NFV SD-WAN package

A paradigm change in WAN connectivity

As enterprise applications increasingly migrate to the cloud and demand for higher data capacity continues to rise, enterprises are striving to boost their wide area networks (WAN). Specifically, they're after greater agility, flexibility, scalability, reliability and higher performance. And as always, the challenge is accompanied by the ever-present battle to keep costs down.

End-user experience and satisfaction are directly related to the network's responsiveness. For this reason, in the quest to keep end-users happy, IT managers need to be constantly concerned with ensuring consistent application performance, latency, packet loss, and jitter.

SD-WAN (software-defined WAN) has emerged as the most successful application of software-defined networking (SDN) to date. It's the leading solution that balances the cost benefits of public internet with the performance of MPLS and the agility of cloud-based service. Firstly, this is because SD-WAN transport independence connections are used to securely connect enterprise networks, branches and data centers to achieve faster, reliable and uninterrupted network connections at the lowest possible cost. Secondly, it enables IT managers to dynamically distribute traffic across multiple WAN transport types (MPLS, internet, 4G/LTE, etc.) based on application policies and business requirements.

In addition, by rapidly responding to changing business and usage needs, SD-WAN enables organizations to dramatically increase WAN performance and security, while improving network agility – and do so without the budget burdens of traditional WAN solutions.

Amdocs named a Leader in Gartner's 2019 Magic Quadrant for Operation Support Systems. Gartner recognized Amdocs for its completeness of vision and ability to execute.

Amdocs SD-WAN package solution allow CSPs to launch managed SD-WAN services in just 3 months with low investment and risk, and improve operational efficiency by 70% thanks to service-orchestration automation.

The opportunity for CSPs

SD-WAN's ability to leverage inexpensive broadband internet bandwidth poses a threat to CSPs' traditional WAN services (such as MPLS), as well as their revenue from existing managed services. Indeed, there is a very large variety of SD-WAN options available to enterprise customers to choose from. While some opt for a DIY (do-it-yourself) approach, others turn to OTT (over-the-top) SD-WAN providers. Nevertheless, for many business customers, the business case for managing and administering many ISPs and OTT providers in order to ensure high WAN availability is questionable. This is because typically, such organizations lack the technical, personnel and capital resources to implement significant WAN upgrades and would prefer to benefit from a managed SD-WAN service offered by CSPs.

Increasingly, CSPs are looking to leverage SD-WAN as an opportunity to increase revenue by growing their variety of on-demand Network as a Service offering and upselling new software-defined network services to existing and new customers. The drawback however, is that they are missing revenue opportunities due to the inability to bring services to the market at the necessary speed. In most cases, the business enablement system's awareness of network capabilities and resources is wanting, while a lack of integration between the network and BSS makes new service introduction a very complex and manual process that could last months. Other major challenges include an increasingly competitive environment and an increase in user sophistication and demands.

CSPs are responding to these challenges by turning their focus to customer experience. Common strategies include employing digital technologies and developing capabilities to provide integrated, automated and orchestrated on-demand programable connectivity and value-added services which can be ordered from a digital marketplace for faster time to market, increased efficiency and a transformed customer experience.

The implication is that to be successful, the networks of tomorrow must be fully aligned with both CSPs' business requirements and strategy, while maintaining the ability to respond rapidly to changing and evolving business customers needs.

SD-WAN security

SD-WAN provides secure, IP-based virtual overlay networks that typically utilize IPsec tunnels over internet or MPLS underlay networks. Many SD-WAN vendors are currently undergoing a process to improve their security capabilities with advanced built-in security features that will meet the needs of some of their business customers. However other business customers may still prefer security solutions delivered by specialty security solution vendors. While SD-WAN embedded security capabilities are similar to those supported by current routers, several other advanced features are not supported by the majority of SD-WAN products. Examples include intrusion prevention systems (IPS), content-specific controls, URL filtering and anti-malware protection. The implications for business customers and enterprises with high-security needs will be to opt for an NGFW (Next Generation Firewall), sourced from a security-specialist vendor.

The above explains why security integration capabilities are becoming an important differentiator, as well as playing a key role in the managed SD-WAN service provider selection process. Other security considerations for business customers include DDoS mitigation and session border controllers.

CSPs are looking to offer business customers a variety of differentiated SD-WAN services that are complement with value-added services (VAS) and advanced security features enabled by best-of-breed NGFW platforms. To achieve this, NGFWs and VAS VNFs need to be deployed in accordance with performance, business requirements and cost perspectives. The optimal path to achieving this comes by combining SD-WAN with both NFV-based virtual functions and existing underlay WAN resources.

Breaking the silos of legacy network management

SD-WAN introduces a variety of deployment scenarios and solution architectures. For example, SD-WAN Edge appliances can be deployed at the customer premises, the data center or in the cloud (CSP or public). To provide additional security and VAS on top of SD-WAN connectivity, VNFs are deployed at the customer premises, the service provider PoP, data center or in the public cloud (e.g. AWS). But this requires that network and compute resources be managed on multiple, disparate locations, data centers, networks and cloud domains. This is because each underlying infrastructure domain represents a silo that uses its own technology and is often managed by different service provider entities.

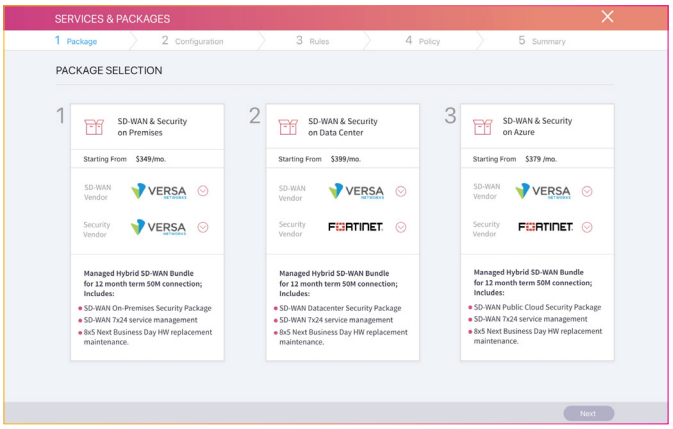
Such complexity is overcome by introducing multi-domain, multi-vendor policy-driven orchestration. Such a strategy eliminates silos by working across all technologies (physical and virtual), while spinning up VNFs directly on the relevant location (customer premise or data center), regardless of topology, application requirement or vendor. An additional benefit is that service orchestration creates an abstraction layer that hides the details and complexity of both the underlayer infrastructure and individual SD-WAN platforms. Importantly, such a strategy also prevents creation of new operational silos for different SD-WAN platforms, while reducing complexity of integrating SD-WAN services with the back-end business support systems.

However, as part of their focus on improving their managed SD-WAN services value proposition, CSPs need to also work towards achieving a number of complementary goals. These include improving the overall deployment experience, improving orchestration and automation capabilities, ensuring integration with security technologies and enhancing application visibility for customers.

The digital enterprise customer

The evolution of the way business customers consume services has created expectations for full visibility of consumed and ordered services in real time. For CSPs, this means that the ability to provide self-control, flexibility, fast processes and easy-to-use and intuitive user experience design has become essential.

The move to virtualization in networks enables this. Network functions virtualization (NFV) introduces a new way to deploy and operate networks with greater flexibility and agility, real-time granularity in traffic management and fast service creation. But for CSPs to benefit from this agility and flexibility – and achieve rapid time to market – it requires them to create a harmonized, SLA-aware platform capable of managing network service and resources scaling in real time. This is achieved by tightly integrating service catalog, customer management, ordering, service orchestration, service policy and assurance systems.

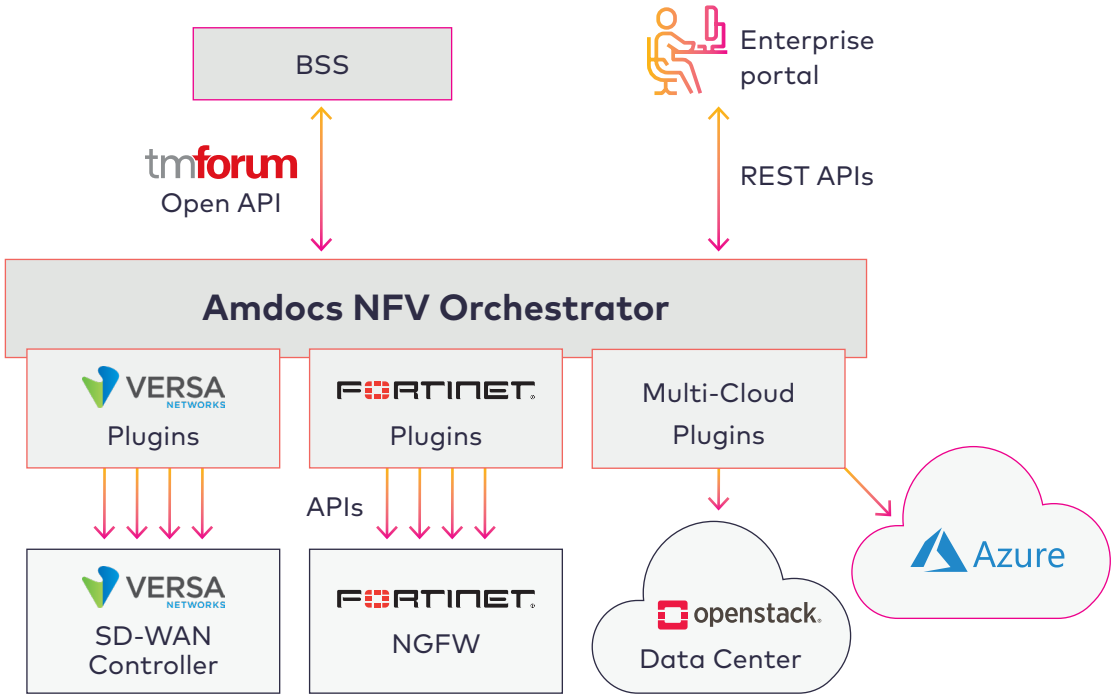


Business customers are looking for an instantaneous service ordering and controls experience. To meet this demand, service providers should enable their business customers to order on-demand services from a digital marketplace, provision, update and monitor their network services and value-added services using a self-service portal. With a few clicks on the mouse an enterprise network administrator should be able to place orders that are delivered in minutes, not months. The portal is integrated with CRM and ordering systems, and eventually with the end-to-end service orchestration that manages fulfillment of SD-WAN and other NaaS service orders and service change/modification requests that were initiated by the customer via the portal.

Amdocs' NFV SD-WAN package solution

Amdocs NFV SD-WAN package enable CSPs to deliver managed SD-WAN services, with the benefits of NFV/SDN and service automation. Our experience in SD-WAN projects has enabled us to create a ready-to-deploy, multi-vendor and multi-domain pre-integrated orchestration solution that accelerates and simplifies the journey for CSPs. This empowers them to offer and monetize managed SD-WAN and VAS services with low investment and risk.

Amdocs NFV SD-WAN package orchestrator configures and manages the end-to-end SD-WAN managed service between SD-WAN edges and SD-WAN gateways over one or more underlay WANs (e.g., internet and MPLS). It also enables automation of the managed SD-WAN service lifecycle, which includes service fulfillment, performance, control, assurance, usage, analytics, security and policy. In addition, it provides an open and extensible platform that reduces the complexity and cost associated with developing and deploying services across multiple vendor, technology and network domains.



To control southbound SD-WAN, security and data center systems, Amdocs' NFV SD-WAN package solution utilizes pre-integrated plugins. At the same time, TMF open APIs are used northbound towards the BSS, and in particular, the ordering system, thereby maximizing the solution's openness and interoperability for seamlessly integrating multiple SD-WAN solutions with existing OSS/BSS platforms.

The solution also leverages a vendor-agnostic service model for composing SD-WAN service connections, VNF service chaining and all network resources required to operate the service. The result is unmatched flexibility, agility and cost savings when operating managed SD-WAN services.

Moreover, a service order decomposition function decomposes orders into service items used by the NFV orchestrator, which then utilizes the plugin interfaces to communicate with the SD-WAN service building blocks, and instantiates the resources and network connections needed for service order fulfillment. The Amdocs NFV SD-WAN package orchestrator constantly monitors SD-WAN service performance throughout, according to the predefined policy, thereby assuring its availability and providing end-to-end service visibility.

Ready for the future

Amdocs' NFV SD-WAN package solution embraces Amdocs' microservices architecture, deployment and best practices such as DevOps and CI/CD. The package software comprises granular, value-based business function and process domains packed into containers to enable agility, scalability and always-on carrier grade availability. Because it uses microservices, where each microservice constitutes an autonomous functionality and DevOps approach, it enables CSPs to rapidly update their systems to support new SD-WAN, security and VNFs plugins in order to enhance their service offering. It allows services to be released in short cycles, with development and test taking several days as opposed to months, thereby accelerating time to market and providing complete transparency to existing customers without impacting the service.

The solution is aligned with the MEF (Metro Ethernet Forum) SD-WAN Service Attributes and Service Definitions technical specification, with the purpose of simplifying integration of multiple SD-WAN solutions into complex multi-technology domain environments using the same SD-WAN lifecycle service orchestration and open APIs.

Customers who start modernizing their offering for business customers using Amdocs pre-integrated NFV SD-WAN package could scale and expand it into Amdocs' modular and programmable Network-as-a-Service (NaaS) solution. Amdocs NaaS solution enables service providers to rapidly design, deploy and monetize on-demand NaaS offerings beyond SD-WAN for their B2B customers, combining virtualized network infrastructure and services with cloud and business applications.

Amdocs NFV powered by ONAP (Open Network Automation Platform) is the industry's first software and services portfolio to leverage the Linux Foundation's ONAP platform, enabling service providers to accelerate network functions virtualization (NFV) and software-defined network (SDN) service innovation to reap the operational benefits of virtualization.

Versa Networks Secure Cloud IP Platform SD-WAN

Versa Networks Secure Cloud IP Platform is a cloud-native multi-tenant software platform that delivers software-defined Layer 3 networking to Layer 7 NSS Recommended security services with full programmability and automation. The Versa software platform enables partners and customers to deliver managed SD-WAN, SD-Security and SD-Branch service offerings for the WAN Edge. Versa's approach is unique by integrating networking and security with full contextual policy management, analytics and application experience driven infrastructure automation in a single software platform that can be deployed as uCPE, baremetal or virtual, on-premises or in the cloud.

Versa components:

- Versa FlexVNF: multi-tenant software that is deployed at the edge. Deployed as baremetal, virtual machine or as software uCPE to deliver transport line conditioning, routing, advanced SD-WAN, NGFW and UTM services.
- Versa Director: the single pane-of-glass that provides unified management and control for all Versa FlexVNF deployed across the software-defined infrastructure. Management of application traffic steering policies, security policies, provisioning, monitoring and configuration.
- Versa Analytics: big-data driven analytics engine to provide near-real time networking and security event correlation from Versa FlexVNF and supported 3rd party PNFs and VNFS.

Fortinet FortiGate Virtual Next Generation Firewall

Fortinet delivers the industry's best threat protection, unified threat management and performance in a virtualized form factor, based on the award-winning FortiGate. Fortinet FortiGate is a Leader in Gartner's 2017 Magic Quadrant for Enterprise Firewalls. FortiGate-VM offers the highest performance and scalability of any virtual firewall available today, with a comprehensive set of validated security capabilities including application control, intrusion prevention, antivirus, web filtering, mobile security, sandbox, SD-WAN, CASB, security rating service and industrial control services.

Features

- Pre-integrated platform for quickly creating, deploying and monetizing managed SD-WAN, security and value-added services
- Multi-domain, multi-vendor service orchestration across data centers and distributed branches
- Plugins for seamless integration with SD-WAN, NGFW, cloud and SDN controllers
- Service and resource (VNF) instance orchestration and lifecycle management
- Real-time enforcement of VNF and service-related policy
- Automated continuous service fulfilment and assurance
- Predefined use cases and service model; configurable service parameters
- Seamless BSS integration for service order lifecycle management via TMF Open APIs
- APIs for enabling business customers visibility and control of SD-WAN and VAS
- Cloud Native, microservices architecture, for cloud deployment and operational efficiency

Benefits

- Rapid time to market for SD-WAN – from inception to production in three months
- 70% operational efficiency improvement due to service orchestration automation
- Accelerates innovation and service agility through ease of VNF onboarding and service chaining
- Access to Amdocs' rich partner ecosystem of VNFs to drive innovation and VAS
- Affordable, scalable, pre-integrated, tested and certified platform reduces deployment time and time to market, while opening the door to future NFV-based services beyond SD-WAN
- Powerful service chaining and tight integration of functions enables creation of managed services that combine SD-WAN capabilities with a range of security and other functions
- Operational efficiency, flexibility and profitability of managed services through service automation and orchestration, zero-touch provisioning, centralized management and multi-tenant software running on commodity hardware
- Greater business agility and responsiveness for business customers needs
- Service delivery across WAN and DC domains, as well as over physical and virtual network elements

Case study: Using NFV orchestration for managed SD-WAN from day one

A leading North American service provider implemented an award-winning, carrier-grade, SD-WAN platform, designed for enterprises, SMBs and multi-site businesses. Subsequently, to future-proof the platform and provide customers with value-added services (VAS), they engaged Amdocs to implement its multi-vendor, multi-domain NFV orchestration, integrated with Versa's SD-WAN platform. This SD-WAN platform combines secure IP-VPN, application-aware routing and a stateful network firewall – all delivered over the public internet via a carrier-class IP-backbone, with secure internet connectivity to the public cloud. Specifically, the role of Amdocs NFV orchestrator is to streamline deployment and instantiation of cloud- and premises-based virtual network functions, as well as data center and distributed wide area network connectivity.

The agile and dynamic solution development process provided by Amdocs and Versa networks significantly reduced time to market from design/inception to production, enabling the operator to bring its new SD-WAN service to market very quickly. Furthermore, Amdocs NFV orchestration service automation contributed to a 65% reduction in service fulfilment operations.

As a result of employing an NFV orchestrator from day one, the service provider achieved its objective of creating an extensible, end-to-end future ready platform for providing additional VAS beyond SD-WAN.

www.amdocs.com

amdocs