Nokia Virtualized Service Router

Release 25

The Nokia Virtualized Service Router (VSR) is a highly flexible virtualized IP edge router.

Architected and optimized for x86 server deployment in network operator and enterprise environments, the Nokia VSR is designed to:

- Enable agile delivery of new and innovative services
- Extend service reach and accelerate time-to-market
- Improve operational efficiency of next-generation IP infrastructure and services.

Based on the Nokia Service Router Operating System (SR OS), the VSR delivers a wide range of IP routing and network applications deployable as a virtual network function (VNF) or container network function (CNF).

Key features

- Wide range of supported functions deployable as VNFs or CNFs
- High performance
- Elastic cloud scalability
- Resiliency and robustness
- Advanced VNF management capabilities
- Advanced CNF deployment environment

Key benefits

- Increased deployment agility
- Rapid service introduction
- Flexible configuration and service chaining
- Lower service rollout risks
- Ease of interoperability
- Optimized use of resources and improved telecommunications and IT integration

Detailed features

Wide range of supported VNFs and CNFs

The Nokia VSR applications span the full range of IP/MPLS services, encompassing:

- Secured enterprise services: Provider Edge (PE) for secured enterprise networking and interconnection of branch offices, cloud and data centers over Ethernet and IP VPNs with optional Network Group Encryption (NGE) of services.
- Residential services: Broadband Network Gateway (BNG), Layer 2 Tunneling Protocol (L2TP) Network Server (LNS), L2TP Access Concentrator (LAC), and virtualized Residential Gateway (vRGW)
- Mobile services: Wireless LAN Gateway (WLGW).
- IP infrastructure services: Border Gateway Protocol (BGP) Route Reflector (RR), Network Address Translation (NAT), Mapping of Addresses and Ports using Translation (MAP-T).
- Application Assurance (AA) for L7 aware classification and control such as video rate limiting.
- Layer 7 Stateful Firewall for GTP Roaming (GRX), Gi, and Security Gateway (SeGW).
- Security: SeGW and NGE.

High performance

To maximize its control plane and data plane performance, the Nokia VSR has been optimized for deployment in scalable, virtualized computing environments.

A high-performance control plane is required to support compute-intensive control plane tasks and to minimize routing table convergence times. In addition, a high-performance data path is critical to ensure high-speed, low-latency packet processing and forwarding.

To deliver industry-leading capabilities for control plane and data plane functions, the VSR implements symmetric multiprocessing (SMP), a multi-threaded software approach whereby different processes are scheduled and run concurrently on different CPU cores for increased service scalability and routing performance on x86 platforms.

In addition, Nokia has optimized the interaction of the VSR with the underlying server and its input/output (I/O) ports. VM technologies such as Open-vSwitch Data Plane Development Kit (OVS-DPDK), single root I/O virtualization (SR-IOV) and Peripheral Component Interconnect (PCI) passthrough help drive the highest possible data plane performance for the VSR in x86 VNF environments. VSR as a CNF supports container network interfaces (CNI) of SR-IOV, Multus, Calico, and DPDK for physical interfaces.

When deployed as a VNF (VM), the VSR can also offload cryptographic computation to Intel® QuickAssist Technology (Intel® QAT) to further increase its performance—for example, its IPsec performance—when deployed as an SeGW.

Elastic cloud scalability

The 64-bit software architecture of the Nokia VSR enables access to more addressable CPU memory for improved routing and service scalability.

The VSR is deployed as a single virtual machine (VM) or container which processes all control plane and data plane tasks. Designed as a high-performance virtual instance capable of delivering a flexible combination of specialized IP routing applications, the VSR can efficiently scale and increase its capabilities through the addition of memory and CPU processing power as required.

Resiliency and robustness

The Nokia VSR is architected and optimized for deployment on x86 server platforms to meet extreme reliability demands for the virtualized environment by leveraging the Nokia SR OS — a real-time, modular and highly available operating system design.

The VSR enables the creation of robust network architectures using multi-node designs with advanced resiliency capabilities such as:

- Multi-chassis Link Aggregation (MC-LAG)
- Virtual Router Redundancy Protocol (VRRP)

- Pseudowire (PW) redundancy
- Dual-homed Virtual Private Wire Service (VPWS)
- BGP multi-homing for Virtual Private LAN Service (VPLS)
- MAP-T
- NAT with synchronized sessions
- BNG with synchronized subscribers
- IPsec with N:M stateful multi-node redundancy.

Advanced management capabilities

The Nokia VSR is compliant with the ETSI Network Functions Virtualization Management and Orchestration (NFV MANO) model.

Nokia has a comprehensive portfolio of products that fully cover the ETSI NFV architecture model, including:

- The Nokia AirFrame Data Center Solution, encompassing the necessary hardware, software and services
- Nokia CloudBand™, an open, modular software portfolio that makes it simple to host, orchestrate, automate and manage VNFs and services.

The VSR offers flexible management options, from open frameworks to OpenStack®-integrated VNF management, Kubernetes for CNF plaftform management, and model-driven element management through the Nokia SR OS. YANG-based data modeling delivers the foundation for programmability and model-driven interface support includes NETCONF, gRPC (gNMI and gNOI) and the Model-Driven CLI (MD-CLI). The Nokia NSP also supports these interfaces using YANG models to customize automation into operational use cases.

Through the Nokia NSP, VSR element management is delivered with end-to-end network management. Use of the Nokia NSP, which also manages Nokia 7750 Service Router (SR) applications, ensures operational consistency and service delivery assurance across both physical and virtual network environments, ensuring a streamlined operational evolution to a virtualized environment.

VSR Licenses

The operation of the Nokia VSR is enabled by an application-specific license (ASL) key containing the purchased rights related to the desired functionality of the VSR. This ensures that customers pay for only the functionality they need. All network functions supported by the VSR as well as all network functions from other systems in the Nokia IP portfolio—delivered as physical network functions (PNFs)—come with license keys that are generated based on the ASLs. These keys are associated with a particular network function instance (physical or virtualized). In the case of the VSR, this instance is the VM or the container.

License keys are obtained from Nokia for each VSR instance needed. Deployment of the VSR license keys may be facilitated by the Centralized License Manager (CLM), which governs the entitlement of license key deployment and enables the following benefits for the service provider:

- Simplified deployment with a pool of licenses instead of individual licenses
- Full control over individual VNFs and CNFs that can be flexibly activated and deployed
- Dynamic management of licenses in a cloud environment where VSR instances can be added and removed regularly.

The CLM is deployed in the customer network to manage the pool of ASL license keys across VSRs and 7750 SRs.

Detailed benefits

The implementation of the Nokia VSR for virtualized SR OS service routing provides many benefits:

- Increased deployment agility and flexibility: Reducing the time to deploy new networking services or optimize existing services can translate to a significant competitive advantage.
- Targeted service introduction: Enables rollout of services based on geography or specific requirements.
- Flexible configuration and service chaining: Enables innovation and creation of new services that can improve customer satisfaction and increase loyalty.
- Lower service rollout risks: Allows service providers to trial and evolve services to determine what best matches new regulatory requirements or customer needs.
- Ease of interoperability: Using standardized and open interfaces allows for integration in a wide variety of deployment environments.
- Optimized use of resources and improved telecommunications and IT integration: Proven high performance with optimized use of resources on a standardized x86 compute platform for different applications, users and tenants enables rollout of profitable services based on measurable business models.

VSR architecture

Nokia has leveraged its leading expertise and innovation in service routing and has architected and optimized the Nokia VSR for the x86-based server architecture by applying advanced design concepts, principles and approaches, including:

- Separation of control plane and data plane tasks: Allows for independent scaling of control plane and data plane within each VSR instance.
- A virtual Forwarding Path (vFP): The vFP is the x86-optimized forwarding path that supports data path functions, including access control lists, QoS classification, policing, Forwarding Information Base (FIB) lookup, and related packet-processing functions.
- SMP: Using this multi-threaded software approach, whereby different processes can be scheduled and run concurrently on different CPU cores, allows for improved service scalability and routing performance on x86 platforms.
- 64-bit OS: The 64-bit software architecture enables access to an increased amount of addressable system memory for improved routing and service scalability.
- Use of acceleration techniques: Using open platforms and partnering with Intel to optimize the interaction of virtualized functions with the underlying server and its I/O, including storage. Nokia is leveraging technologies such as the SR-IOV PCI passthrough, and DPDK to consistently drive the highest possible data plane performance in x86 environments.

As a result of these advanced design concepts, principles and approaches, Nokia's flexible and robust virtualized router implementation on the VSR allows:

- Optimal utilization of hypervisor (host) resources
- High performance for both control plane (routing) and data plane (packet forwarding) functions
- Separation of control plane and data plane CPU cores
- Advanced multi-system redundancy features
- Resilient cloud scaling
- Superior life-cycle management capabilities with a unique approach to consistent operations across physical and virtualized network elements.

VSR deployment

The Nokia VSR is deployed in an integrated model, where the VSR control plane and data plane functionality are implemented on a single VSR routing instance. In this model, the virtual CPU and memory are shared among:

- Control tasks, including:
  - Dynamic Host Configuration Protocol
  - RADIUS/Gx
  - Interior gateway routing protocols
  - Exterior gateway routing protocols
  - Routing table management
  - Policies
- Packet forwarding data plane tasks
- Optional, value-added functions such as IPsec, NGE, NAT and AA
- System management tasks such as NETCONF, Simple Network Management Protocol and Secure Shell (SSH).

Figure 1 shows the deployment model of the VSR as a VNF VM. Figure 2 shows the deployment model of the VSR as a CNF container.

VSR flexible licensing

The Nokia VSR supports a wide range of IP/MPLS edge services.

VSR deployment models are flexible. A network can be can be deployed running a wide range of standalone VSR instances (e.g., PE, BNG, RR, NAT, etc.) or VSR instances implementing multiple network function roles (e.g., BNG and NAT). Selection of which VSR features are to be used is enabled through a modular and flexible licensing scheme.

VSR licensing also allows customization and easy addition of integrated value-added services, such as AA, IPsec, Generic Routing Encapsulation (GRE) tunnels and NAT functions, and features such as Lawful Interception (LI).

Table 1 outlines the main functions supported by the VSR.

Figure 1. VSR VM deployment model

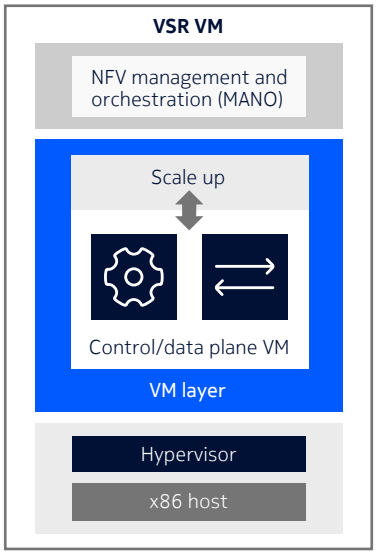


Figure 2: VSR CNF deployment model

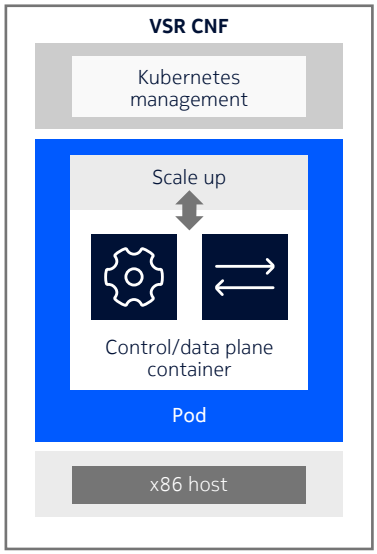
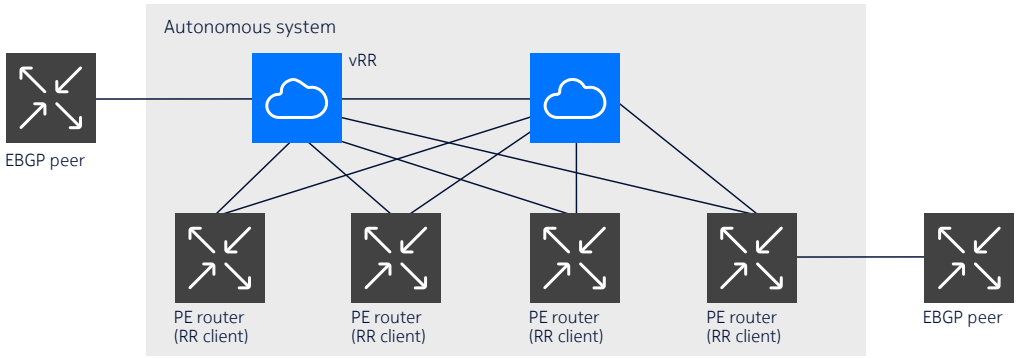


Table 1. Supported network applications

VSR Role	Description
Route Reflector	• A control plane function, route reflection eliminates the need for a full internal BGP mesh between peers
Provider Edge	• Represents the IP/MPLS network edge for enterprise services
Application Assurance	• Enables Layer 3 to Layer 7 (L3–L7) visibility and intelligent, policy-driven analytics and control of IP applications, with per-application, per-subscriber and per-VPN service granularity. Provides TCP Optimization (TCP-O) for WLGW DSM subscribers.
Layer 7 Stateful Firewall	• An in-line integrated stateful firewall that protects mobile packet core infrastructure from malicious security attacks; enables operators with advanced, next-generation firewall functionality, including GRX and Gi, and additional features such as in-browser notifications, URL filtering, HTTP enrichment and redirect
Broadband Network Gateway	• Represents the IP/MPLS edge for residential services delivery
L2TP Network Server	• Enables connectivity to L2TP Access Concentrators (LACs) and allows the creation of a VPN over a third-party or shared infrastructure
Network Address Translation	• Enables NAT applications, allowing network operators to conserve IPv4 addresses and maintain IPv4 internet access while migrating to IPv6 (NAT44, NAT64, Dual-Stack Lite)
Mapping of Addresses and Ports using Translation (MAP-T) Border Relay	• Uses MAP-T protocol translation as a NAT technique to transport IPv4 packets over a private IPv6 network (e.g., an ISP's IPv6 network) • Acts as a MAP Border Relay (BR) and implements stateless IPv4-to-IPv6 translation • Works in conjunction with stateful IPv4/port translation and stateless IPv4-to-IPv6 address translation performed by customer equipment
Security Gateway	• Enables comprehensive, network-integrated Layer 3 IPsec VPN connectivity for remote or network-to-network encrypted IPsec security • Delivers 3GPP SeGW functionality for secure mobile backhaul with additional features such as Stateful Layer 7 Firewall
Network Group Encryption	• In combination when operating the VSR as a PE, enables a versatile, scalable, seamless and uniform group-based framework for encryption and authentication for any type of IP/MPLS traffic • Delivers "nonstop encryption" with flexible and easy assignment of network elements in the NGE domains and the use of the Nokia NSP for robust and reliable encryption key management
Wireless LAN Gateway	• Aggregates tunneled traffic from the Wireless LAN access points
Virtualized Residential Gateway	• Enables virtualization of specific residential services functions, which have historically been implemented in the residential gateway device deployed in the home (residential CPE) • Soft-GRE tunnel access

The following examples provide more information on some of the supported network applications. For additional information about feature support and standards compliance, contact your local Nokia representative.

virtualized Route Reflector



Overview

A Route Reflector, as specified in IETF RFC 4456, is a specific role in a BGP routing scheme where only a select number of routers—RRs—are designated as prefix distribution and policy nodes. These routers participate in volume routing topology updates and provide the best paths (according to network policy) to their clients. Because route reflection is a control plane function, it is ideally suited for virtualization.

Deployment

The VSR virtualized Route Reflector (vRR) is operationally equivalent to the BGP RR on the Nokia 7750 SR or on the Nokia 7950 Extensible Routing System (XRS) because the VSR also implements the Nokia SR OS, re-architected and optimized for the x86 server environment.

The VSR enables flexible RR deployment as: a single RR for all services; separate RRs for each service (e.g., internet, Layer 3 VPN or Layer 2 VPN); or RRs for specific groups of services (e.g., all IPv6 protocols). In addition, the VSR enables linear RR performance scaling by fine-tuning resources based on application needs.

The vRR dramatically improves overall network convergence times by performing heavy-duty BGP route processing, for which traditional network elements (designed for high-throughput applications) are not as well suited. The VSR also optimizes the use of all available CPU cores.

The VSR enables easy addition of memory and CPU resources to improve RR scalability and performance. Increased memory allows for an increased number of BGP peers and routing entries. Additional CPU resources improve performance for reflecting or advertising routes as well as improving route convergence times.

The vRR can be deployed in all types of IP environments, facilitating internet connectivity or deployment of Layer 3 IP VPN services.

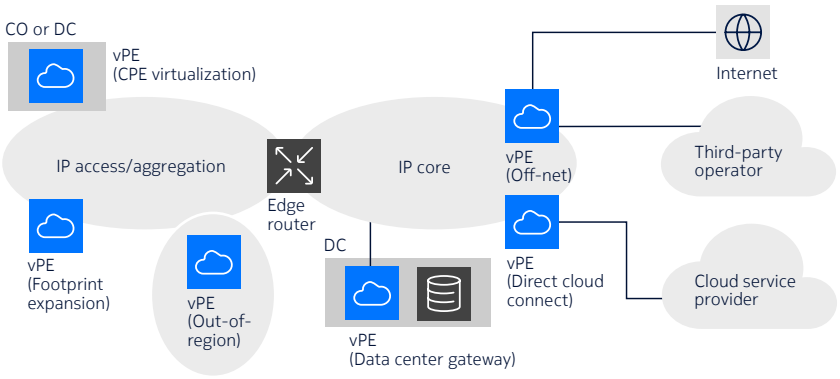
Layer 2 Ethernet VPNs (EVPNs), a next generation of Ethernet services, are also supported. EVPNs are growing in importance in the industry because they offer sophisticated access redundancy combined with Layer 3 VPN-like operations for scalability and control.

Optimal Router Reflection

The vRR comes with Nokia's innovative Optimal Router Reflection (ORR). ORR allows flexible placement of the VSR-based vRR functionality anywhere in the network, with the ability to define reference points independent of the physical location of the vRR. This flexibility can enable service providers to create robust network architectures with optimal placement of network functions.

- Improve network performance with industry-leading vRR implementation
- Enable cloud scaling with easy addition of memory and CPU resources
- Optimize the use of available x86 hardware resources

virtualized Provider Edge



Overview

The VSR virtualized Provider Edge (vPE) is an essential network function for delivering highly available Carrier Ethernet, IP VPN and internet services over IP/MPLS infrastructure. Service providers can deploy a vPE for rapid service innovation and to extend service reach, open new markets and accelerate time-to-market. Enterprises can deploy a virtualized router as an alternative to using a physical router in their network.

Deployment

A vPE can be deployed as:

- PE router: Transition to a more elastic, on-demand deployment model and to complement chassis-based infrastructure with platform flexibility for expansion of the existing footprint or for out-of-region deployment.
- PE Gateway: For off-net locations, provides internet and third-party operator connectivity from a host site with a more elastic, on-demand deployment model.
- Data Center Gateway (DCGW): Provides an efficient way to rapidly extend connectivity between new software-defined networking (SDN)-enabled data centers and existing VPN customers in network locations where the existing PE router may not support DCGW functions.
- Enterprise WAN router: For enterprise network locations, enables rapid value-added services with consistent operations between virtual and physical elements.

In addition, vPE can be deployed for direct cloud connectivity, delivering guaranteed public cloud connectivity to VPN customers by directly connecting them to public cloud service providers.

The VSR-based vPE supports comprehensive IP edge routing features and can be extended with additional service options as needed:

- AA for powerful per-application QoS, per-VPN analytics and policy-driven application control
- Carrier-grade NAT (CG-NAT) to manage the transition to IPv6
- Network-integrated Layer 3 IPsec VPN connectivity
- NGE for encryption and authentication of any type of IP/MPLS traffic.

- Accelerate cloud evolution in service provider and enterprise networks
- Offer differentiated retail and wholesale enterprise services in an agile manner
- Expand enterprise services into new markets and augment service reach

virtualized Application Assurance

Overview

The VSR virtualized Application Assurance (vAA) is a virtualized implementation of deep packet inspection (DPI). The vAA functionality can be applied to any type of network traffic in residential, enterprise and WLAN environments.

The vAA enables L3–L7 visibility, analytics and intelligent, policy-based control of IP traffic flows with per-application, per-subscriber and/or per-VPN service granularity. The vAA functionality is optimized for cloud environments and allows extensive control of network applications as well as application-level reporting and traffic management capabilities. AA offers Transmission Control Protocol (TCP) maximum segment size (MSS) adjusted to prevent packet fragmentation, as well as TCP Optimization for Wireless LAN Gateway DSM subscribers.

Network operators benefit from superior deployment flexibility, a rich feature set, carrier-grade performance and comprehensive support tools, enabling quick deployment and operationalization of a flexible and powerful AA feature set in cloud and hybrid environments.

Deployment

The Nokia VSR can provide vAA functionality as a fully integrated Application Detection and Control (ADC) network function in all VSR configurations (e.g., PE, BNG, SeGW, RGW, WLGW), where AA tasks are performed as an integral part of the data plane packet processing. Alternatively, the VSR can be deployed as a transit AA function, performing as a dedicated ADC element and offering a rich set of features and options complementing IP edge and gateway systems that either cannot support an integrated ADC or that lack required features or performance.

The vAA policy models can be applied network-wide or tailored and dynamically associated with specific service types, VPNs or individual subscribers and users, using RADIUS or Diameter policy control from an authentication, authorization and accounting (AAA) server or a Policy and Charging Rules Function (PCRF).

The Nokia NSP delivers element management and allows network operators to seamlessly manage AA functionality delivered from a PNF such as the Nokia 7750 SR as well as virtualized AA functionality on the Nokia VSR using the same operations, administration and maintenance (OAM) protocols and management practices.

The Nokia NSP provides comprehensive support to define and manage AA policies and policy updates, allowing operators to tailor the deployment of AA functionality to individual applications or groups of applications (e.g., multimedia, peer-to-peer, web and instant messaging).

- Add high-performance and cloud-scalable stateful L3–L7 packet processing to a virtualized network domain
- Quickly introduce application-based value-added services with flexible deployment policy models (network-wide, service-based or per-subscriber)
- Provide detailed analytics, reporting and control of network applications

virtualized Layer 7 Stateful Firewall

Overview

The VSR virtualized Layer 7 Stateful Firewall uses AA application-level analysis, enabling the Nokia VSR to provide an in-line integrated stateful firewall that protects mobile packet core infrastructure from malicious security attacks. Using the AA stateful packet filtering feature combined with AA Layer 7 classifications and control empowers operators with advanced, next-generation firewall functionality.

In stateful inspection, the firewall inspects packets at Layer 3–Layer 7 and also monitors the connection's state.

Deployment

The Nokia VSR can provide vAA firewall functionality as a fully integrated firewall network function in all VSR configurations where vAA firewall tasks are performed as an integral part of the data plane packet processing):

- PE
- BNG
- SeGW
- RGW
- WLGW.

Alternatively, the VSR can be deployed as a transit AA firewall VNF function performing as a dedicated firewalling security function and offering a rich set of features and options. In mobile backhaul, a vAA firewall VSR can be deployed at the following network interfaces to provide firewall security functions:

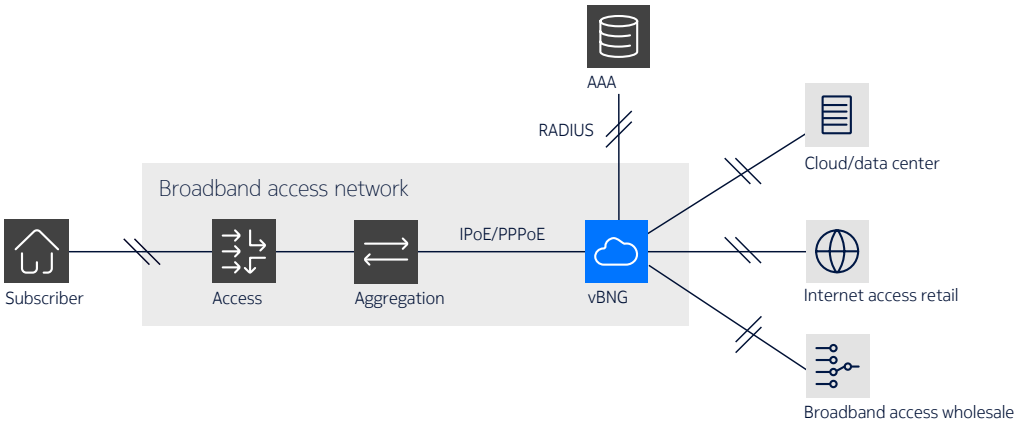
- 3GPP S1-MME/S1-U
- 3GPFF S5/S8.

The Nokia NSP delivers element management and allows network operators to seamlessly manage AA functionality delivered from a PNF such as the Nokia 7750 SR as well as virtualized AA firewall functionality on the Nokia VSR using the same OAM protocols and management practices.

The NSP provides comprehensive support to define and manage AA firewall policies and policy updates, allowing operators to tailor the deployment of a vAA firewall. The NSP provides the operator with the required firewall security-related reports and statistics.

- Add high-performance and cloud-scalable stateful (L3–L7) firewall packet processing to a virtualized network domain
- Provide detailed analytics, reporting and control of network security

virtualized Broadband Network Gateway



Overview

The VSR virtualized Broadband Network Gateway (vBNG) is an essential network function for network operators and ISPs offering retail and wholesale services to the residential market:

- Legacy Broadband Remote Access Server replacement to deliver residential internet access services using a virtualized platform with elastic scaling
- Advanced subscriber management capabilities to foster a more user-centric and differentiated online experience
- A complement to existing BNG network equipment to address basic high-speed internet (HSI) and IPTV services with a more agile service delivery architecture for the cloud era

Deployment

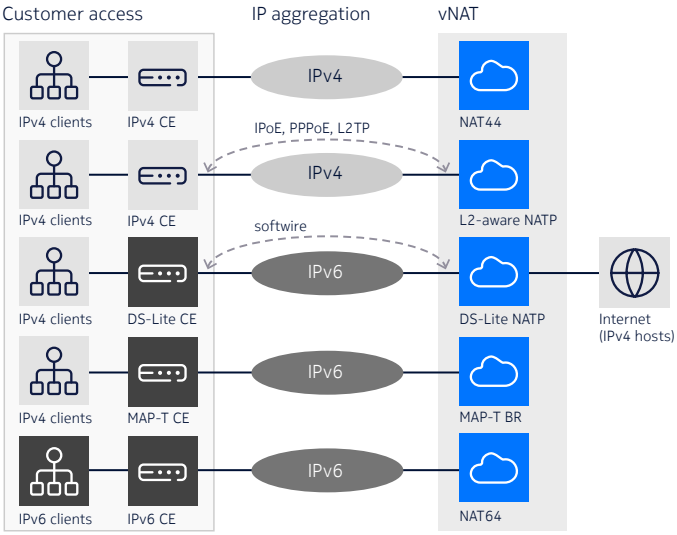
The vBNG supports subscriber service edge virtualization for internet retail and wholesale service delivery over xDSL and FTTx access technologies, with dual-stack IPoE and PPPoE session management and RADIUS authentication. To enable a fully virtualized BNG user plane function (UPF), the vBNG is compatible with BBF TR-459 Control and User Plane Separation (CUPS). Comprehensive application QoS and security policy enforcement, and captive web subscriber portals help deliver a personalized and rich cloud experience.

The Nokia VSR as a vBNG supports enhanced subscriber management and comprehensive IP edge routing features, and can be extended with additional service options as needed:

- CG-NAT to manage the transition to IPv6
- AA for powerful application QoS, analytics and security policy enforcement
- Advanced features such as in-browser notifications, captive portals and URL filtering

- Virtualize the residential subscriber services edge to quickly address new market opportunities with a cloud-based service delivery model
- Elastically scale capacity using standard, open-source IT compute virtualization in a distributed edge or centralized data center environment
- Compatible with RADIUS authentication, authorization and accounting (AAA) to ease integration with legacy systems

virtualized Network Address Translation



Overview

IPv6 has gained wide-scale deployment and acceptance in private clouds and on the internet, but IPv4 services still need to be supported for many years until the migration to IPv6 is complete. Network Address Translation (NAT) helps network operators achieve an orderly and phased transition to IPv6 and maintain IPv4 service continuity during the migration process.

- NAT44 allows many IPv4 clients to reuse the same public IPv4 address to scale IPv4 services within the confines of the available address space.
- DS-Lite (RFC 6333) allows interworking IPv4 clients with IPv4 hosts over an IPv6 access network by using tunneling techniques in combination with NAT44.
- Subscriber-aware Network Address and Port Translation (NATP)applies the soft-wire concept of DS-Lite to Layer 2 subscriber sessions and is deployed as an integrated function of the BNG. This model provides better scalability and performance, simplifies multi-node redundancy and reduces log data.
- MAP-T enables IPv4 interworking over IPv6 by using a stateless Border Relay at the PE and a stateful NAT44 function at the customer edge.
- NAT64 enables IPv6 clients to interwork with legacy IPv4 hosts on the internet.

Deployment

The Nokia VSR can be configured to deliver a standalone vNAT function when the VSR is configured as a PE.

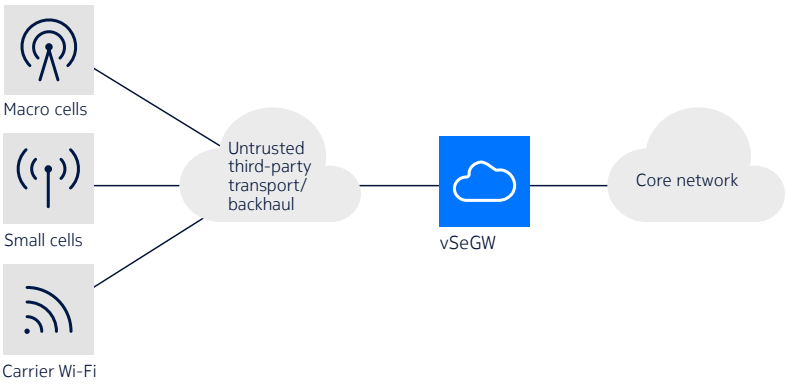
Alternatively, vNAT functionality can be fully integrated when the VSR is configured as a vBNG or as a vWLGW.

In both cases, vNAT is Layer 2-aware, and tight coupling and full synchronization of subscriber context (BNG and NAT or WLAN and NAT) is achieved.

The vNAT functionality is based on the field-proven Nokia SR OS. The Nokia NSP delivers element management and allows network operators to seamlessly manage integrated NAT capabilities (delivered on a service router platform) and virtualized NAT functionality using existing OAM protocols and management practices.

- Versatile IPv4-to-IPv6 migration support with large-scale NAT44, DS-Lite, L2-aware NATP, NAT64 and MAP-T (RFC 7599)
- Leverage standard, open-source IT compute virtualization for elastic scaling
- Deploy on general-purpose server hardware for superior investment protection

virtualized Security Gateway



Overview

The VSR virtualized Security Gateway (vSeGW) provides comprehensive, highly scalable and network-integrated Layer 3 IPsec-based VPN connectivity. The vSeGW functionality can be applied to any type of network traffic in fixed, wireless (cellular and Wi-Fi®) and converged environments.

The vSeGW can be used in mobile networks as a scalable and high-performance 3GPP SeGW. In addition, it can be used as a Remote Access Concentrator and an SeGW 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.

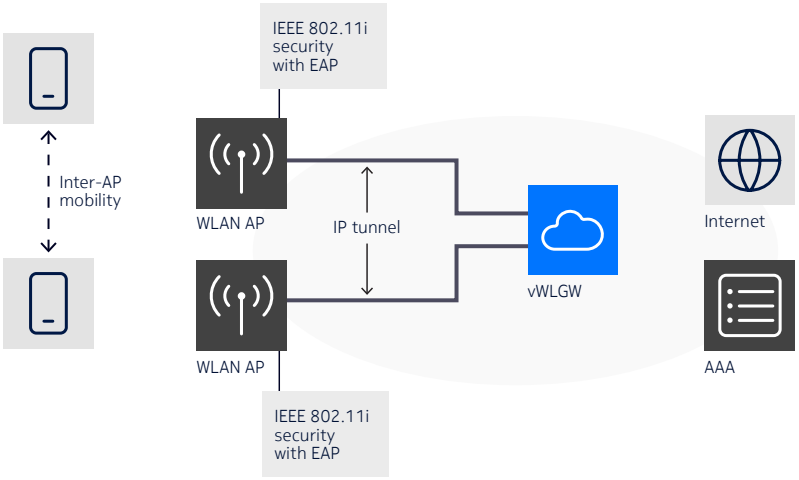
Deployment

The Nokia VSR can be deployed as a standalone SeGW or it can deliver SeGW functionality as an integral part of the data plane packet processing with other virtualized networking functions (e.g., PE, BNG, WLGW).

The Nokia NSP delivers element management and allows network operators to seamlessly manage SeGW functionality from a dedicated platform (such as the Nokia 7750 SR) and vSeGW functionality (on the Nokia VSR) using the same OAM protocols and management practices.

- Deploy a high-performance, resilient 3GPP 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, including hardware acceleration using IntelQAT for cryptographic computation

virtualized Wireless LAN Gateway



Overview

The virtualized Wireless LAN Gateway (vWLGW) supports a variety of wholesale and retail deployment scenarios, allowing both wireline and wireless network operators to leverage unlicensed Wi-Fi as an access technology. It supports a range of IP networking capabilities that enable seamless integration into existing fixed and mobile networks.

Deployment

The Nokia VSR can be deployed as a standalone WLGW or it can deliver WLGW functionality as an integral part of the data plane packet processing with other functions such as a vPE or a vBNG.

The vWLGW aggregates tunneled traffic from the WLAN access points and applies QoS. The vWLGW also supports mechanisms to coordinate with the network operator's back-end subscriber, policy and billing infrastructure for authentication and the parameters needed to create subscriber context.

Network operators can benefit from the high availability as well as the advanced gateway capabilities, which enable integration with NAT and AA functions.

The Nokia NSP delivers element management. The NSP allows network operators to seamlessly manage WLGW functionality from a dedicated platform (such as the Nokia 7750 SR) and vWLGW functionality (on the Nokia VSR) using the same OAM protocols and management practices.

- Allow wireline and wireless providers to leverage Wi-Fi® access to expand service footprint
- Preserve cellular spectrum by offloading data onto unlicensed Wi-Fi
- Offer wholesale Wi-Fi access service at Layer 2 and/or Layer 3 to retail service providers

Technical specifications

Virtualization infrastructure

CPU models

- Intel® Xeon® Processor E5-26xx v4 (Broadwell-EP)
- Intel Xeon 41xx/51xx/61xx/81xx Silver, Gold or Platinum (Skylake SP)
- Intel Xeon 42xx/52xx/62xx/82xx Silver, Gold, or Platinum CPUs (Intel Cascade Lake SP)
- Intel Xeon 43xx/53xx/63xx/83xx Silver, Gold, or Platinum CPUs (Intel Ice Lake SP)
- Intel Xeon 44xx/54xx/64xx/84xx Silver, Gold, or Platinum CPUs (Intel Sapphire Rapids SP)

VNF hypervisors and host OS

- Linux Kernel-based Virtual Machine (KVM) on CentOS 7.0, 7.2, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9
- Linux KVM on CentOS 8.1, 8.2, 8.3
- Linux KVM on Red Hat Enterprise Linux 7.1, 7.2, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9
- Linux KVM on Red Hat® Enterprise Linux® 8.1, 8.2, 8.3, 8.4, 8.6, 8.8
- Linux KVM on Ubuntu 14.04 LTS, 16.04 LTS, 18.04.5 LTS and 20.04.1 LTS
- VMware ESXi™ 6.0 (Update 2) and 6.5 (Update 1)
- VMware ESXi™ 6.7 and vCenter Server 6.7
- VMware ESXi™ 7.0 (Update 1c) and vCenter Server 7.0 (vCD 10.2)
- VMware ESXi™ 7.0 (Update 3)
- VMware ESXi™ 8.0

VNF I/O virtualization

- VirtIO (with Linux KVM)
- VMXNET3 (with VMware ESXi)
- PCI passthrough
- SR-IOV

CNF Kubernetes host OS

- Linux kernel 4.18 or later

CNF CNI

- SR-IOV
- Multus
- Physical interface types using DPDK
- Calico
- Macvlan plugin for the management interface
- Host-device plugin for external interfaces
- Helm or YAML installation using DPDK interfaces
- Podman or Docker instantiation using MACVLAN or linux bridge user plane interfaces for Route Reflector

VNF vSwitch

- Linux bridge (vhost-net)
- Open vSwitch 2.3.0 (vhost-net)
- Open vSwitch 2.4.0 with DPDK 2.1.0 (vhost-user)
- Open vSwitch 2.5.0 with DPDK 2.2.0 (vhost-user); requires QEMU 2.5.0 or later
- Open vSwitch 2.9 with DPDK 17.11

VNF DPDK

- Open vSwitch open-source DPDK (using VirtIO)

OpenStack

- RPM Distribution of OpenStack (RDO) OpenStack Liberty
- RDO OpenStack Mitaka
- RDO OpenStack Newton
- RDO OpenStack Ocata
- RDO OpenStack Pike
- RDO OpenStack Queens
- RDO OpenStack Rocky
- Red Hat® OpenStack Platform: OSP 8, 9, 10, 11, 12, 13 and 16.1
- Mirantis OpenStack 9.0

Container Orchestration

- Openshift version 4.14 and later
- Alicloud
- Wind River Studio Cloud Platform versions version 22.12 or 24.09 or later, using Intel or Mellanox SR-IOV interfaces

VSR base system specifications

L1/L2 networking

- Ethernet ports: Access, network, hybrid
- Link aggregation groups (LAG)
- Link Aggregation Control Protocol (LACP)
- Multi-chassis LAG (MC-LAG)
- Null, 802.1Q VLANs
- Q-in-Q encapsulation
- Configurable media access control (MAC) addresses
- Configurable MTU and jumbo frame support
- Interface statistics: Ports, service access points (SAPs), services, etc.
- Network interfaces
- Spoke Service Distribution Point (SDP) IP interfaces
- Flex PW-port: L2oGRE using IPv4 or IPv6 transport
- Flex PW-port: MPLS SDP binding
- Port cross-connect (PXC)

IPv4 and IPv6 routing protocols

- IPv4 and IPv6 forwarding
- Static routes
- Open Shortest Path First (OSPF) v2, v3
- Intermediate System to Intermediate System (IS-IS)
- Routing Information Protocol (RIP) and Routing Information Protocol next generation (RIPng)
- Border Gateway Protocol v4 (BGP4) and Multiprotocol BGP (MP-BGP)
- Address Resolution Protocol (ARP), IPv6 Neighbor Discovery (ND)
- Internet Control Message Protocol (ICMP), v6
- Equal-cost multipath (ECMP)
- Unequal-cost multipath/weighted ECMP for BGP IP routes and Interior Gateway Protocol (IGP) shortcuts over Resource Reservation Protocol - Traffic Engineering (RSVP-TE) tunnels
- Unicast Reverse Path Forwarding (URPF)
- Virtual Router Redundancy Protocol (VRRP)

IPv4 and IPv6 multicast protocols

- Base router and Virtual Private Routed Network (VPRN) support for the following protocols:
  - Internet Group Management Protocol (IGMP), v1, v2 and v3
  - Multicast Listener Discovery (MLD), v1 and vv2
  - Protocol-Independent Multicast (PIM)
  - Multicast Source Discovery Protocol (MSDP)

MPLS and segment routing

- Label Distribution Protocol (LDP) for IPv4 FECs
- Point-to-point RSVP label switched paths (LSPs)
- LDP-over-RSVP
- BGP label-unicast IPv4 (3107)
- IPv6 PE router (6PE)
- OSPFv2/IS-IS shortcuts to IPv4 prefixes (using LDP or RSVP)
- BGP shortcuts to IPv4 prefixes (using LDP, RSVP or BGP 3107)
- OSPFv2 segment routing extensions
- IS-IS segment routing extensions
- Segment Routing - Traffic Engineering (SR-TE)
- BGP segment routing policies

Layer 2 VPNs and Data Center Gateway

- E-pipe:
  - Ethernet virtual leased line (VLL) signaled by T-LDP using MPLS or GRE transport
  - Ethernet VLL signaled by BGP using MPLS or provisioned GRE SDP transport
  - Ethernet VLL using Layer 2 Tunneling Protocol, version 3 (L2TPv3) (static)
  - Ethernet VLL signaled by BGP-EVPN using MPLS
  - Static Ethernet VLL using Virtual Extensible LAN (VXLAN) IPv4 transport

- Virtual Private LAN Service (VPLS):
  - Ethernet VPLS signaled by T-LDP using MPLS or GRE transport
  - Ethernet VPLS signaled by BGP using MPLS or provisioned GRE SDP transport
  - Ethernet VPLS signaled by BGP-EVPN (Ethernet VPN) using MPLS or VXLAN transport
- Virtualized Data Center Gateway (DCGW) with Nuage Networks Virtualized Services Directory (VSD) integration, including support for fully dynamic XMPP Model
- Routed VPLS (R-VPLS)
- Resiliency:
  - Pseudowire redundancy
  - Dual-homed virtual private wire service (VPWS)/VLL
  - BGP multi-homing for VPLS
  - MC-LAG
  - Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP) and Multiple Spanning Tree Protocol (MSTP)

Layer 3 services

- Internet access (IES services)
- IPv4 and IPv6 VPNs (6VPEs)
- MPLS and GRE auto-bind and spoke SDPs
- RFC 4364 IPv4 VPNs using MPLS or GRE transport
- RFC 4659 IPv6 VPNs using MPLS or GRE transport
- IP VPN inter-AS option B
- IP-in-IP and GRE IP tunneling
- Global Routing Table (GRT) lookup and VPRN-to-GRT route leaking

Filtering, OpenFlow control plane protection

- Ingress IPv4 and IPv6 filters
- Egress IPv4 and IPv6 filters
- IP filter override for Routed VPLS (R-VPLS) services
- All IP filter match criteria as supported by 7x50 platforms:
  - Nokia 7950 Extensible Routing System (XRS)
  - Nokia 7750 SR/SR-s
- Standard actions: Forward, drop and HTTP redirect
- Conditional actions:
  - Drop-extracted-traffic (for control plane protection)
  - Drop based on packet length
  - Drop based on time-to-live (TTL)
- Ingress policy-based routing (PBR) actions:
  - Forward to next-hop
  - Forward to router (another routing instance)
  - Redirect-policy
- NAT action
- Reassemble action
- Filter logging (ingress and egress)
- Distributed CPU protection (static policers)
- IPv4 BGP flowspec
- IPv6 BGP flowspec
- OpenFlow

OAM

- Bidirectional Forwarding Detection (BFD), centralized and distributed
- SDP ping
- Virtual Extensible LAN (VXLAN) ping

Model-driven management[1]

- Configuration via model-driven (MD) interfaces:
  - NETCONF
  - MD-CLI
  - gRPC/gNMI
- State information retrieval via MD interfaces:
  - NETCONF
  - MD-CLI
  - gRPC/gNMI
- Streaming telemetry through gRPC/gNMI subscriptions; operations through NETCONF using YANG models and gNOI

Quality of Service

- Ingress pre-classification for class-aware early discard (optional)
- Ingress classification to forwarding-class based on 802.1p, Differentiated Services Code Point (DSCP), MPLS EXP or IPv4/IPv6 filter rules
- Egress re-classification
- Ingress and egress unicast policing and hierarchical policing
- Egress marking of 802.1p, DSCP or MPLS EXP
- Egress queue shaping based on configurable Peak Information Rate (PIR) and Maximum Burst Size (MBS)
- H-QoS:
  - Up to three tiers of egress user schedulers
  - Egress HQoS with queue parenting to port or user scheduler
  - Eight strict priority levels per egress user scheduler
  - Weighted round robin (WRR) scheduling in each scheduler level
- Aggregate SAP limit, including frame-based accounting
- Aggregate subscriber rate limit, including frame-based accounting

Service mirroring and Lawful Intercept

- Basic LI management infrastructure
- Ether and ip-only mirror types
- Debug mirror sources: ports
- LI mirror sources: subscribers, SAPs, spoke-SDP
- Mirror destinations: SAP, spoke-SDP
- Routable LI encapsulation (IP/User Datagram Protocol [UDP] and IP/GRE)
- Pre-NAT (private IP) and post-NAT (public IP) subscriber mirroring/LI (Note: Pre-NAT mirroring/L1 is only supported with L2-aware NAT)

For additional information about standards compliance and feature support, contact your local Nokia representative.

1 Nokia SR OS YANG model implementation on the Nokia VSR is equivalent to the implementation on the physical routers. Contact your local Nokia representative for information about the availability of specific configuration paths for model-driven management on the VSR.

Learn more

For more information about the Nokia VSR portfolio, visit the Nokia VSR web page

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.

With truly open architectures that seamlessly integrate into any ecosystem, our high-performance networks create new opportunities for monetization and scale. 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) CID182483