Nokia Virtualized Security Gateway

VSR Release 16

- Deploy a high-performance, resilient 3GPP security gateway (SeGW) on a carrier-grade virtualized router
- Elastically scale IPsec capacity and performance using standard, open-source IT compute virtualization
- Optimize the use of available x86 hardware resources and overall system performance

Overview
The virtualized Security Gateway (vSeGW) is a virtualized network function (VNF) delivered by the Nokia Virtualized Service Router (VSR).

The 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.

The vSeGW functionality on the VSR is based on the field-proven Nokia Service Router Operating System (SR OS).

The Nokia Network Services Platform (NSP) delivers VNF and element management and allows network operators to seamlessly manage SeGW functionality from a dedicated platform (such as the Nokia 7750 Service Router or the Nokia 7450 Ethernet Service Switch) and virtualized SeGW functionality (on the Nokia VSR) using the same operations, administration and maintenance protocols and management practices.

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.

Virtualized Security Gateway
The virtualized Security Gateway (vSeGW) provides comprehensive, highly scalable and network-integrated Layer 3 IPsec-based VPN connectivity.

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

The vSeGW can be used in mobile networks as a scalable and high-performance 3GPP security gateway. In addition, it can be used as a Remote Access Concentrator and a Security Gateway for site-to-site or network-to-network encrypted IP security.

IPsec services can be combined with the Nokia VSR comprehensive range of IP/MPLS services for fixed, mobile and converged network applications.
Network operators benefit from superior deployment flexibility, a rich feature set, carrier-grade performance, high availability and comprehensive support tools, enabling quick deployment and operationalization of a flexible and powerful IPsec feature set in cloud and hybrid environments.

Introducing the cloud-optimized security gateway

A carrier-grade vSeGW solution that caters to your evolving needs

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

- High-performance, scalable, virtualized IP encryption and decryption, leveraging built-in cryptography acceleration extensions to the x86 instruction set like Intel® AES New Instructions (Intel® AES-NI) and Intel® Hyper-Threading Technology (Intel® HT Technology)
- 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-128
- AES-192
- AES-256

Authentication and hashing algorithms
- MD5
- SHA1
- SHA256
- SHA384
- SHA512

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

Tunnel authentication methods
- IKEv1/v2 pre-shared keys
- IKEv1 XAUTH
- IKEv2 X.509 certificates
- 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 Internet Key Exchange (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 Internet Key Exchange (IKE) Peers
- RFC 3947 Negotiation of NAT-Traversal in the IKE
- RFC 3948 UDP Encapsulation of IPsec ESP Packets
- RFC 4301 Security Architecture for the Internet Protocol
- RFC 4303 IP Encapsulating Security Payload (ESP)
- RFC 4307 Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)
- RFC 4308 Cryptographic Suites for IPsec
- RFC 4434 The AES-XCBC-PRF-128 Algorithm for the Internet Key Exchange Protocol (IKE)
- 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 5998 An Extension for EAP-Only Authentication in IKEv2
- 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 7468 Textual Encodings of PKIX, PKCS, and CMS Structures

Please refer to the Nokia VSR data sheet for system feature specifications and standards compliance.