Securing mobile anyhaul with the Nokia IPsec Security Gateway

Application note

Abstract

This application note examines the challenges involved in properly securing the backhaul portion of a 4G network and the backhaul, midhaul and fronthaul (anyhaul) portions of a 5G network. It discusses the unique characteristics that 5G will introduce and the requirements for a layer 3 IPsec security solution. Finally, it describes how pairing the Nokia IPsec Security Gateway with the Nokia NetGuard Certificate Manager can enable mobile operators to implement a security gateway solution that delivers the industry's highest standards of compliance, capacity and throughput.

Contents

Introduction

The evolution of mobile networks to 4G/LTE brought an improvement in radio spectrum management that enabled network operators to deliver true mobile broadband services for the first time. It also enabled them to transition away from specialized mobile backhaul networking protocols and use IP everywhere. With 5G, this standardization on IP continues. It will eventually lead to the convergence of all access types—wired Ethernet, point-to-point wireless, Bluetooth, Wi-Fi, MulteFire, 4G/LTE and 5G—onto a multipurpose IP/MPLS network.

This consolidation of networks onto IP also comes with risks, especially when it comes to security. The flat IP networks that will connect everything will offer many opportunities for threat actors to exploit the underlying IP connectivity for their own nefarious purposes. Despite the significant costs associated with securing the operation of networks, state regulators and standards bodies will increasingly insist on compliance with new and evolving security regulations and standards.

5G networks will eventually connect billions, as opposed to millions, of devices and sensors. Many of these devices and sensors will be assembled from common IP networking components that are outside the control of network operators. As the number of devices and processes connecting to the cloud explodes, perimeters will expand and attack surfaces will grow.

Security for this expanding network infrastructure is a wide-ranging topic. This application note explains how the Nokia IPsec Security Gateway can be used to protect anyhaul networks for 3GPP mobile technologies, with a focus on addressing the changes that 5G brings.

Mobile anyhaul security issues

Mobile operators need to protect their networks. They must create a security perimeter for their valuable network resources while providing greater network coverage and capacity to more users and devices. Operators also need a common security model that can apply to all mobile technologies.

Operators have several different security risks to consider. Some mobile anyhaul uses third-party networks, such as wholesale carriers, which can be a source of unauthorized entry. An attacker can snoop and even manipulate traffic on transit links, including fiber. Some segments go through Wi-Fi or the internet. Insiders within the operator’s organization also account for a significant percentage of security breaches. Finally, radio access network (RAN) nodes are not always physically secure. With 5G, small cells will play a much bigger role in providing the density of coverage that is a key part of 5G’s higher performance. In contrast to a typical macrocell Evolved Node B (eNB) or Next-generation Node B (gNB), small cells will be much less physically secure.

There are several other key differences to consider with 5G, such as the addition of virtualization and decomposition in its cloud-native architecture. Whereas 4G allowed either a centralized or distributed RAN, both of which are still possible with 5G, there is now also the possibility of supporting centralized and distributed Cloud RAN. These 5G architectures enable operators to place distributed units (DUs) and centralized units (CUs) in regional cloud data centers and the edge cloud (see Figure 1). This creates new midhaul and fronthaul links that need to be secured, as discussed below.

5G also supports Control and User Plane Separation (CUPS). This allows operators to, for instance, distribute various functions to the edge of the network for multi-access edge computing (MEC). This approach is often used for time-sensitive networking because it enables the lower latencies needed to support critical machine-to-machine communications for automation. Network slicing, a key feature of 5G standalone (SA), also potentially multiplies the number of points that need to be secured with each slice created.

Mobile anyhaul security elements

This application note focuses on how to secure the connections between the core network and the eNB and gNB. The approach is to secure the anyhaul at layer 3 (L3) using a secure IP gateway, which is introduced in the 5G standard in 3GPP TS 33.501, TS 33.210 and TS 33.310. This makes the security method agnostic to the RAN.

Three essential functions are required to secure a link: **authentication, integrity** and **confidentiality**.

Authentication ensures that the sender and receiver are who they say they are by checking the authenticity of their certificates during IPsec tunnel setup. This allows entities to build trust relationships between each other based on their mutual trust of a certificate authority (CA). In a simple deployment, the trusted CA issues a certificate and “signs” certificates of the end entities that need to establish a secure connection between themselves. Entities trust each other’s certificates because they trust the issuing CA and can verify its signature using its root certificate.

The **integrity** of the data transmission in IPsec is ensured by authenticating the packets sent by the downstream radio unit (RU), DU or CU to ensure that the data has not been altered in any way. The downstream peer uses IPsec Encapsulating Security Payload (ESP) with integrity protection to apply a keyed one-way hash function to the datagram. The security gateway performs the same operation in reverse. Getting the same result ensures the integrity of the transmission.

For **confidentiality**, the security gateway uses IPsec encryption to ensure traffic confidentiality. IPsec is built into the DU and CU, which enables them to upload traffic directly to the mobile core using IPsec tunnels to reach the security gateway, which decrypts the traffic before it enters the core network.

The Nokia IPsec Security Gateway, can be combined with a certificate authority such as the Nokia NetGuard Certificate Manager, to provide these three types of protection for securing layer 3 traffic. It has been highly successful in securing 4G/LTE networks. After a decade of successful deployments, there have been no known breaches of 4G/LTE public mobile networks. The two Nokia products have also withstood rigorous testing by public safety authorities, which are now adopting them for public safety networks in many jurisdictions.

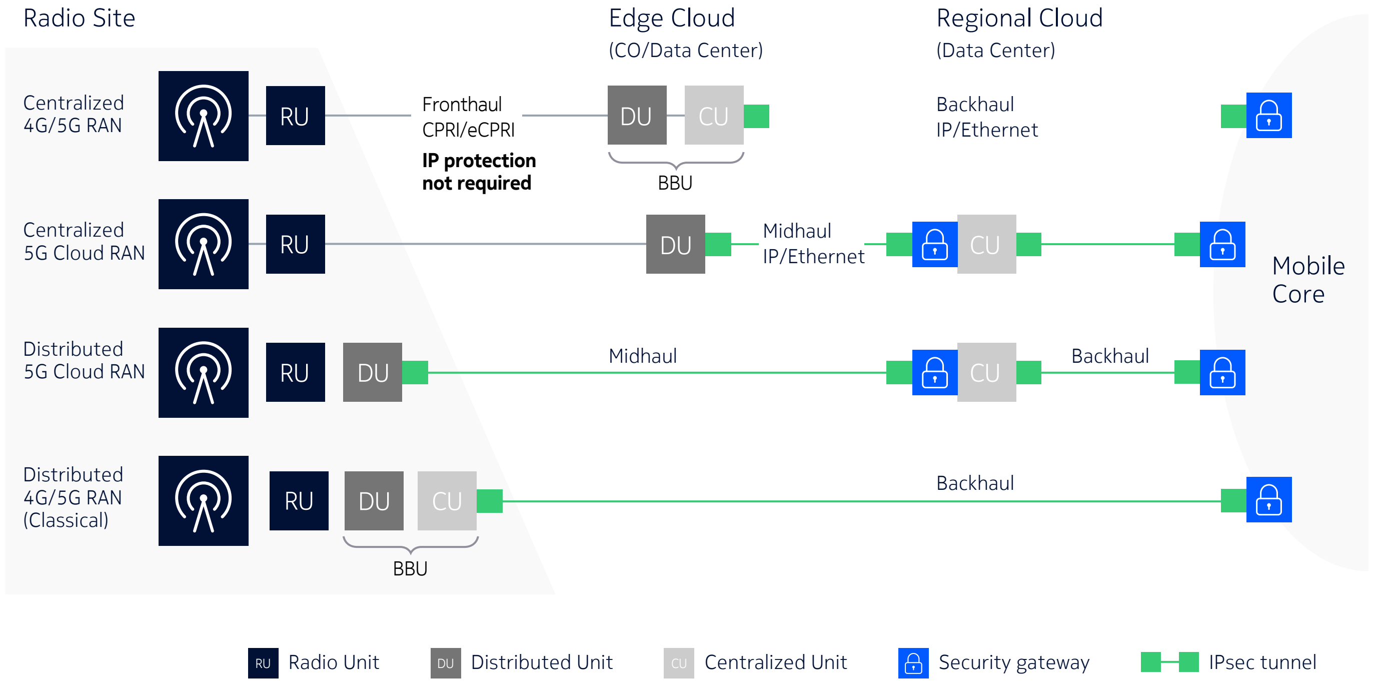
How it works in a 5G network

The gNB incorporates three main functional modules: the CU, the DU and the RU. These can be deployed in multiple combinations and configurations. Additionally, with CUPS, the CU can be decomposed into the CU user plane (UP) and CU control plane (CP), each of which has a separate connection to the DU (F1-U and F1-C).

Having this flexibility in the physical distribution of 5G core (5GC) and RAN functions requires that gateways be distributed to ensure that the various links are secured. Security solutions need to be flexible to address a mix of fronthaul, midhaul and backhaul. They should also be able to terminate IPsec tunnels from the full range of radio access sites, including macrocells, small cells and Carrier Wi-Fi.

Figure 1 shows four pragmatic RAN deployment models and the placement of secure gateways required in each case. Note that only the upstream receiver of this traffic, whether it is a CU or the mobile core, requires a security gateway to receive this IPsec traffic.

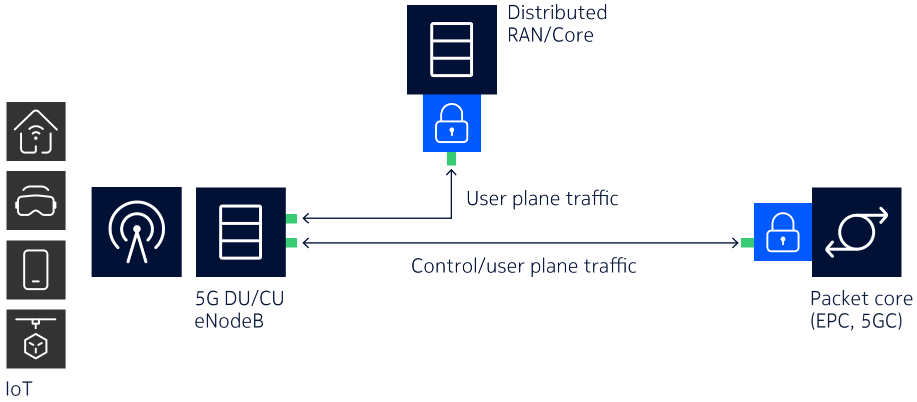
Figure 1. Securing various RAN options in 5G with different distributions of RU, DU and CU



The key difference with 5G is its addition of Cloud RAN options, both centralized and distributed. For example, the centralized 5G Cloud RAN decomposes the eNB and gNB, placing the DU in the edge cloud and the CU in a regional cloud. In the distributed Cloud RAN, the DU is located with the RU and there is no fronthaul portion. As Figure 1 illustrates clearly, these configurations introduce additional anyhaul connections that need to be secured.

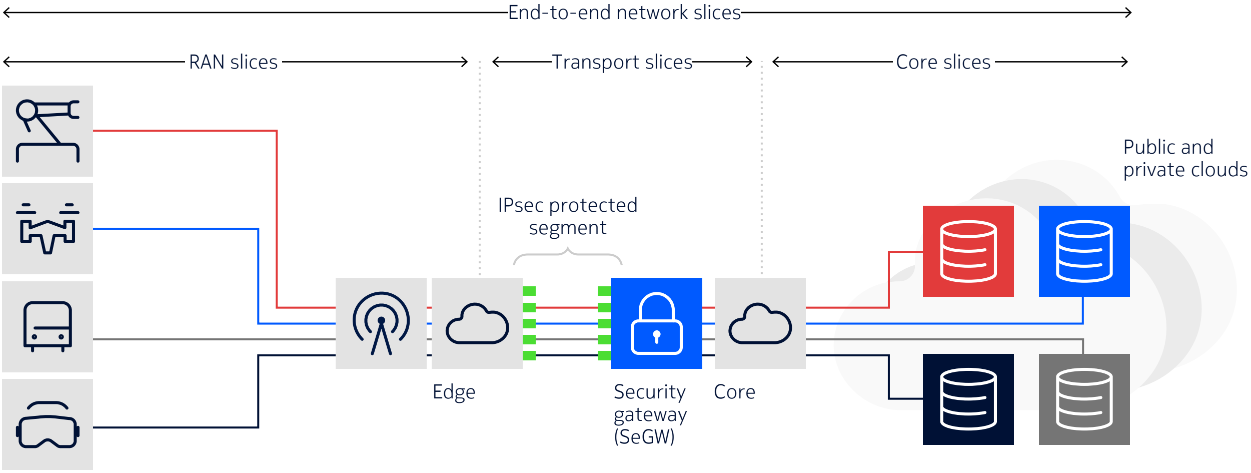
With CUPS configurations, protection can be extended to the user (data) plane, control plane and management plane through multiple backhauling options, as shown in Figure 2.

Figure 2. CUPS requires distributed security gateways for distributed network functions



Standards for securing 5G network slicing have not yet been determined. However, it is likely that these standards will use some method of applying IPsec tunnels to slices on the transport leg.

Figure 3. Securing network slices by applying IPsec tunnels per slice



The Nokia IPsec Security Gateway solution

Platform

The Nokia IPsec Security Gateway solution is available on the Nokia 7750 Service Router (SR) and the Nokia Virtualized Service Router (VSR). These platforms can be implemented in centralized or distributed deployment models and come in several form factors to suit different capacity requirements. The IPsec Security Gateway functionality can be added to Nokia routers already deployed in a network or implemented with dedicated routers. To ensure high availability, the platforms can also be deployed in redundant configurations.

Specialized cards are required in the 7750 SR platforms to support the IPsec Security Gateway functionality. Several Integrated Service Adapter (ISA) cards and an external Extended Services Appliance (ESA) are available to provide processing-intensive gateway services concurrently with other edge services, with no trade-offs between performance and advanced service delivery. The ISA cards and the ESA provide high-touch packet operations for advanced service capabilities, including IPsec Security Gateway and firewall.

Operators can extend the IPsec Security Gateway's flexible architecture by adding more ISA cards as half- or full-slot boards in a 7750 SR platform as IPsec traffic volumes increase. Alternatively, ESA modules connect to 100 GbE ports on 7750 SR routers, which saves slots on the routers. Up to 16 ISAs or ESAs can be added per router.

Virtualized security gateway

For operators that want to move more quickly to cloud technologies, Nokia delivers the IPsec Security Gateway functionality on the industry-leading Nokia VSR, as a virtualized network function (VNF). The IPsec Security Gateway application on the VSR leverages the cloud scalability of the x86 server architecture to accelerate cryptographic computation. Operators can scale up by adding more CPU and memory resources and scale out by adding more virtual machine resources. The application uses Intel QuickAssist Technology (QAT) to offload IPsec cryptography computation and significantly increase IPsec throughput.

Quantum-safe IPsec

We are entering the quantum era, where new quantum technologies will have significant and far-reaching benefits, but also consequences. As the development of quantum computers accelerates, we are approaching a critical inflection point where what the industry calls a cryptographically relevant quantum computer (CRQC) could soon be available. The CRQC will make most current asymmetric mathematics-based cryptography schemes obsolete, including Rivest–Shamir–Adleman (RSA), Diffie-Hellman (DH) key exchange and elliptic-curve cryptography (ECC). This threatens the integrity of digital infrastructures and economies because the industry has largely defaulted to these asymmetric cryptography solutions over the past several decades.

The availability date of a CRQC—often referred to as Q-Day—is the subject of market debate. But threat actors are already preparing for Q-Day. Many are collecting encrypted data from targeted organizations today and storing it so they can decrypt it when they eventually gain access to a CRQC. The industry refers to this ongoing activity as harvest now, decrypt later (HNDL). Network operators need to take steps now to secure their networks and mitigate this risk.

CRQCs impact IPsec in two areas but with different threat models:

1. Key exchange is used to derive the all the keys used by IPsec, including packet encryption keys. A threat actor can save encrypted IPsec traffic for future decryption with a CRQC in an HNDL attack.
2. Public key infrastructure (PKI) authentication is used to authenticate IPsec peers. A threat actor with a CRQC could impersonate an IPsec peer by forging certificates to compromise live IPsec communications.

There is ongoing work in standard organizations to extend IPsec for new mathematics-based post-quantum cryptography (PQC) algorithms. NIST has announced new PQC algorithms, and other organizations are also engaged in the development of PQC algorithms. Even with the announcement of these PQC algorithms, the work to absorb them into standards and operational cryptography frameworks will likely take several years. The time to achieve operational maturity should not be underestimated.

To provide a secure and trusted quantum-safe IPsec cryptography solution, the Nokia IPsec Security Gateway is implementing a phased approach.

1. Near term:
   a. Key exchange: The implementation of RFC8784 enables the provisioning of additional post-quantum preshared keys (PPKs) with quantum-safe entropy. These keys are incorporated into the IKEv2 key derivation process and are considered quantum-safe against a CRQC.

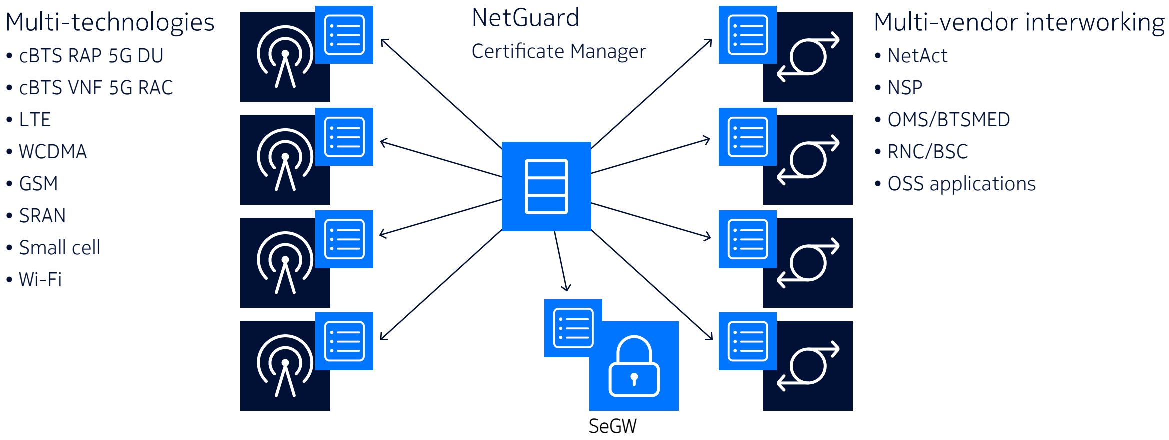
   b Authentication: If required, preshared key authentication could be used to mitigate any risk concerns.
2. Longer term: The migration to quantum-safe cryptography (QSC) algorithms for key exchanges and PKI authentication.

Certificate management

A trusted CA provides a public key certificate to a client to authenticate a user’s public key. The Nokia NetGuard Certificate Manager automatically downloads certificates and handles PKI certificate lifecycle management. It is a multivendor and multi-technology solution with self-organizing networks and plug-and-play support for automated certificate enrolment.

Nokia provides a complete, seamless interworking solution for a PKI-based infrastructure when the IPsec Security Gateway is combined with the NetGuard Certificate Manager, which performs the CA and sub-CA functions.

Figure 4. Nokia NetGuard Certificate Manager

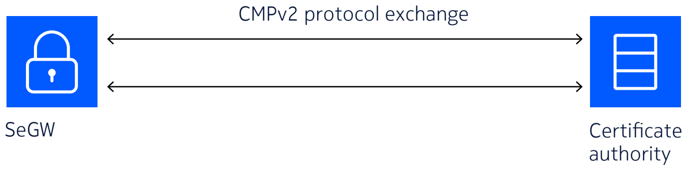


CMPv2 and EST

Certificate Management Protocol (CMPv2) and Enrollment over Secure Transport (EST) are two protocol options that provide online communication between the IPsec Security Gateway (end-entity) and the CA.

This enables the IPsec Security Gateway to enroll and renew a certificate with the CA and ensures that certificates can be distributed in a simple and secure way (Figure 5).

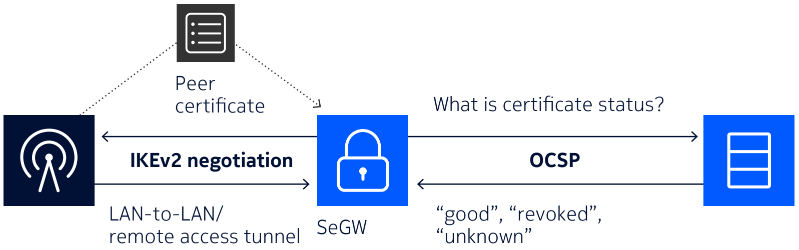
Figure 5. Nokia IPsec Security Gateway support for CMPv2



OCSP

The IPsec Security Gateway supports Online Certificate Status Protocol (OCSP), which enables the gateway to check the revocation status of a certificate in real time. This eliminates the need for periodic updates to the certificate revocation list (CRL) and removes the risk of relying on an outdated revocation status (Figure 6).

Figure 6. Nokia IPsec Security Gateway support for OCSP


Peer certificate
IKEv2 negotiation
LAN-to-LAN/ remote access tunnel
SeGW
What is certificate status?
OCSP
“good”, “revoked”, “unknown”

Automatic certificate and CRL update

Every certificate has a limited lifetime but CRL contains certificate revocation information issued by the CA, so it is important to keep the certificate and CRL up to date. The IPsec Security Gateway supports the following automatic update mechanisms:

- Certificate: The system automatically renews the certificate using the CMPv2 or EST protocol before the certificate expires.
- CRL: The system automatically downloads and updates the CRL from an HTTP server, either at regular intervals or before CRL expiration. These options make CRL management much easier for the operator.

The Nokia advantage

Capacity and throughput

The Nokia IPsec Security Gateway has the industry's highest capacity and throughput. For small cells, including femtocells, it can support 500,000 tunnels. For macrocell traffic, each ISA card or 7750 SR can support up to 32,000 IPsec tunnels by using full chassis capacity. Assuming one IPsec tunnel per eNB or gNB, that means each router can support 32,000 eNBs or gNBs. The VSR is also capable of supporting 32,000 tunnels. IPsec tunnel groups can be configured as required, with tunnel groups being load balanced across the available hardware resources.

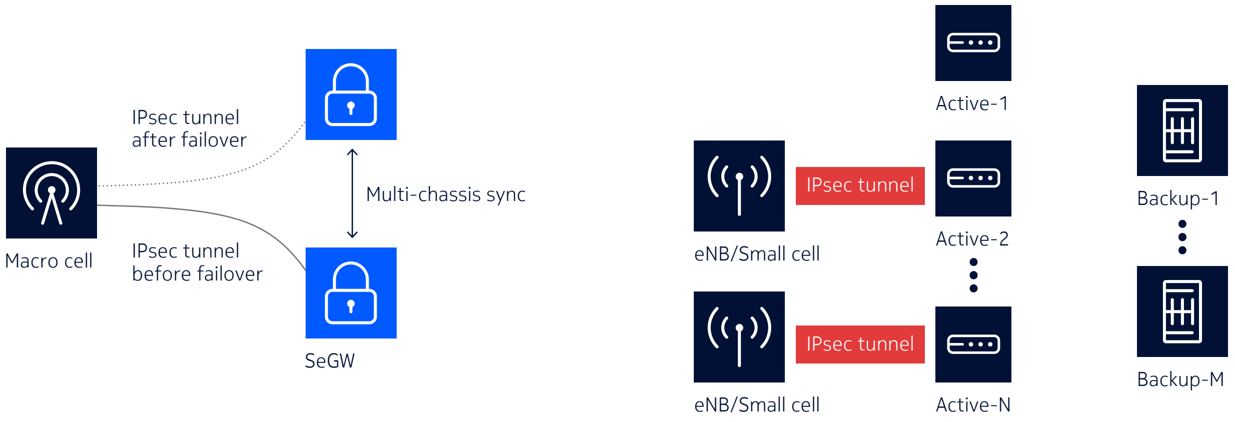
Throughput is the more important parameter in network design. Each ISA2 card has a throughput of 40 Gb/s. The 7750 SR can take 16 ISA2 cards for a maximum throughput of 640 Gb/s per system. Each ESA-400G has 200 Gb/s IPsec throughput for a maximum of 3.2 Tb/s throughput per system. The Nokia VSR appliance option can support more than 100 Gb/s throughput.

Carrier-grade high availability

High availability is one of most important requirements for a mobile network. The IPsec Security Gateway meets stringent carrier-grade requirements for high availability with:

- Fully redundant hardware components: control module, switch fabric, power and fan
- High availability across control modules
- N:M multi-chassis stateful IPsec redundancy (multi-chassis IPsec [MC-IPsec]) (Figure 7)
- Carrier-grade non-stop routing and non-stop services
- Load balancing at the port, card, service and tunnel levels
- Fast convergence across technologies, including Bidirectional Forwarding Detection (BFD), Multiprotocol Label Switching (MPLS), Virtual Router Redundancy Protocol (VRRP), interior gateway protocols (IGPs) and Border Gateway Protocol (BGP).

Figure 7. Nokia IPsec Security Gateway N:M multi-chassis redundancy



In multi-chassis stateful failover, all tunnel states are synchronized between multiple chassis or systems. Failover is fully transparent to the IPsec peer connected to the IPsec gateway. There is no need to renegotiate the tunnel and affect a service.

The immediate benefit for operators is that they can deploy radio sites based on a single IPsec tunnel (per service or for all services) instead of cumbersome, less scalable active/standby IPsec tunnels. They can do this while providing hitless service resiliency in case of a potential network or IPsec Security Gateway failure.

Because redundancy objectives and network characteristics can vary between different operators and different network builds, multi-chassis stateful failover is offered in an optimally flexible N:M mode. When we reduce N so that it is equal to 1, a single active chassis is assigned to one or more backup systems. This allows for sequential failover. For instance, a local system can fail over to a local, which, in turn, fails to a remote system and so on. While this approach provides full redundancy irrespective of how much traffic flows through a protected system, it also requires the largest capital investment.

At the other end of the spectrum, reducing M to be equal to 1 allows any number of active systems to share a single designated backup. While this approach requires the smallest capital investment, the backup chassis can quickly become a congestion point if multiple failovers force it to address more traffic or tunnels than its rated capacity.

Operators often choose to sit somewhere in the middle, assigning multiple active systems to multiple backup systems so they can achieve the optimal balance point between cost and redundancy based on their unique network characteristics and redundancy objectives.

Full IPv6 support

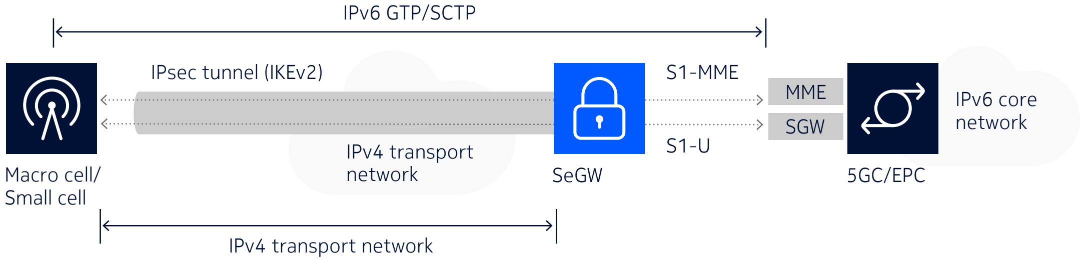
The number of user equipment (UE) and other mobile devices is increasing rapidly and, in response to the depletion of IPv4 addresses, IPv6 adoption is growing in all these devices. As a result, many networks need to evolve to IPv6 for bearer traffic between the device and the eNB or eNG and the ultra-broadband mobile gateways. Also, IPv6 can better support mobility plane evolution and scalability for traffic across other standardized mobile network interfaces. While more operators are deploying IPv6 to transport mobile traffic back to the core network, the transport portions of the network, including the backhaul network, may not support IPv6.

The Nokia IPsec Security Gateway addresses diverse network scenarios through comprehensive IPv6 support, including:

- IPv6 over IPv6
- IPv4 over IPv6
- IPv6 over IPv4 (Figure 8)
- IPv4 over IPv4.

This support gives mobile network operators maximum flexibility for planning and rolling out IPv6 in their networks.

Figure 8. Nokia IPsec Security Gateway support for IPv6 over IPv4 tunnels

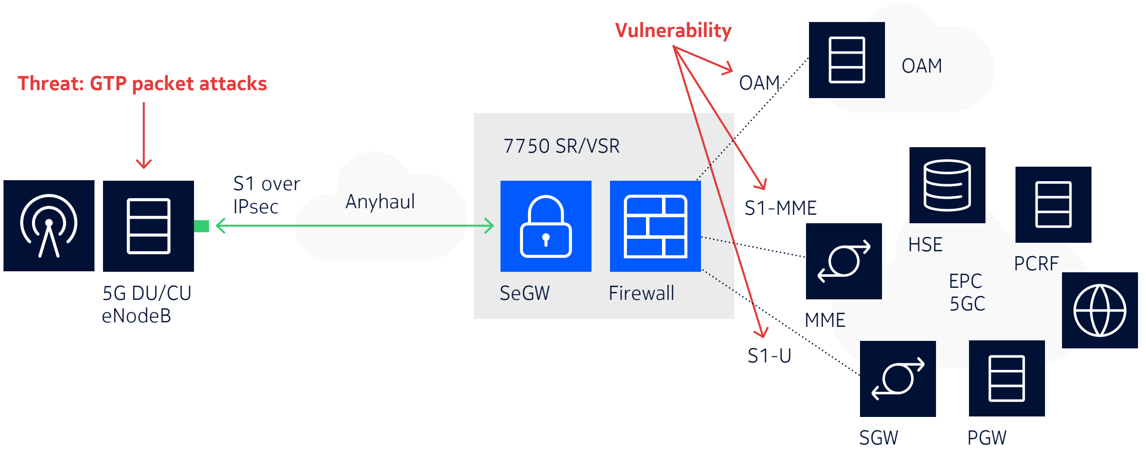


Firewall

The IPsec Security Gateway is complemented by the firewall capability included in the Nokia Service Router Operating System (SR OS) Application Assurance (AA) software package. AA software also runs on ISA cards or the ESA, which eliminates the need for external appliances. The AA Firewall protects the mobile core network from threats carried on the following types of traffic:

- Operations, administration and management (OAM)
- S1-MME, which uses the Stream Control Transmission Protocol (SCTP)
- S1-U, which uses the GPRS Tunneling Protocol - User Plane (GTP-U)

Figure 9. Nokia IPsec Security Gateway firewall capabilities



Protects core network from:
- Port scans
- Flood attacks
- Malformed packets

Protects traffic types:
- S1-MME (SCTP)
- S1-U (GTP-U)
- OAM

Nokia advantages:
- High performance
- Reliability
- Shares the same infrastructure

The AA Firewall performs stateful integrity and rule checking for applications admitted to the network. This includes protection against flooding, port scan, unsolicited traffic, malformed packet, unsupported GTP message types and Transmission Control Protocol (TCP) violation attacks.

Integration with Nokia IP portfolio

Implementing the IPsec Security Gateway on the 7750 SR or VSR platforms offers many advantages. Nokia designed security into the SR OS software from the start and has proven its best-of-breed design credentials in communications service provider networks for 15-plus years.

The 7750 SR and VSR platforms enable the IPsec Security Gateway to leverage the full range of layer 2 and layer 3 services to seamlessly interoperate with IP/MPLS-based networks. Standard IP routing and MPLS protocols are used for interoperability, and the same operational and management models are leveraged wherever a 7750 SR- or VSR-based network is deployed.

With this flexibility, the IPsec Security Gateway functionality can be delivered in many different converged deployment scenarios to meet an operator’s requirements. Many operators around the world have chosen the IPsec Security Gateway for fixed and mobile applications in diverse networking environments because of its ability to interwork with networking equipment from all major equipment vendors.

Conclusion

Pairing the Nokia IPsec Security Gateway with the Nokia NetGuard Certificate Manager enables operators to protect their 4G and 5G networks. It also enables mobile networks to securely and effectively interoperate in many access scenarios that are emerging in the ultra-broadband mobile era. The NetGuard Certificate Manager enables authentication of 4G and 5G network elements using X.509 digital certificates.

Abbreviations

3GPP	3rd Generation Partnership Project
4G	fourth-generation wireless (includes LTE)
5G	fifth-generation wireless
5GC	5G Core
AA	Application Assurance
BBU	baseband unit
BFD	Bidirectional Forwarding Detection
BGP	Border Gateway Protocol
BSC	base station controller
BTS	base transceiver station
BTSMED	BTS mediator
CA	certificate authority
cBTS	compact BTS
CMPv2	Certificate Management Protocol

CO	central office
CP	control plane
CPRI	Common Public Radio Interface
CPU	central processing unit
CRL	certificate revocation list
CRQC	cryptographically relevant quantum computer
CSP	communications service provider
CU	centralized unit
CUPS	Control and User Plane Separation
DU	distributed unit
eCPRI	enhanced CPRI
eNB	Evolved Node B
ESA	Extended Services Appliance
EPC	Evolved Packet Core
ESP	Encapsulating Security Payload
EST	Enrollment over Secure Transport
gNB	Next-generation Node B
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
GTP	GPRS Tunneling Protocol
GTP-U	GPRS Tunneling Protocol - User Plane
HNDL	harvest now, decrypt later
HSE	high-speed Ethernet
HTTP	Hypertext Transfer Protocol
ISA	Integrated Service Adapter
IKE	Internet Key Exchange
IP	Internet Protocol
IPsec	Internet Protocol Security
LAN	local area network
LTE	Long Term Evolution
MC-IPsec	multi-chassis IPsec
MEC	multi-access edge computing
MME	mobility management entity

MPLS	Multiprotocol Label Switching
NCM	NetGuard Certificate Manager
NIST	National Institute of Standards and Technology
NSP	Network Services Platform
OAM	operations, administration and management
OCSP	Online Certificate Status Protocol
OMS	NetAct IoMS solution
OS	operating system
OSS	operations support system
PCRF	Policy and Charging Rules Function
PGW	Packet Data Network Gateway
PKI	public key infrastructure
PPK	post-quantum preshared key
PQC	post-quantum cryptography
QAT	QuickAssist Technology
QSC	quantum-safe cryptography
RAC	radio access controller
RAN	radio access network
RAP	radio access point
RNC	Radio Network Controller
RSA	Rivest–Shamir–Adleman
RU	radio unit
S1	LTE interface
SA	standalone
SCTP	Stream Control Transmission Protocol
SeGW	security gateway
SGW	serving gateway
SR	Service Router
SRAN	Single RAN
TCP	Transmission Control Protocol
UE	user equipment
UP	user plane
VNF	virtual network function

VRRP	Virtual Router Redundancy Protocol
VSR	Virtual Service Router
WCDMA	Wideband Code Division Multiple Access

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: (October) CID174280