

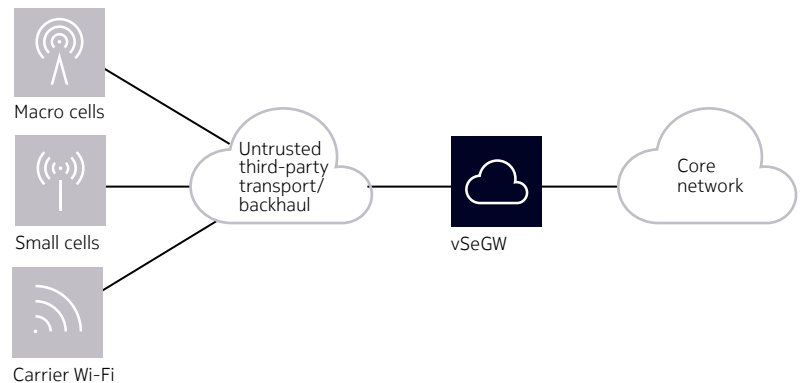
## Nokia Virtualized Security Gateway

VSR Release 20

Network operators looking for the scalability and flexibility of cloud architectures can deploy high-performance 3GPP security gateways (SeGWs) on carrier-grade virtualized routers. These provide the same functionality and resiliency as physical 7750 SR-based SeGWs.

The virtualized Security Gateway (vSeGW) is a virtualized network function (VNF) delivered by the Nokia Virtualized Service Router (VSR). It provides comprehensive, highly scalable and network-integrated Layer 3 IPsec-based VPN connectivity.

In mobile networks, the vSeGW can be used as a scalable, high-performance 3GPP security gateway. For site-to-site or network-to-network encrypted IP security, it can be used as a remote access concentrator as well as a security gateway.



### Features

- A rich feature set based on rigorous standards implementation
- Carrier-grade performance
- High availability
- Comprehensive support tools

### Benefits

- Quick IPsec deployment in cloud and hybrid environments
- Elastic scalability using standard, open-source IT compute virtualization
- Optimizes the use of available x86 hardware resources and overall system performance
- Cost efficient when used with the VSR's IP/MPLS services for fixed, mobile and converged network applications
- Superior deployment flexibility

## vSeGW implementation

vSeGW functionality can be enabled in VSR systems and applied to any type of network traffic in fixed, wireless (cellular and Wi-Fi®) and converged environments. It is based on the field-proven Nokia Service Router Operating System (SR OS).

The vSeGW has been design-optimized for Linux 64-bit operating systems (CentOS, Red Hat® Enterprise Linux® and Ubuntu) in combination with KVM/QEMU and VMware ESXi hypervisors. The vSeGW can optionally be deployed using OpenStack (Red Hat® OpenStack® Platform or RDO project distributions) and Nokia CloudBand.

For rapid deployment, Nokia also provides the vSeGW preinstalled and configured on the VSR Appliance (VSR-a) platform.

The Nokia Virtualized Service Router (VSR) can be deployed in two ways: it can be a stand-alone SeGW or it can act as an integral part of the data plane packet processing with other virtualized networking functions (e.g., Provider Edge, Broadband Network Gateway, Wireless LAN Gateway).

The Nokia Network Services Platform (NSP) delivers VNF and element management and allows network operators to seamlessly manage SeGW functionality from Nokia 7750 Service Routers and vSeGWs using the same operations, administration and maintenance protocols and management tools.

## A cloud-optimized security gateway

The Nokia VSR provides a rich set of security gateway features and functions, including:

- IP encryption and decryption, leveraging built-in cryptography acceleration extensions to the x86 instruction set including Intel® AES New Instructions (Intel® AES-NI) and Intel® Hyper-Threading Technology (Intel® HT Technology)
- Uses Intel QuickAssist (QAT) offload technology to accelerate IPsec throughput up to 100 Gb/s per VSR
- IPv4 and IPv6 support
- Internet Key Exchange (IKE) v1/v2
- Static/dynamic LAN-to-LAN tunnel
- Remote-access tunnel support; address assignment options are:
  - RADIUS
  - Local pool
  - External Dynamic Host Configuration Protocol (DHCP) v4/v6 server
- Pre-Shared Key/XAUTH/Certificate Authentication (IKEv2 only)/EAP (IKEv2 only)
- RADIUS-based authentication, authorization and accounting (AAA) for IKEv2 remote-access tunnel
- 3GPP standards compliant

## Technical specifications

### Encryption algorithms

- DES
- 3DES
- AES-CBC-128/192/256
- AES-GCM-128/192/256

### Authentication and hashing algorithms

- MD5
- SHA1
- SHA256
- SHA384
- SHA512
- AES-GMAC-128/192/256
- AES-XCBC

### Key distribution methods

- Manual exchange
- IKEv1 and IKEv2 with Perfect Forward Secrecy (PFS) support

### IPsec encapsulation formats

- Encapsulating Security Payload (ESP) with authentication support in tunnel mode

### Key exchange algorithms

- Diffie-Hellman Group: 1/2/5/14/15/19/20/21

### Tunnel authentication methods

- IKEv1/v2 pre-shared keys
- IKEv1 XAUTH
- IKEv2 X.509 certificates (RSA/DSA/ECDSA)
- IKEv2 EAP

### High availability

- Dead Peer Detection (DPD)
- Inter-VSR stateful IPsec redundancy

### Standards support

- RFC 2403 The Use of HMAC-MD5-96 within ESP and AH
- RFC 2404 The Use of HMAC-SHA-1-96 within ESP and AH
- RFC 2405 The ESP DES-CBC Cipher Algorithm With Explicit IV
- RFC 2407 IPsec Domain of Interpretation for ISAKMP (IPsec DoI)
- RFC 2408 Internet Security Association and Key Management Protocol (ISAKMP)
- RFC 2409 The Internet Key Exchange (IKE)
- RFC 2410 The NULL Encryption Algorithm and Its Use With IPsec
- RFC 3526 More Modular Exponential (MODP) Diffie-Hellman group for IKE
- RFC 3566 The AES-XCBC-MAC-96 Algorithm and Its Use With IPsec
- RFC 3602 The AES-CBC Cipher Algorithm and Its Use with IPsec
- RFC 3706 A Traffic-Based Method of Detecting Dead IKE Peers
- RFC 3947 Negotiation of NAT-Traversal in the IKE
- RFC 3948 UDP Encapsulation of IPsec ESP Packets
- RFC 4106 The Use of Galois/Counter Mode (GCM) in IPsec ESP
- RFC 4109 Algorithms for IKEv1
- RFC 4301 Security Architecture for the Internet Protocol
- RFC 4303 IP ESP
- RFC 4307 Cryptographic Algorithms for Use in the IKEv2
- RFC 4308 Cryptographic Suites for IPsec
- RFC 4434 The AES-XCBC-PRF-128 Algorithm for the IKE



- RFC 4543 The Use of Galois Message Authentication Code (GMAC) in IPsec ESP and AH
- RFC 4868 Using HMAC-SHA-256, HMAC.SHA-384, and HMAC-SHA-512 with IPsec
- RFC 4945 The Internet IP Security PKI Profile of IKEv1/ISAKMP, IKEv2 and PKIX
- RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
- RFC 5282 Using Authenticated Encryption Algorithms with the Encrypted Payload of the IKEv2 Protocol
- RFC 5903 ECP Groups for IKE and IKEv2
- RFC 5998 An Extension for EAP-Only Authentication in IKEv2
- RFC 6379 Suite B Cryptographic Suites for IPsec
- RFC 7296 Internet Key Exchange Protocol Version 2 (IKEv2)
- RFC 7321 Cryptographic Algorithm Implementation Requirements and Usage Guidance for Encapsulating Security Payload (ESP) and Authentication Header (AH)
- RFC 7427 Signature Authentication in IKEv2
- RFC 7468 Textual Encodings of PKIX, PKCS, and CMS Structures

Please refer to the [Nokia VSR data sheet](#) for system feature specifications and standards compliance.

## About Nokia

We create the technology to connect the world. Powered by the research and innovation of Nokia Bell Labs, we serve communications service providers, governments, large enterprises and consumers, with the industry's most complete, end-to-end portfolio of products, services and licensing.

From the enabling infrastructure for 5G and the Internet of Things, to emerging applications in digital health, we are shaping the future of technology to transform the human experience. [networks.nokia.com](https://networks.nokia.com)

Nokia operates a policy of ongoing development and has made all reasonable efforts to ensure that the content of this document is adequate and free of material errors and omissions. Nokia assumes no responsibility for any inaccuracies in this document and reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Nokia is a registered trademark of Nokia Corporation. Other product and company names mentioned herein may be trademarks or trade names of their respective owners.

© 2020 Nokia

Nokia Oyj  
Karaportti 3  
FI-02610 Espoo, Finland  
Tel. +358 (0) 10 44 88 000

Document code: SR2006045109EN (July) CID 200488