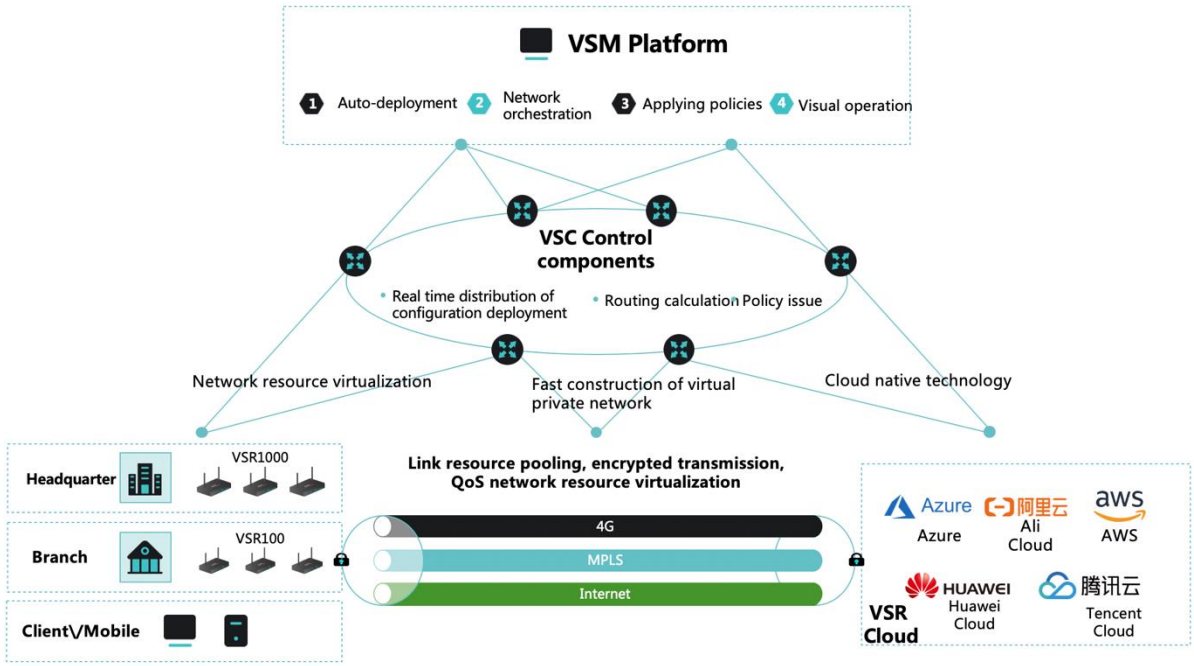
NetLinkz VSN 2.0 - Product Brief

Product Overview

The NetLinkz Virtual Security Network (VSN) platform is an enterprise-grade intelligent networking solution that allows customers of all sizes to deploy an economical SD-WAN service that is fast, reliable, elastic and secure. The VSN is a distributed software platform which runs on off the shelf commonly available hardware, that features rapid deployment at the edge and in the cloud, and offers advanced traffic management features such as Quality of Service (QoS).



A range of VSR (Virtual Security Router) edge devices are available, including virtual and mobile versions. Customers can deploy a combination of VSR edge devices to suit the traffic profile of their network and its locations.

The VSR1000 component of the VSN gives customers the opportunity to establish a self-owned global backbone network for added network security and performance, and gives them the ability to connect clouds hosted by two or more cloud-service providers to establish ultra- high-performance hybrid clouds.

Access control and monitoring are centralised in the VSM (Virtual Security Manager), giving administrators enterprise-wide network management capabilities and options for extension via comprehensive APIs.

Problems Addressed

Organisations with multiple facilities (or those that operate large collections of devices, such as the military, health service providers and IoT operators) must reconcile the following when constructing their operational networks:

- Multiple ISPs with limited or no service quality guarantees
- Public networks with no inherent mechanisms to ensure end-to-end traffic control
- Multiple access channels with different bandwidth and reliability characteristics (i.e. MPLS, Internet, LTE/4G, 5G, satellite etc.)
- A wide range of available cloud infrastructure with variable levels of access (SaaS services, cloud services and data centres)
- Large numbers of devices with varying transmission capabilities (Server, PC, Mobile, IoT device, AI node etc.)

The VSN allows customers to underpin their network operations with an intelligent networking platform that provides a secure and elastic network overlay that extends all the way to the edge of the customer's network, and offers high quality of service and infinite scalability.

How are Problems Solved

The VSN solves the operational challenges associated with public networks, heterogenous cloud infrastructure and device proliferation by separating network functions into three layers:

- **Management layer** – being the VSM, which allows for automatic deployment, network orchestration, security policy application and centralised management
- **Control layer** – being the VSR1000, which provides fast construction of virtual private networks via real-time distribution of configuration information and deployment directives, and routing calculations necessary for traffic handling
- **Data forwarding layer** – being the VSR family of edge devices, which (a) provide traffic encryption/decryption for security right to edge, (b) bond the available access channels for maximum throughput and (c) enforce quality of service policies to maximise the available bandwidth

By dividing network operations between layers, the VSN provides an intelligent platform that is efficient, feature-rich and elastic.

Features & Benefits

Ease of Deployment and Management

- The VSN is an "out-of-the-box" intelligent networking solution that does not require on-site network engineers for edge setup (zero-touch deployment)

- The VSR is a “plug-and-play” router that is shipped pre-configured and optionally with an active 3/4/5G network connection
- The VSM offers a centralised dashboard (or “single pane of glass”) through with the VSN is configured and monitored
- VSR configuration updates are pushed to the edge automatically

Intelligent, High-Performance Networking

- The VSN offers autonomous adjustment of bandwidth & smart routing to maximise network utilisation across the available transmission infrastructure
- The VSN can switch between peer-to-peer and hub-and-spoke mode when required to adapt to disruptions in provider networking infrastructure
- The VSN employs a powerful backbone over any existing network that vastly improves long-haul network performance & reliability

Security

- The VSN utilises IPSec with 256-bit encryption that protects all network transmissions from edge to edge (and to the device, via the VSR Mobile app)
- The VSN uses access control lists (ACLs) to ensure that network services are only available to authorised users
- Security policy management is centralised in the VSM and enforced at the edge

Cutting-edge Feature Set

- The VSN blends open standards with cutting-edge virtual technology, giving it a rich feature set that is ahead of the SDWAN market (VNR – multi-tenant routing, VPP, DPDK, Docker, IPV6)
- The VSN offers 5G-ready edge devices that support IoT and extends the SDWAN edge to the mobile device (via the VSR Mobile app)
- The VSN architecture employs new containerisation technology and offers APIs in all networking layers, making it more customisable than any other SDWAN solution

FAQ

Below are some responses to frequently asked questions about the VSN

QUESTION	ANSWER
Is the VSN compatible with other networking solutions?	YES – the VSN is a virtual overlay network. It is network-hardware agnostic (i.e. its operations are not influenced by the underlying network hardware) and it can operate in parallel with other SD-WANs solutions

How does the VSN security compare with other SD-WAN products?	Netlinkz security has previously won global recognition (via the 5th US Global Security Challenge in 2010 and numerous other awards, and the KPMG penetration testing and assurance in 2019) and the VSN was designed with security in mind. It combines the tried-and-tested security mechanisms (such as IPSec tunnels featuring AES 256-bit encryption, PKI for key management and TLS for HTTPS communications) with sophisticated proprietary security mechanisms such as ACLs (access control lists) and unique identity based registration/authentication for edge devices
Is the VSN all about security?	NO – while security is a key feature of the VSN, the VSN is also designed to deliver high-performance, low latency, intelligent traffic handling and network resilience
Is hardware required to run the VSN?	A range of VSR hardware is available; however, all versions of the VSR can be loaded onto a virtual machine (whether in the cloud, IDC or on-premise hypervisor) – making the VSN a hardware-optional solution
What kind of network is required for a VSN to operate?	Any IP-based network including ADSL, MPLS, 3/4/5G, cable/fibre, satellite etc.
Can a VSR utilise multiple outbound networks?	YES – a VSR can access a 3/4/5G network and a secondary network connected via ethernet
Can VSN networks be globally distributed?	YES – the VSN core switches (VSR1000s) and the virtual backbone that operates between them are designed for global distribution
Can the VSN join multiple cloud service offerings together to create hybrid clouds?	YES – once the VSR Cloud software is installed in a cloud, the resources in that cloud will available (subject to configuration by a VSN administrator) to users on the VSN. From the user's perspective, the target resource will be a VSN resource, as opposed to a resource belonging to a specific cloud

Is the VSN tied to any particular cloud service vendor?	NO – the VSR1000 and VSR Cloud can be deployed on virtually any cloud (including public cloud, proprietary IDC clouds and on-premise hypervisors)
Does the VSN only extend as far as the edge?	NO – one of the VSN's most impressive features is that it offers the VSR Mobile app, which allows an authorised VSN user's device (i.e. a Windows PC, Mac, Android phone/tablet or iOS phone/tablet) to join the VSN. This is a unique and powerful feature that makes the VSN truly unique in the SD-WAN marketplace
Does the VSN offer centralised management?	YES – the VSM (or virtual security manager) provides a "single pane of glass" through which the VSN can be monitored and managed. The VSM offers edge device metrics, network metrics, configuration management, update management, user management, notifications and alerts.
Does the VSN include visual traffic monitoring tools?	YES – the VSN includes a GUI application that plots VSN traffic against Google maps provided by the Google maps API
Can the VSN be paired with specialised systems for DDoS prevention etc.?	YES – the VSN is fully compatible with most specialised systems such as DDoS protection, next-generation firewalls and IDS/IPS (intrusion detection/prevention systems) etc.
Does the VSN feature zero-touch deployment?	YES – all VSR hardware is shipped preconfigured and VSR100 edge devices can be shipped with an active 3/4/5G connection for customers with no networking services at site. No highly skilled engineers need to be present on site. Device configuration, management and updated are achieved through a centralised dashboard (VSM), making the VSN very easy to maintain after deployment
How long do VSN deployments take?	Given the VSN's zero-touch deployment model and its ability to leverage virtual machines, rather than hardware, the VSN

	can be deployed in a fraction of the time required for most other SD-WAN solutions
Is VSN support outsourced?	NO – Netlinkz employees based in Australia provide 24/7 support for VSN customers. All support staff have intimate knowledge of the VSN architecture and features