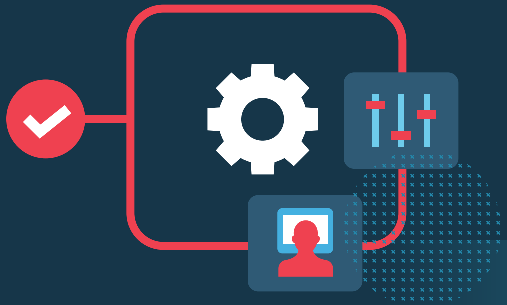
nuagenetworks
From Nokia

Virtualized Network Services

SOLUTION BRIEF



Virtualized Network Services: Transcend connectivity and empower IT with SD-WAN 2.0

The proliferation of automated and on-demand delivery of applications and services brought on by cloud computing technology has changed the way enterprises look at their wide area networks (WANs). This shift has put pressure on the rigid and manual way that traditional network WAN services have been deployed, resulting in a higher operational burden that drives up WAN OPEX while delaying time to revenue. To tackle these challenges, enterprises have deployed the first generation of automated WAN networking, called software-defined WANs (SD-WANs).

The first iteration of SD-WAN 1.0 certainly addressed the initial challenge, but the enterprise environment continued to evolve. Business applications started to proliferate, and their workloads rapidly shifted beyond the traditional boundaries of the private data center to various public clouds and began being offered in the form of various cloud services (e.g. IaaS, PaaS, SaaS). With 5G now being deployed commercially, IoT applications are adding even more strain on the network and the teams that deliver them.

First generation SD-WAN 1.0 solutions cannot solve this problem because they have primarily been relegated to solving the WAN connectivity issue and have not been built with the entire network in mind. SD-WAN 1.0 needs to evolve to empower enterprises with a sound multicloud capability as part of a comprehensive digital transformation business strategy. This strategy demands an end-to-end, scalable, secure, and flexible network that can rapidly adapt to the needs of the next generation of business applications.

SD-WAN 2.0 Highlights

- Provide an infrastructure that enables enterprises to implement their own unique multicloud strategy that intelligently spans private DCs, SaaS clouds, public clouds, and branch locations from a single governance model
- Leverage one of the world's leading routing stacks in SR OS to offer massive and proven scale across multiple tenants supporting more branches, more overlay L2/L3 VPN tunnels, with full mesh connectivity
- Apply software-defined security policies that protect laterally within the perimeter of the network while programming proactive dynamic threat responses
- Hosts, manages, and maintains third party VNFs on Nuage Networks NSG family of uCPE devices while programming service chains to ensure that each application packet flow receives the precise service treatment it needs.

© Copyright 2020 Nuage Networks

New challenges in enterprise networks

The multicloud challenge

Enterprises are now looking at their SD-WAN infrastructure for more than just WAN connectivity. They need to offer a flexible multicloud environment and unify their entire network to provide the end-to-end application visibility and control required to deliver a range of IT services, such as the flexible and automated deployment of virtualized network functions (VNFs), or to provide programmable security across the entire network. To accommodate this, they need to build a seamless "overlay" network or abstracted forwarding plane that can intelligently automate network connectivity across private data centers (DCs), public clouds, SaaS clouds, and branch locations.

Scaling the network

The scaling requirements are staggering in this new era of cloud automation. Thousands of applications, hundreds of locations, a multitude of cloud services, and distributed compute serving mobile users, IoT-enabled people, and things are creating a scaling issue that needs to be addressed. In addition, the design of an enterprise network will need to move from hub- and-spoke topology to a more efficient but scale-intensive full-mesh topology to optimize performance. Enterprises need an SD-WAN solution that is built for this level of scale.

Securing the network challenge

Cloud-based architectures have rendered traditional perimeter-based security measures insufficient to protect enterprise networks from within their perimeters. The massive volume and ephemeral nature of today's business applications create a new threat landscape that can infect enterprise networks laterally from within. Enterprises need to address these challenges by leveraging software-defined security techniques that can be designed in advance and applied to each application that traverses the network.

Virtualizing the branch

The sprawl of dedicated branch devices that support network functions such as L7 FW, WAN optimization and IPS/IDS is operationally difficult to manage and maintain and creates vendor lock-in. In the era of virtualization, enterprises are moving toward hosting these functions as a VNF hosted on a universal customer premises equipment (uCPE) platform. Transitioning to a virtualized CPE (vCPE) model will lower OPEX and CAPEX because it greatly simplifies the operational model of the branch. However, enterprises need a way to manage the onboarding and lifecycle of these VNFs in an operationally efficient manner.

Nuage NetworksTM Virtualized Network Services (VNS) and SD-WAN 2.0 address these challenges by empowering enterprise networks to:

- Enable each enterprise's unique multicloud strategy and unify their network under a single governance model with no restrictions
- Scale each enterprise network to accommodate the new era of micro-services, 5G, and IoT-driven business applications
- Secure the entire enterprise network from within by leveraging application-level visibility and control, while protecting the network with software-defined security policies
- Enable the management and orchestration of VNFs on uCPE platforms while proactively programming each application's path in the network across these service

Virtualized Network Services

Securing the network challenge

Nuage Networks VNS is an industry-leading SD-WAN solution. It automates the provisioning, configuration, and management of WAN connections to provide the optimal quality of service (QoS) at the lowest cost while meeting strict business policy and security requirements for each application. VNS can provide this policy-based automation while seamlessly connecting WAN branch sites to on-premises private data centers, public clouds, and provider-managed VPN networks.

VNS relies on a central policy repository to define business- and application-specific rules that dynamically optimize WAN links and remote branch appliances or devices. With VNS, the SD-WAN enabled network is dynamically optimized to route traffic governed by specific application policies or by the most cost-effective network path to meet each application's performance criteria. For example, VNS can immediately drive down high WAN costs by leveraging commodity internet broadband, LTE, or other low-cost WAN uplinks whenever possible for certain applications. VNS also can leverage LTE transport as a back-up transport link for application resiliency programmed on a per-application basis.

VNS reduces remote hardware and management costs because it has no requirement for expensive proprietary branch hardware. With automation capabilities from VNS, the tedious, time-intensive tasks associated with setting up new sites or VPN service connectivity can be reduced from several weeks to a few minutes. VNS gives enterprises greater flexibility to customize their VPN service on demand, while eliminating IT overhead at remote sites.

Addressing the new enterprise challenges with SD-WAN 2.0

The SD-WAN 2.0 capabilities of VNS are uniquely equipped to handle all of the new challenges in enterprise networks. Figure 1 illustrates some of the key attributes of SD-WAN 2.0.

SD-WAN 2.0 is a multi-tenant platform that is built from a single governance model that provides application-level visibility and control of private data centers, branch locations, and cloud services across any WAN transport service. It extends policy control across the entire network by enabling integration into data centers and public clouds. It also leverages special routing functions to create a seamless underlay network from otherwise heterogeneous WAN transport services. The platform provides an elegant integration into public clouds, creating a "branch in the cloud" that is considered by the system as another branch to which policies can be applied. With this infrastructure in place, enterprises can implement any multicloud strategy, count on enjoying tremendous scale, and provide comprehensive software-defined security while virtualizing their network for the future.

Key aspects of SD-WAN 2.0

Enabling multicloud and unifying the enterprise network with SD-WAN 2.0

Enterprises need automated connectivity to unify the enterprise WAN. However, the WAN underlay network can be complex, disconnected, and diverse, especially in larger multi-national enterprises. SD-WAN 2.0 hides this complexity and creates a seamless end-to-end WAN that connects private data centers, branch locations, and public cloud services so there are no restrictions or obstacles when the enterprise IT manager programs the network. As shown in Figure 2, SD-WAN 2.0 provides specific integration in various points in the network, including the heterogeneous WAN underlay, the data center, brownfield non-SD-WAN parts of the network, extranets, and public cloud services.

Connecting heterogeneous WAN underlay segments

In many cases, enterprises have deployed IP/MPLS, internet broadband, and even mobile (3G/LTE) WAN underlay transport services. For larger multi-national enterprises, these services are often delivered by various WAN transport providers where

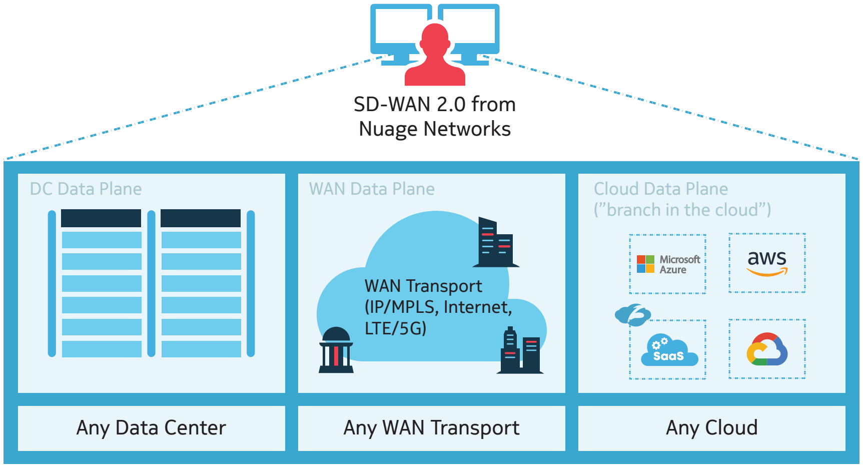


FIGURE 1. SD-WAN 2.0 – Key attributes

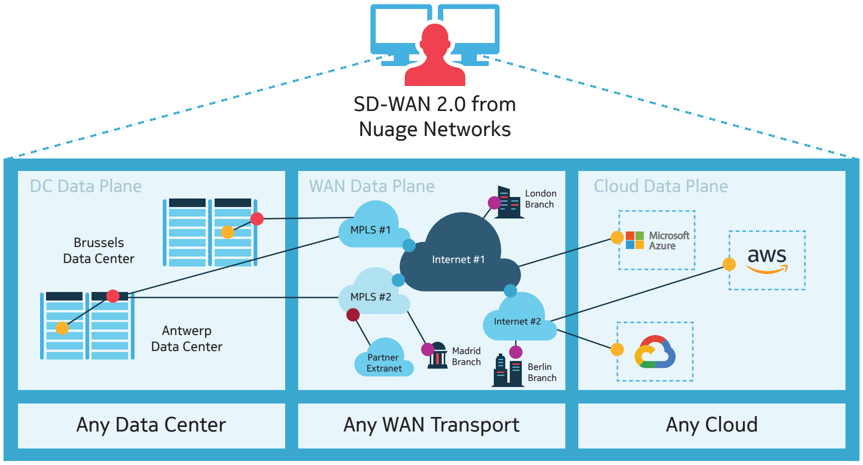


FIGURE 2. Creating a seamless underlay network with SD-WAN 2.0

● NSG - Underlay border router ● NSG - Virtualized ● NSG - Border router ● NSG - uCPE ● NSG - Underlay border router

© Copyright 2020 Nuage Networks

each region and country could look different in terms of underlay transport infrastructure and providers. Although the SD-WAN service should be agnostic to the WAN underlay transport type, there are cases where underlay connectivity between specific sites is from disjointed or heterogeneous transport WANs (e.g. internet broadband or IP/MPLS) that do not provide the required underlay connectivity.

In these cases, SD-WAN 2.0 provides a managed policy-controlled function at the boundary of the disjointed or heterogeneous underlays that joins both segments to make the underlay whole. This is the Network Services Gateway (NSG) – Underlay Border Router (UBR) routing function. As shown in Figure 2, the NSG-UBR is located at the boundary of the heterogeneous transport segments. Its function is to stitch them together to create a seamless whole. The result is a boundaryless SD-WAN service that spans diverse geographies and heterogeneous WAN transport services.

Brownfield support for non-SD-WAN parts of the network

For many large enterprises, it is crucial for SD-WAN deployments in new locations to support connectivity to legacy IP/ MPLS connected sites. With SD-WAN 2.0 integration, both new SD-WAN overlay connections and existing non-SD-WAN IP/ MPLS transport links will be compatible, and both parts of the network will continue to provide connectivity. In general, this means that SD-WAN 2.0 provides an intelligent and automated breakout or handover capability to legacy Provider Edge (PE) underlay routers. This capability is also provided by the NSG-UBR deployed at the boundary of the existing IP/MPLS part of the network.

Extranet support

This capability can be extended to safely connect to third-party or partner extranets. Extranets connect portions of a partner's intranet to the enterprise and are very tightly designed and controlled. Extranet rules are programmed in the underlay network. As SD-WAN 2.0 is deployed, it will need to be compatible with the configuration and rules of legacy extranets. For example, if the enterprise network shares IP addresses with the connected extranet, SD-WAN 2.0 will have to support bidirectional network address translation (NAT) to continue to allow bidirectional communication between entities from each network. This capability is provided by the NSG-UBR.

Extranet support

Traditional SD-WAN 1.0 deployments and software-defined networking (SDN) data center solutions have typically been treated as two separate silos. This has required manual stitching of their respective underlay boundaries and manual connecting of their separate SD-WAN/SDN policy, control and data planes. Most SD-WAN solutions deliver traffic from the branches to a gateway in the data center and rely on a different solution to carry the traffic within the data center to the proper workload. This breaks the end-to-end automation and security paradigm and adds much more complexity.

To offer true end-to-end connectivity, the SD-WAN solution must provide an interworking function with full automation that does not require stitching and manual configuration across two different solutions. This function must ensure seamless and boundaryless connectivity from users in branches all the way to applications within the data center. In the simplest example, enterprises can integrate into a private data center using an NSG – Border Router (BR) at the boundary between the data center and the WAN. Enterprises can also extend SD-WAN 2.0 directly to a host or specific set of hosts in the data center using a Virtualized NSG (NSG-v) deployed in the virtualized compute environment as a
virtual machine (VM).

Integration with public clouds

The industry is witnessing greater demand for public cloud services, creating a need for enterprises to uniquely integrate into any public cloud to extend their SD-WAN reach. Unfortunately, many SD-WAN 1.0 integrations are customized and complex, and reduce workload portability while creating a public cloud vendor lock-in. SD-WAN 2.0's approach is to integrate the NSG-v directly into the front-end of the allocated set of compute resources (e.g. virtual public cloud). This avoids complex proprietary API integration while providing a standard policy-based connection that is less dependent of the selected public cloud service. With this approach, the public cloud service is managed as another branch site and will benefit from the same single point of visibility and control, like the rest of the network.

Proven tremendous scale with SD-WAN 2.0

Nuage Networks Virtualized Services Platform (VSP) and its SD-WAN 2.0 capabilities were built from the ground up using the Service Router Operating System (SR OS). This proven OS is deployed in all of the top 50 routing networks worldwide measured by routing spend. It is deployed in more than 650 enterprise networks and more than 700 service provider networks. It is also the OS for more than 900,000 routers shipped to date.

One of the hallmarks of SR OS is performance consistency. Its performance does not deteriorate as features are turned on and scale requirements increase. The independent European Advanced Networking Test Center (EANTC) recently conducted a test of SD-WAN 2.0's scale. Key test results included:

- Support for scaling up to 4,000 branches
- Support for up to 396,000 overlay tunnels
- Support for 129,240 full mesh overlay tunnels per tenant
- Management of up to 40 tenants in a multi-tenant premise
- The full test results can be downloaded here

EANTC summarized the tests this way:
"EANTC validated the scalability, functional capabilities, reliability, and manageability of the Nuage Networks SD-WAN 2.0 solution extensively." [1]

Secure the network from end to end with SD-WAN 2.0

Enterprises today have thousands of users in hundreds of global sites running tens of thousands of applications that access workloads across private data centers, central offices, public clouds, and branches. This application and workload diversity is proliferating, which is dramatically increasing an enterprise's attack surface and making network security a massive undertaking. Traditional perimeter-based approaches are no longer enough to protect laterally within the network.

With SD-WAN 2.0's infrastructure in place, IT managers are already in a good position to address these new security challenges. Having a seamless end-to-end network managed by a single policy and network governance model is an essential starting point. With SD-WAN 2.0, IT managers can address these new emerging security threats from their network in three ways:

1. Understand the network and the applications that flow through them using real time traffic flow visibility.
2. Protect the network with software-defined security measures.
3. Resolve any network issues with pre-programmed dynamic threat responses.

As shown in Figure 3, these security measures will apply to the entire network, from data centers operating a hybrid environment with multiple hypervisors, containers, and bare metal servers across the WAN to branches and public cloud services.

Real-time application traffic flow visibility

The SD-WAN 2.0 platform provides enterprise IT managers with comprehensive real-time visibility into all application traffic flowing across the network, including the ability to collect and display per-flow, end-to-end traffic patterns with source, destination, traffic type and rates. The platform allows IT managers to use this information to automatically create security rules based on real-time traffic and current business goals.

By using application-based traffic flow data, IT managers can visualize service tiers (e.g. web server, database, video streaming, optimization), workloads (e.g. VM #1, VM #2, container #1) and type (TCP, UDP) that apply to each application flow, as well as traffic patterns between each tier. This knowledge provides insight into what applications and resources are used and how to specifically segment the network for each application to determine which automated security policies should be applied.

Understanding this application-level traffic information is important for validating compliance requirements. Specific network and security requirements may need to be met to abide by a corporate information security policy. SD-WAN 2.0

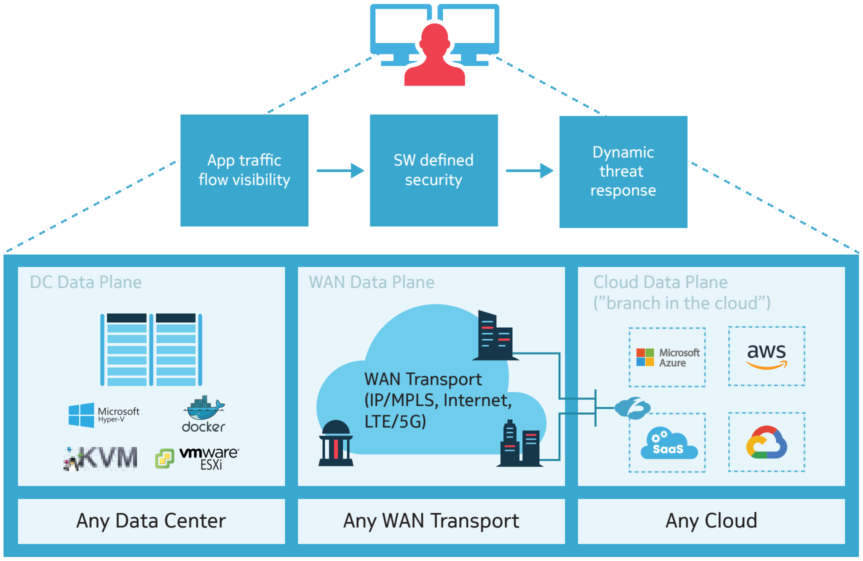


FIGURE 3. Software-defined security with SD-WAN 2.0

[1] EANTC Independent Test Report, Nuage Networks SD-WAN 2.0 solution, September 2018

will tighten security for the entire enterprise network, making compliance validation more precise and highly automated.

Software-defined security

Modern attacks seek vulnerabilities to enter the network and move from east to west within the perimeter to target high-value targets. A network that extends beyond the data center into the WAN connecting to the branches and public clouds demands intra-perimeter security measures. Automation through software-defined security is essential to scale across the tens of thousands of business applications within this perimeter. These new software-defined measures are required to supplement traditional perimeter-based security and ward off lateral attacks.

Leveraging comprehensive flow visibility from SD-WAN 2.0, IT managers are better equipped to segment the network for each application or group of applications in advance, assigning service tiers and supporting workloads that each application uses. With per-application or per-group segmentation, IT managers can create policies to isolate application-specific traffic and all associated network resources within a dedicated and secure logical domain. To succeed, this approach must be supported across all locations and workloads. As network resources change throughout the lifecycle of the application, the security measures will dynamically follow, eliminating the requirement for any custom or manual security configuration. This technique, known as micro-segmentation, is commonly limited to the WAN in SD-WAN 1.0 deployments.

SD-WAN 2.0 offers end-to-end micro-segmentation that spans all remote locations, as well as public data centers and private clouds. With this capability, SD-WAN 2.0 will prevent lateral attacks originating in remote locations from ever reaching critical assets inside the data center, something that traditional SD-WAN 1.0 deployments fail to do.

In addition to end-to-end micro-segmentation, SD-WAN 2.0 provides the ability to create and automate a holistic security approach that includes integrating with third-party next-generation firewalls (NGFWs) at specific branches or connecting with other security functions anywhere else in the network (e.g. SaaS- based security services). With SD-WAN 2.0's service chaining capability, each application flow will receive the security treatment it requires.

As an example of integration with third-party security functions, Nuage Networks has partnered with Zscaler to secure internet-destined traffic. Any traffic that breaks out to the internet can be routed directly to the Zscaler cloud. There, the entire security stack as a cloud service can be programmed to secure internet traffic and deliver a fast user experience — without backhauling and without deploying stacks of security appliances at each location. This use case is depicted in Figure 3.

Dynamic threat response

SD-WAN 2.0 delivers the ability to define and implement dynamic threat responses by responding to suspicious traffic flows in real-time without user intervention.
Some examples include:

- Real-time alerts that inform the IT manager of suspicious activity for each application, down to the service tier level of granularity. For example, the manager may get an alert when a certain TCP port on a virtual database (DB) server starts receiving an unexpected amount of traffic from a new source
- Automatically redirecting or copying suspicious traffic to an Intrusion Prevention System (IPS) or NGFW for a more in-depth analysis
- Quarantining or blocking suspicious traffic sources automatically upon detection

Enable the virtualization of the network with SD-WAN 2.0

A shift is occurring in the industry to replace local proprietary CPE appliances with virtualized instantiations (or VNFs) of them. These vCPEs and are being hosted on uCPE platforms. uCPEs are general-purpose, open-standards, and commonly x86-based platforms that can be purchased and maintained at much lower costs. By hosting multiple VNFs on a local uCPE, enterprises benefit from increased agility, increased operational efficiency, better overall quality of service, and lower CAPEX and OPEX.

SD-WAN 2.0 satisfies this market shift by offering a comprehensive range of NSGs that represent uCPE platforms that can be selected based on throughput and port requirements and can host VNFs from third-party vendors. The IT manager can use the existing SD-WAN 2.0 infrastructure to optimize the operational model of deploying VNFs on a uCPE platform by providing preconfigured management and policy functions such as:

- A comprehensive catalog of VNFs that are available to each enterprise, user and branch
- Lightweight lifecycle management of each VNF, with the ability to create, bootstrap, delete, and upgrade each one
- Centralized multi-tenant policy control, which enables service providers to configure each VNF, defining which branch site, enterprises and users have access to them
- Offer traffic policies and service chains to define what applications should be treated with what VNF and how each packet flow traverses the network.

The SD-WAN infrastructure can be pre-integrated with all peripheral systems that are needed to support these uCPE-hosted VNFs. This approach includes integration with the overall orchestration system as well as the NFV management and orchestration (MANO) environment.

A holistic approach to virtualization

With full visibility and control of the entire network and its resources, SD-WAN 2.0 can provide a holistic and flexible approach to connect each application flow with the specific VNFs they need, regardless of where the VNFs are hosted. Some VNFs can be hosted on the uCPE platform, including WAN optimization, next-generation firewall, and intrusion detection and prevention systems (IDS/IPS). Others are embedded as features in the SD-WAN 2.0 software, including Layer 7 URL filtering, Dynamic Host Configuration Protocol (DHCP), IPSec, and network address translation/port address translation (NAT/PAT). Other VNFs are deployed across the entire enterprise network in data centers or public clouds.

With SD-WAN 2.0, the IT manager can program a service chain to ensure that the relevant application traverses through the correct set of services. Figure 4 depicts a service chain programmed to ensure that the traffic flow goes through two service functions from a private data center, one from a public cloud and two within the NSG uCPE platform itself, before ending in the branch LAN to a user.

VNS and SD-WAN 2.0 product architecture

Figure 5 depicts the overall product architecture of VNS and SD-WAN 2.0. Nuage Networks VSP is the only platform that enables both VNS and Virtualized Cloud Services (VCS). VCS is the SDN networking framework within the data center environment.

Management plane functions

The Virtualized Services Directory (VSD) is a programmable policy and analytics engine. It provides a flexible network policy framework that enables the IT manager to define, apply, and enforce business policies across the network service in a user- friendly manner.

The VSD contains a network service directory that supports role-based administration of network resources. It enables centralized management of network configuration – including moves, adds, and changes – using an intuitive graphical user interface.

With VSD, service providers and enterprises can centrally view and change the running policies on their network service, including deployment of new policies on a single site, multiple sites, or a network-wide basis. The VSD is also the network traffic collection point where site-specific and service-wide trending reports are available. To maintain the integrity of the service, the VSD allows the definition of sophisticated rules such as collection frequencies, rolling averages and samples, and Threshold Crossing Alerts (TCAs) to provide access to current and historic network performance information. It aggregates statistics over hours, days, and months and stores them using an Elasticsearch database to facilitate data mining and performance reporting.

Information security and compliance functions are also completed through the VSD. This enables enterprises to reduce the overhead required to meet certain network compliance and auditing standards and comply with industry regulations, such as the Sarbanes-Oxley Act.
Network functions for the service are selected using the VSD's Network Functions Store. This store provides a comprehensive set of common network functions, such as

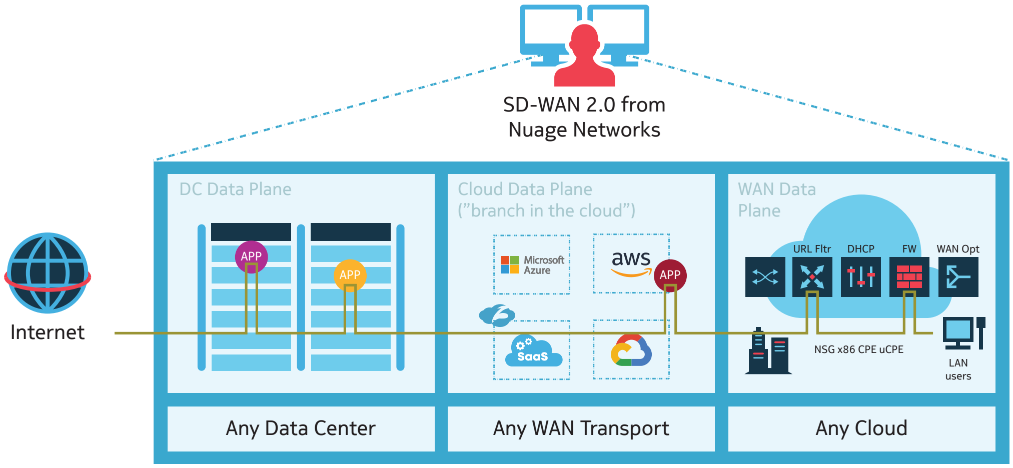


FIGURE 4. Service chaining across multiple VNFs with SD-WAN 2.0

Layer 4 stateful firewalling, service chaining, IPSec, NAT/PAT, business intelligence, load balancing, IP address management, and domain name services that can be inserted directly into the network service as tiered service options. The VSD also supports VNF onboarding, repository management and lightweight VNF lifecycle management, complementing the ability of NSGs to host third-party VNFs. This reduces the requirement for dedicated network elements to be deployed at remote locations greatly simplifying the operation model for the enterprise.

VSD supports a northbound RESTful API for all VSD functions to allow for full integration with cloud management systems (CMSs). It can be deployed as a standalone or clustered solution, depending on scaling and resiliency needs.

The VSD also includes an SD-WAN customer portal. This secure, multi-tenant, web-based application can be used for self-service management of enterprise SD-WAN networks for the VNS SD-WAN solution. The portal includes separate dashboard views for enterprise end users, which are based on customizable widgets. For in-depth analysis and troubleshooting, the portal provides a reporting engine that can generate reports on traffic, application discovery, applications' SLA violations, network performance and security auditing.

The SD-WAN customer portal offers easy-to-consume workflows for full lifecycle management of Layer 2/Layer 3 VPNs and branches. For service providers, the portal provides customer profile management. Service providers or customer administrators can create fine-grained access control in accordance with an organization's role-based access control (RBAC) strategy.

Based on AngularJS, the portal interface offers flexibility to match service provider branding requirements, including color themes and logos. Multilingual support is available and can be set on a per-user basis.

Control plane functions

The Virtualized Services Controller (VSC) is the industry's most powerful SDN controller. It functions as a centralized and robust network control plane for the network services, maintaining a full view of the network and service topologies. The VSC is built on the SR OS and benefits from its performance, robustness, and scale. Through the VSC, virtual routing and switching constructs are established to program the network-forwarding plane using the OpenFlowTM protocol. Multiple VSC instances can be federated within and across the network by leveraging the Multiprotocol Border Gateway Protocol (MP-BGP), a proven and highly scalable network technology that allows the network service to grow with the requirements of the business.

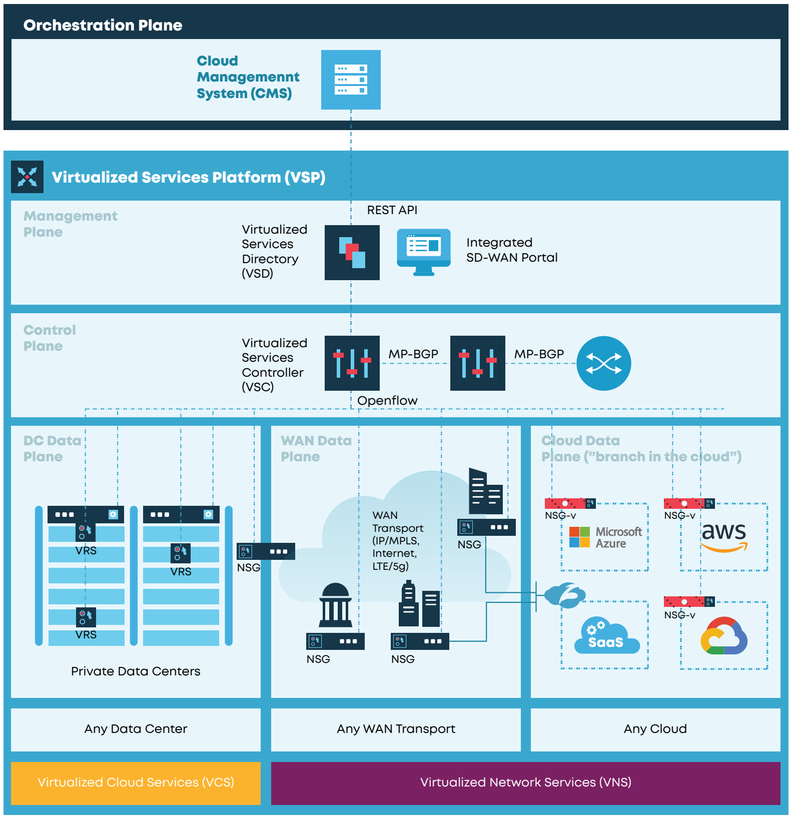

Orchestration Plane
Cloud Managemennt System (CMS)
Virtualized Services Platform (VSP)
Management Plane
REST API
Virtualized Services Directory (VSD)
Integrated SD-WAN Portal
Control Plane
Virtualized Services Controller (VSC)
MP-BGP
MP-BGP
Openflow
DC Data Plane
VRS
VRS
VRS
NSG
Private Data Centers
WAN Data Plane
WAN Transport (IP/MPLS, Internet, LTE/5g)
NSG
NSG
NSG
Cloud Data Plane ("branch in the cloud")
NSG-v
NSG-v
NSG-v
Microsoft Azure
aws
SaaS
Any Data Center
Any WAN Transport
Any Cloud
Virtualized Cloud Services (VCS)
Virtualized Network Services (VNS)

FIGURE 5. Product architecture of VNS and SD-WAN 2.0

Data plane functions

The NSG constitutes the network-forwarding plane for VNS and SD-WAN 2.0. It encapsulates data traffic, enforces Layer 2 to Layer 4 network policies, and establishes Layer 2 or Layer 3 overlay VPNs as defined by the VSD. The NSG also has form factors that support built-in Wi-Fi access and LTE uplink support. On the NSG, advanced services can be turned on, including network functions such as load balancing, service chaining, business intelligence, and NAT/PAT. Inherent security features also can be enabled, including IPSec tunnels, Layer 4 and Layer 7 stateful firewalls, and Layer 7 URL filtering. The NSG also supports VMs and container VNFs, complementing the VSD's support for VNF onboarding, repository management, and lightweight VNF lifecycle management. These services can be applied to the NSGs centrally, on a service-wide basis, or based on a location-specific deployment model.

Deployment of the NSG utilizes an automated bootstrapping process that includes several multi-factor authentication options. The automated nature of this bootstrap function reduces the requirement for specialist networking resources at remote locations. In most cases, the customer's branch staff can unbox and plug in the NSG themselves. This lowers the cost of service deployment and greatly reduces the requirement for truck rolls.

The NSG family of uCPE platforms offers support for various hardware variants (NSG-X, NSG-X200, NSG-E200/300 series, NSG-C) that accommodate a range of throughput options up to 10 Gbps. The NSG family also offers a virtualized software image deployment option (NSG-v) that provides maximum flexibility to meet the diverse throughput, network interface, and network functionality requirements of each specific branch location. The NSG-v can be deployed on any x86-based virtualized compute platforms that enterprises may have at their sites. It can also be run on Nuage Networks-recommended commercial off-the-shelf, x86-based network devices procured by customers' own channels. The NSG-v software is used to integrate into public cloud services.

A specialized version of the NSG called the NSG-BR is a software function that typically acts as an overlay network gateway between the on-premises data center or cloud network and the WAN. Traditional SD-WAN and DC SDN solutions treat the DC and WAN as two network silos that require manual stitching of policy, control, and the data plane. With the NSG-BR deployed at the data center boundary, these two silos are seamless. Another specialized version called the NSG-UBR enables seamless connectivity between NSGs in disjointed underlay networks. With the NSG-UBR, a single VNS or SD-WAN 2.0 domain can span multiple heterogeneous underlay transport networks without having to link the domains.

The Virtual Routing and Switching (VRS) module serves as a virtual endpoint for automated network services in a virtualized data center environment. It detects changes in the compute environment as they occur and instantaneously triggers policy- based responses to ensure that the network connectivity needs of applications are met.

Summary

SD-WAN has lived up to its promise of automating the enterprise WAN to provide operational and agility benefits. But an era shaped by the cloud and rapidly shifting business applications and requirements demands more than an automated WAN connectivity model. Enterprises need to transcend connectivity alone. IT departments need to be empowered to automate and optimize end-to-end capabilities like security, or virtualization from a single governance model.

This is where SD-WAN 2.0 comes in. It was built to unify the enterprise network from end to end while offering a holistic scope of visibility and control to program the entire network to dramatically improve operations and service agility. The future is rapidly changing, and it is difficult to predict the future needs of enterprise networks as 5G, IoT, AI and other technologies enter maturity. With SD-WAN 2.0 in place, enterprises can rely on an open and flexible infrastructure that has been proven to adapt to future business needs.

nuagenetworks
From Nokia

www.nuagenetworks.net Nuage Networks and the Nuage Networks logo are trademarks of the Nokia group of companies. 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