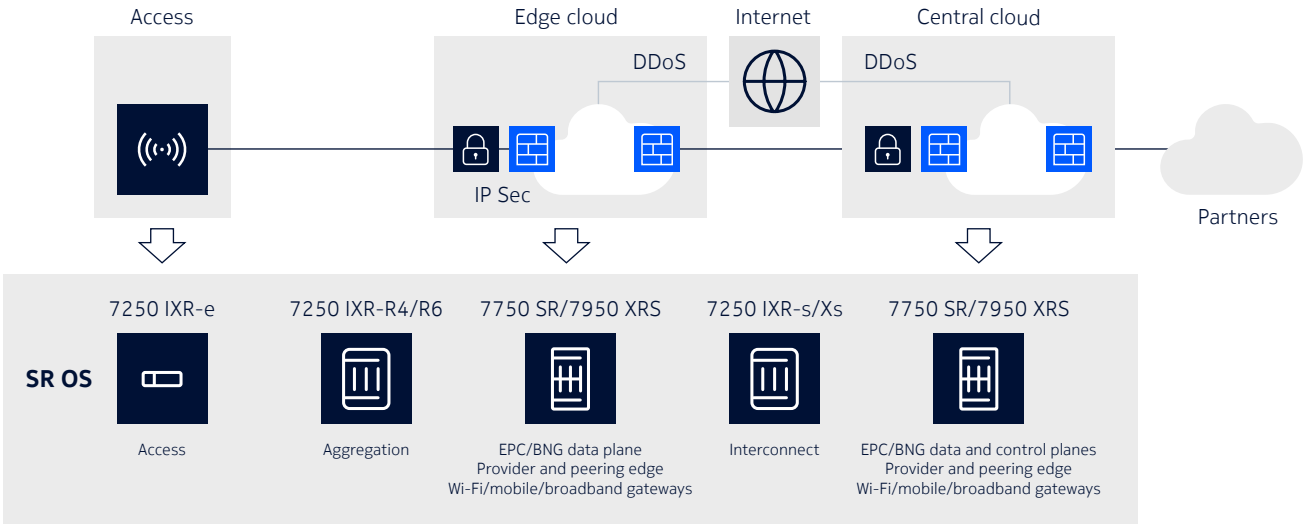
Whenever practical, this consolidation of hardware and software resources can minimize costs, optimize performance through reduced inter-virtual machine links, and minimize overhead through management as a single node.

Nokia IP network security portfolio

The Nokia IP network security portfolio contains all of the elements discussed for a secure IP network framework.

Figure 7 shows the portfolio deployed in a converged fixed/mobile network.

Figure 7. Nokia IP network security portfolio



Nokia's entire IP network portfolio leverages the protection of a common SR OS self-defending netOS.

For applications where fractional bandwidth usage or predictable traffic levels are guaranteed, such as most access, aggregation and interconnect roles, Nokia provides the 7250 Interconnect Router (IXR) family of routers. The lighter security load at these sites makes merchant PBCA network silicon and SR OS a suitable choice.

At the edge, core and peering layers, traffic levels are higher and less predictable then at the access and aggregation layers. Peering and edge sites also serve as targets or entry points for attacks levied against the service provider and its customers. Because of this greater threat exposure, higher traffic load and pivotal role they play in enabling services, IP routers and gateways at these sites require the additional protection of FP4/FP5 silicon and the 7750 SR/7950 XRS.

MACsec encryption can be deployed on single hop segments connecting 7250 IXR routers at the access and aggregation layers. ANYsec encryption can be used for network transit once traffic reaches the distributed services edge. Alternatively, the Nokia NSG can be used in mobile environments where IPsec prevails, with ANYsec encryption used for transit beyond the services edge. Nokia SR OS firewalls can be deployed throughout to stop unsolicited traffic from crossing zero-trust zones.

Conclusion

With IP networks playing an increasingly important role in our daily lives, attacks against them will continue to grow in scale, sophistication and frequency. Both network performance and the confidentiality/integrity of data that flows through them are being targeted. To earn customer trust, service providers must be able to demonstrate they can proactively avoid these attacks, or at minimum, quickly identify and eradicate them.

Success entails a fundamental shift in how service providers protect their IP networks. It requires moving away from overlay security solutions to security capabilities built into the network infrastructure itself.

Nokia has pioneered this network-centric approach to security by embedding it into the DNA of every layer of our IP network infrastructure. IP silicon innovation, a self-defending netOS, multiple security tools and big data analytics work together to protect service provider networks and customers — at massive scale and without performance compromises.

Learn more

To learn more about Nokia solutions for secure IP networks, visit the IP Network Security web page.

Abbreviations

ACL	access control list
ARP	Address Resolution Protocol
BFD	bidirectional forwarding detection
BGP	Border Gateway Protocol
BNG	broadband network gateway
CPU	central processing unit
CUPS	control plane and user plane separation
DDoS	distributed denial of service
DHCP	Dynamic Host Configuration Protocol
DNS	domain name system
GTP	GPRS Tunneling Protocol
ICMP	Internet Control Message Protocol
IGP	Interior Gateway Protocol
IoT	internet of things
IXR	(Nokia 7250) Interconnect Router
LDP	Label Distribution Protocol
MPLS VRRP	MPLS Virtual Router Redundancy Protocol

NAT	network address translation
netOS	network operating system
NSG	(Nokia) Network Security Gateway
OAM	operations, administration and maintenance
RAN	radio access network
SR	(Nokia 7750) Service Router
SR OS	(Nokia) Service Router Operating System
TCP	Transmission Control Protocol
uRPF	unicast reverse path forwarding
XRS	(Nokia 7950) Extensible Routing System

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

Document code: 557002 (May) CID210495