Nokia Virtualized Application Assurance
VSR Release 16

- Add high-performance and cloud-scalable stateful Layer 3 (L3) to Layer 7 (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 Application Assurance
The virtualized Application Assurance (vAA) is a virtualized network function (VNF) that 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.

The VSR can provide vAA functionality as a fully integrated Application Detection and Control (ADC) network function in all VSR configurations (e.g., Provider Edge, Broadband Network Gateway, Security Gateway, Residential Gateway, Wireless LAN [WLAN]), 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 VNF, 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.

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.

Overview
The virtualized Application Assurance (vAA) is a deep packet inspection (DPI) virtualized network function (VNF) delivered by the Nokia Virtualized Service Router (VSR).

The vAA functionality can be applied to any type of network traffic in residential, enterprise and wireless LAN (WLAN) environments.

The vAA 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 AA functionality delivered from a physical network function such as the Nokia 7750 Service Router or the Nokia 7450 Ethernet Service Switch as well as virtualized AA functionality (on the Nokia VSR) using the same operations, administration and maintenance protocols and management practices.

The vAA 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 vAA can optionally be deployed using OpenStack (Red Hat® OpenStack® Platform or RDO project distributions) and Nokia CloudBand.
Introducing cloud-optimized Application Assurance

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

The vAA function on the Nokia VSR is enabled by a flexible licensing scheme that allows in-service upgrades and additions of system features as service needs evolve.

The 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).

The vAA policy models can be applied network-wide or tailored and dynamically associated with specific services 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).

Application identification

- Real-time, per-flow, stateful L3-L7 packet inspection, to dynamically identify and intelligently meter traffic flows, applications and underlying protocols
- Unique identification of all enterprise, mobile and residential applications using protocol signatures in combination with IP address and ports, Uniform Resource Identifier (URI) strings, Differentiated Services Code Point (DSCP) values or traffic direction, to classify applications and detect flow performance behavior
- Full support for IPv4 and IPv6 traffic and applications
- Application detection is highly flexible, allowing in-service configuration of new application types. This is enabled by programmable application and application group definitions

Application Assurance

- Extensive per-application policy enforcement and charging with granular bandwidth shaping, policing and prioritization, defined per subscriber or per VPN site, to intelligently categorize application traffic based on policy
- Delivery of deterministic end-to-end application behavior through application performance measurement and application-based QoS, and application control by traffic rate or number of flows
- Provides L7 stateful firewall to block unsolicited traffic, with full application-level gateway support for all AA signaling protocols (for example, Session Initiation Protocol [SIP], File Transfer Protocol [FTP], Real-time Streaming Protocol [RTSP])
- Firewall support includes all features needed to provide mobile network protection on 3GPP S1-U, S1-MME and IuPS interfaces
- AA firewall filter rules provide protection for consumers and cloud infrastructure against malicious traffic such as Denial of Service (DoS) attacks
- In-browser notification (IBN) messages such as overlay images, banners or splash pages can be used for a variety of use cases. IBN is application- and content-aware, providing control over when, where and how IBN messages are delivered
- Large-scale URL filtering, parental control and web content-based classification services using an Internet Content Adaptation Protocol (ICAP) interface
- URL filtering using local lists imported in-service, used for blacklist internet filtering
- HTTP redirect with application-aware context for selective redirect use cases, including HTTP whitelisting for non-authenticated subscribers
- Transmission Control Protocol (TCP) maximum segment size adjustment to prevent packet fragmentation
Application reporting

- Per-protocol, per-application and per-application group volume statistics accounting for all subscribers and L2 and L3 VPNs (every byte, every packet, every flow for every application counted) using XML record export for volume accounting
- End-to-end application volume statistics available between specific subscribers, VPN sites and servers
- Performance reporting for TCP-based applications (including client and server side), network delay/loss/jitter, session establishment/closure delay/jitter, and client-server transaction delay/jitter
- Integrated Telchemy VQmon® passive performance measurement technology on in-service traffic for VoIP and video conference mean opinion score (MOS)-related measurements for Real-Time Transport Protocol (RTP)-based audio/video applications
- cflowd v10 Internet Protocol Flow Information Export (IPFIX) record export for application volume and performance measurements, including Domain Name Server (DNS) performance
- RADIUS accounting export of application-based charging groups for application-aware, usage-based billing plans
- Reporting on application use by device manufacturer and model as well as OS version, and reporting of top web domains visited

Technical specifications

Supported services

- ePipe Service Access Point (SAP)
- ePipe Spoke-Session Description Protocol (SDP): Multiprotocol Label Switching (MPLS) + Generic Routing Encapsulation (GRE)
- WLAN Gateway Enhanced Subscriber Management (ESM) and Distributed Subscriber Management (DSM) AA subscriber types
- Virtual Private LAN Service (VPLS) SAP and Spoke-SDP
- Internet Enhanced Service/Virtual Private Routing Network (IES/VPRN)
- IES/VPRN SAP app-profile/divert
- IES/VPRN SAP transit-ip
- IES/VPRN SAP aarp
- IES/VPRN IPSec Private SAP app-profile/divert
- IES/VPRN Enhanced Subscriber Management (ESM)
- AA tunnel support (Dual-Stack Lite, 6RD/6to4, Teredo tunneling, GRE)

Standards support

- RFC 3507, Internet Content Adaptation Protocol (ICAP)
- RFC 5102, Information Model for IP Flow Information Export
- 3GPP R11 and R12, Support for ADC rules over Gx interfaces

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

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.

© 2018 Nokia

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

Document code: SR1808028049EN (August) CID 200486