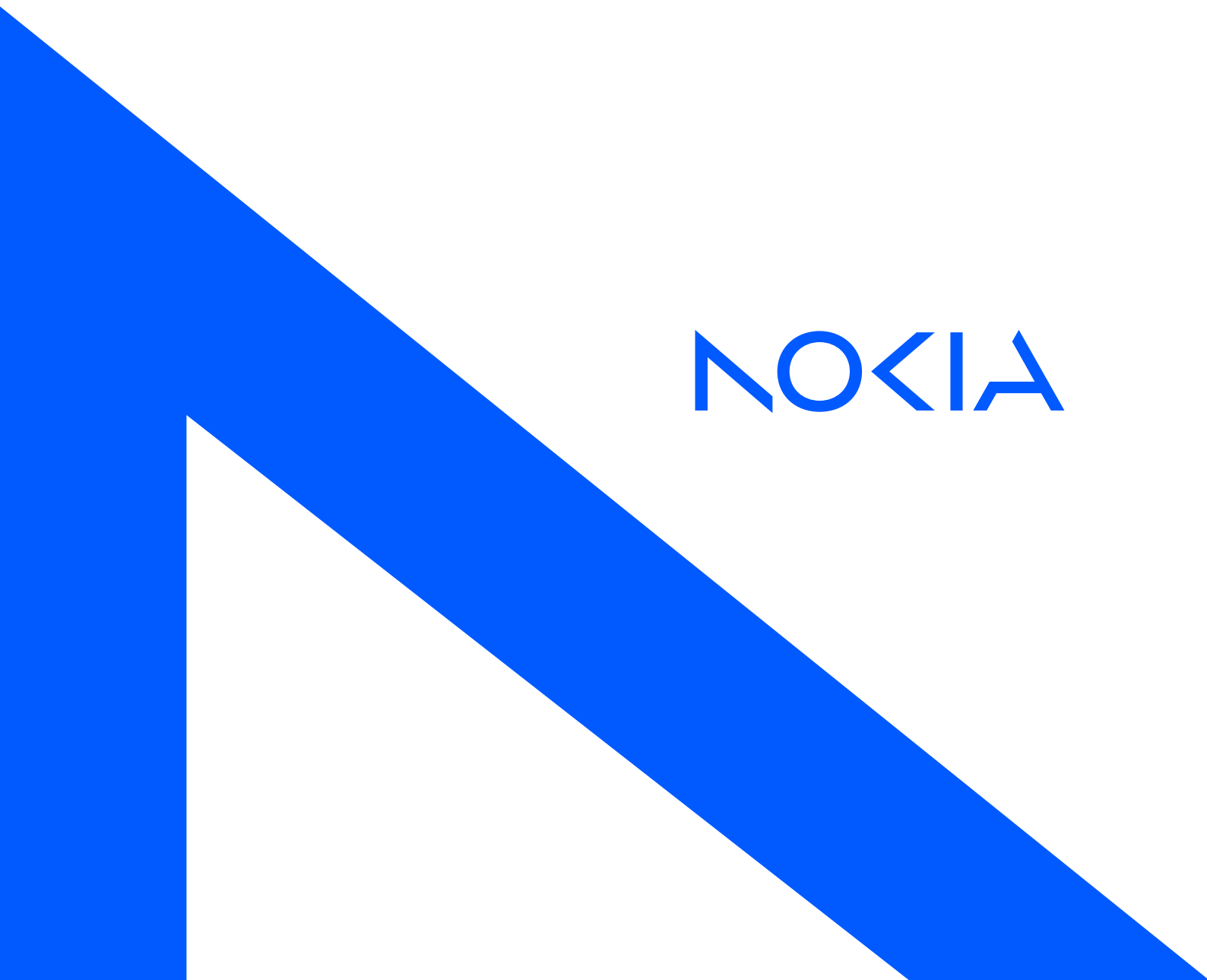
ANYsec universal line-rate encryption for communications service providers

Application note



Abstract

As the economic and political fallout from data breaches continues to escalate, the confidentiality and integrity of data flowing through communications service provider (CSP) networks is being increasingly scrutinized. Enterprises embracing digitalization are concerned about loss of revenue and reputation. Government is especially concerned with the growing number of attacks aimed at critical infrastructure, seemingly by nation-state players.

While many encryption options provide the basic mechanism for encrypting traffic flowing through CSP networks, none have provided the combination of low latency, simplicity and transport flexibility required for universal CSP deployment.

The silicon-based ANYsec technology in Nokia's FP5 chipset fulfills this role by extending the low latency and simplicity of MACsec to a new generation of engineered networks based on IP, MPLS and segment routing. With ANYsec, CSPs can transform any IP service into a secure IP service by turning encryption on whenever and wherever it's required — with no impact on performance.

Contents

Introduction

Data is increasingly “in flight”. As enterprise IT infrastructure becomes more distributed through multiple private data centers, distributed cloud services, or a hybrid of the two, data spends an increasing amount of time in transit over public or private networks.

At the same time, the communications service providers (CSPs) responsible for transporting these data flows are embracing open technologies, third-party transport options and globalization. All of these choices can make their networks more porous and vulnerable to attacks. The confidentiality and integrity of data in flight, or more specifically, the growing vulnerability of data flows to theft and manipulation, is a rapidly growing concern.

It’s a concern for enterprises. According to IBM[1], it takes 280 days for most enterprise victims of a breach to discover and contain it. Most small business do not survive the process, going bankrupt within six months.

It’s a growing concern for national security. HP-sponsored research[2] estimates that cybercrime activity conducted by nation-state players has increased two-fold from 2017-2020, with enterprise/industry, media and critical infrastructure making up approximately 85 percent of targets. In the first half of 2021 alone, breaches led to 25 percent of US beef operations being shut down, gas supply to most of the eastern US seaboard shut down, a major financial company being locked out of their network for two weeks, and tampering with the public water supply at a major treatment plant.

It’s a concern for CSPs looking to secure new revenue from the digitalization and network transformation of critical industries. Getting there means demonstrating their networks are impervious to man-in-the-middle attacks, and that their customers’ data flows are protected from theft or manipulation. Any breach can cause serious damage to the reputations of both provider and customer.

CSPs must also contend with integrity and confidentiality of their own data flows. According to OMDIA,[3] approximately one quarter of all servers sold by 2024 will go to edge data centers, which translates to more CSP data in flight and greater vulnerability to breach.

Encryption requirements for service provider IP networks

While many mechanisms are used to protect data flow confidentiality and integrity, the most secure and prevalent option is encryption. Most encryption happens within applications and at the transport layer or above using transport layer security (TLS). But since TLS only encrypts application layer payloads, it leaves IP and other network data exposed as the packet transits a CSP network. It also puts the security onus on the application developer and the user to protect the data in flight. Customers work around this by configuring and deploying specialized encryption equipment at all their sites, but this entails significant and on-going operational and capital costs, and it limits the kinds of CSP services they can leverage.

1 Cost of a Data Breach Report, IBM, 2021

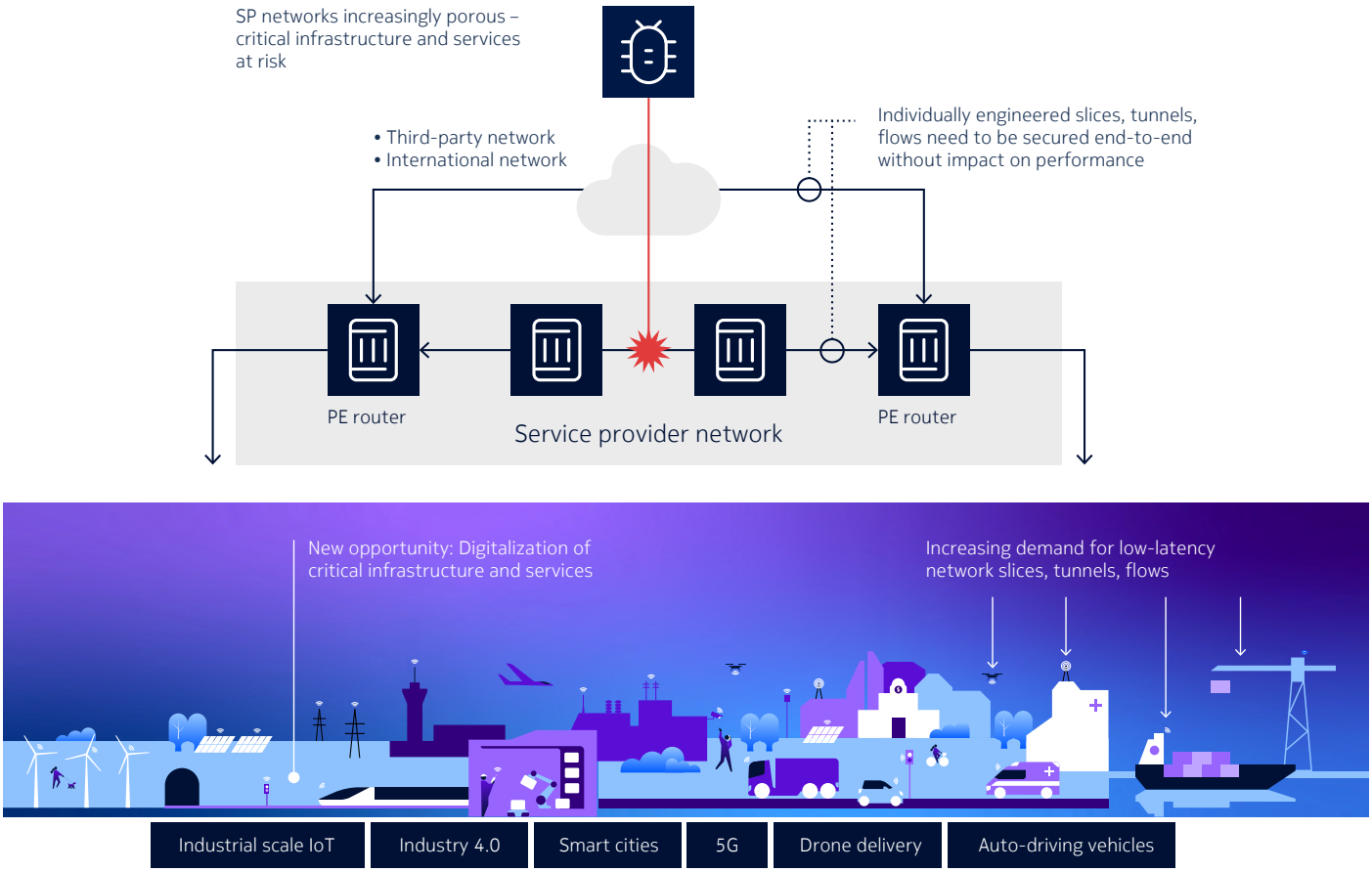
2 Nation States, Cyberconflict and the Web of Profit, Dr. Michael McGuire, University of Surrey, 2021.

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

CSPs can help their customers resolve these issues and drive new IP service revenue for themselves by encrypting all data that transits their network. To instill customer confidence and make this a profitable venture, CSP-based encryption must have the following attributes:

- **Low latency**: Required to support the many new low-latency networked applications and services that are in integral part of Industry 4.0, smart cities, 5G and industrial scale IoT
- **Simple, low cost**: Required to enable mass-scale deployment
- **Flexibility**: CSPs are increasingly creating individually engineered tunnels/slices/flows using segment routing and multiprotocol label switching (MPLS) to build their next generation transport infrastructure. Encryption technology designed for CSPs must be able to encrypt these flows as well as IP, Ethernet and virtual LAN (VLAN) frames/packets.
- **High security**: Based on the most stringent, 256 bit encryption standards

Figure 1. Encryption is a growing imperative for service provider networks



Traditional encryption options

Until now, CSPs have tried to provide data-flow confidentiality/integrity with limited deployments of MACsec, IPsec or proprietary technologies. None of these options have been able to fulfill more than one or two of the requirements listed above.

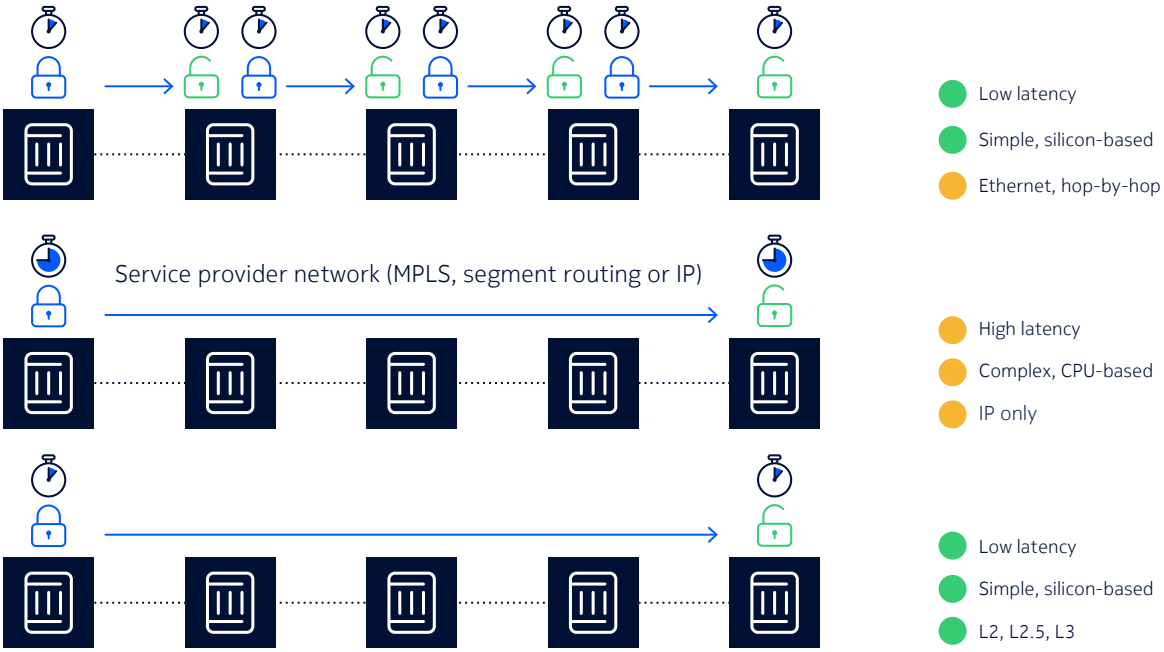
MACsec's big advantage is its simplicity. It allows for silicon-based implementations that deliver the nano-second latencies required by Industry 4.0 and smart cities applications. But MACsec was designed for point-to-point Ethernet links, which means it must be implemented hop by hop in MPLS, segment routing or IP networks. Each encryption hop must be manually configured, making deployment operationally complex. Frames must be un-encrypted at every hop to determine the next hop, thereby increasing the security risk and adding to the overall latency.

IPsec, on the other hand, was designed specifically for single hop encryption across a wide area network. IP packets are encrypted at one end of an IP network and de-encrypted at the other. But IPsec requires a more complex control plane that entails software intervention and CPU processing. It must be implemented in CPU-based platforms such as specialized appliances or specialty CPU blades that consume precious slots within routers. CPU processing also means that IPsec latencies are much higher, starting at the multi-microsecond range. This makes it unsuitable for time sensitive networking. Finally, because IPsec is IP only, it cannot natively encrypt tunnels, flows and slices engineered using MPLS and segment routing.

ANYsec universal line-rate encryption

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

Figure 2. Comparing ANYsec with traditional network encryption options



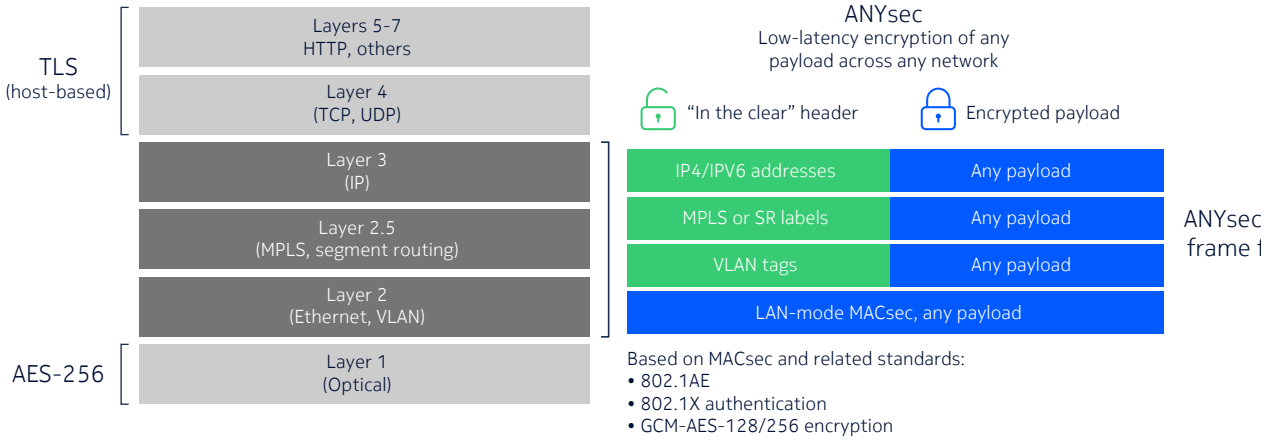
ANYsec starts with the benefits of MACsec — low latency, simplicity and highly-secure, standards-based encryption — and extends these attributes beyond Ethernet links and VLANs to include MPLS, segment routing and IP transport networks.

With ANYsec, CSPs can encrypt individually engineered tunnels/flows/slices at network ingress, switch or route them natively across IP, MPLS or segment routed networks, and de-encrypt them when the tunnel/flow/slice is terminated on the other side. Encryption is always optimized for the network payload and transport method employed.

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.

Figure 3 provides a summary of ANYsec network encryption options and packet formats. ANYsec supports traditional MACsec encryption, in both LAN and WAN modes. It extends MACsec-related standards such as 802.1AE, 802.1X authentication and GCM/AES-128/256 bit encryption to all other network payloads, and it allows any in-the-clear (unencrypted) network headers to be inserted. This includes traditional Ethernet and VLAN tags, as well as MPLS labels, segment routing labels and IP addresses — whatever is necessary to optimally transport encrypted frames/packets/flows across a network.

Figure 3. ANYsec delivers line-rate encryption for all network layers (2, 2.5 and 3) and payload



ANYsec sample use cases

ANYsec 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. 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.

Figure 4 below shows how ANYsec can be used to transform transport services, whether they are used for internal or wholesale transport, into highly secure services. Tunnels/slices that correspond to indiviswdual customers or service quality characteristics can all be encrypted from provider edge (PE) to PE without impact on performance or latency.

Figure 4. Highly-secure, low-latency transport services (internal or wholesale

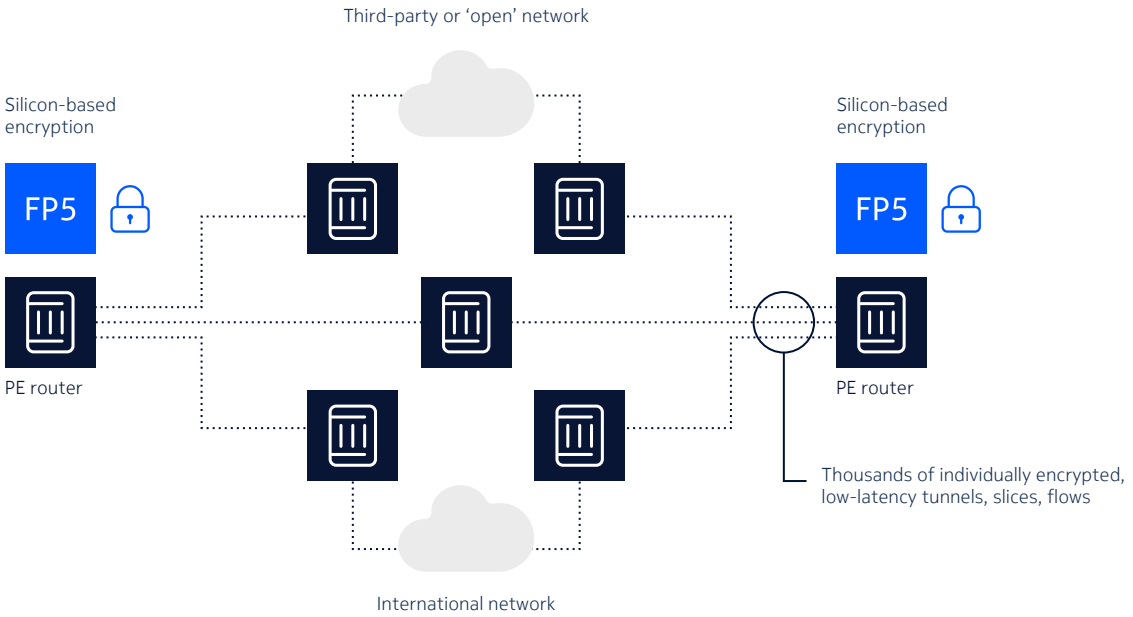
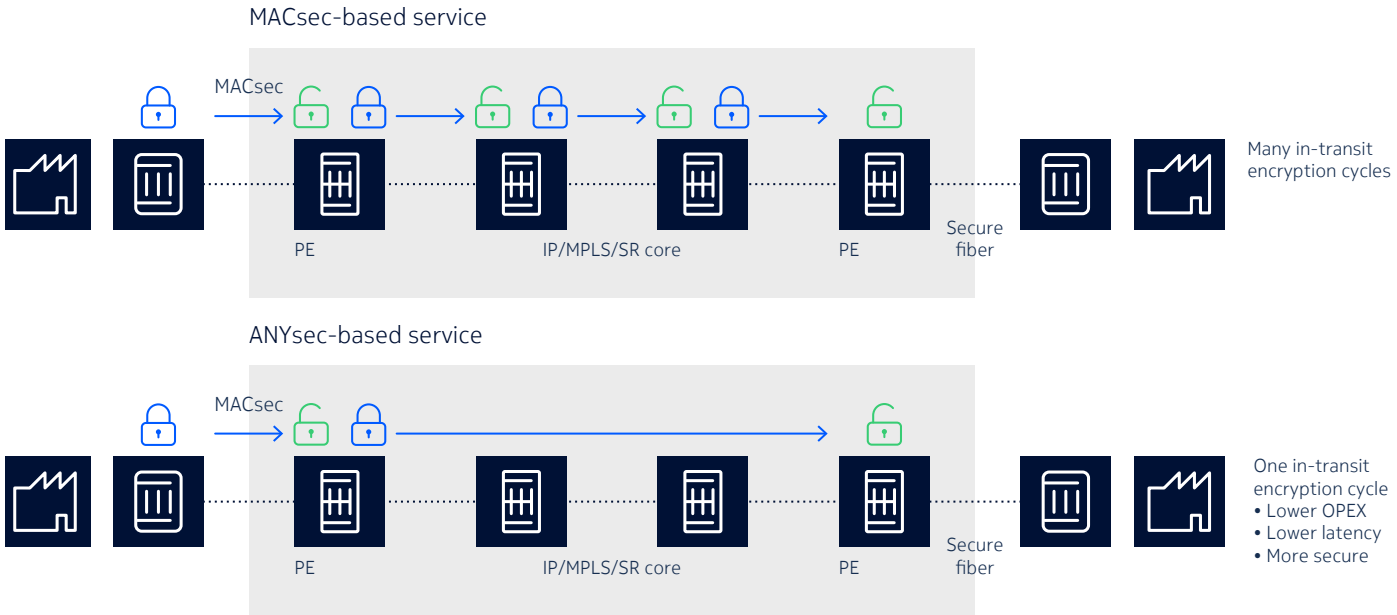


Figure 5 below shows how ANYsec can be used to transform high-performance, secure VPN services. While MACsec technically provides the low latency required, it requires hop-by-hop configuration within CSP IP/MPLS/SR networks. This is time-consuming to configure and contain, it increases security risks by requiring de-encryption at each hop, and each de-encrypt/encrypt cycle adds to the total latency of the service. With ANYsec, the CSP simply flips on encryption on all MPLS/SR tunnels associated with a particular customer, eliminating the latency, security risk and operational complexity of all the intermediary encryption hops.

Figure 5. ANYsec-based secure VPN services



Summary

At Nokia, we redefined and redesigned network security, from fundamental building blocks that we use to put networks together to our industry-first, secure IP framework that covers all aspects of IP network security. Our approach delivers cost-effective protection to all customers, services and network resources, everywhere, all the time.

Offered through the FP5 silicon in our 7750 SR series of routers, ANYsec is the universal, line-rate encryption capability in our secure IP networks framework. ANYsec extends the low latency and simplicity of MACsec to MPLS, IP and segment routed networks so that CSPs can encrypt any service, across any network, at any time without advance planning or impact on performance.

With ANYsec, CSPs can elevate network security to be a monetization tool that enables new types of security-enhanced or security-enabled services for 5G, Industry 4.0 and smart cities.

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: 557005 (May) CID210676