IDC
Analyze the Future

IDC TECHNOLOGY SPOTLIGHT

The Transformative Potential of the Software-Defined Branch

April 2017

Sponsored by Versa Networks

The emergence of software-defined networking, coupled with the growing adoption of network function virtualization (NFV), is leading to new opportunities for service providers and enterprises. Managed service providers (MSPs) are leveraging the combination of these technologies to help enterprises transform their wide area networks by enabling branch offices to better meet their IT/network needs as they increasingly adopt transformative cloud-based applications. Through network visibility and cost-effective, application-aligned WAN connectivity, SD-WAN is enabling the branch network to serve as a catalyst for competitive advantage. As SD-WAN takes hold in the branch and its benefits are realized, enterprise IT should evaluate virtualizing security and other network functions and related technologies; it should also look at embracing the end-to-end opportunities of a full software-defined branch (SD-Branch). This Technology Spotlight examines SD-WAN's emergence, the incremental possibilities and broader context of the SD-Branch, and how service providers and enterprises can benefit from this expanded set of branch use cases. It also looks at the role of Versa Networks in this strategically important market.

Introduction

Thanks to digital transformation, enterprise IT is experiencing an evolution with respect to the wide area network and how services are delivered to and consumed by corporate offices, branches, and mobile users. Over the past several years, a growing roster of cloud-hosted SaaS applications has been a key element of the digital transformation that is opening new possibilities for the enterprise. From cloud-hosted ERP to CRM, video collaboration, and beyond, the enterprise can use the network to optimize its business with unprecedented effectiveness. Digitization also directly extends to customer experience. Enterprises in public-facing verticals are now *expected* to provide services such as guest WiFi, with many embracing new ways to engage customers through the network such as location services and digital signage. This rapidly expanded digital ecosystem has rendered legacy branch network and IT architectures insufficient. Branches need greater agility and a streamlined, easy-to-manage IT architecture that allows optimal cloud connectivity and access, prevents branch clutter, provides 24 x 7 visibility and analytics with reduced maintenance time, and carries a low total cost of ownership (TCO). All of this must operate on top of a dynamic, end-to-end security foundation.

Many enterprises are addressing both their digital evolution and increasingly nuanced branch network needs through SD-WAN. SD-WAN optimizes application access across multiple/hybrid WAN connections and promises a lower TCO than traditional services like MPLS by leveraging broadband internet or other connectivity as an alternative. Meanwhile, SD-WAN is growing in popularity with enterprises and service providers alike: IDC forecasts the worldwide market for SD-WAN infrastructure and services will grow to more than $6 billion by 2020. The need for SD-WAN is particularly acute for distributed enterprises that generally have a relative lack of onsite infrastructure and application hosting expertise across their distributed sites.

Key Trends Around SD-WAN

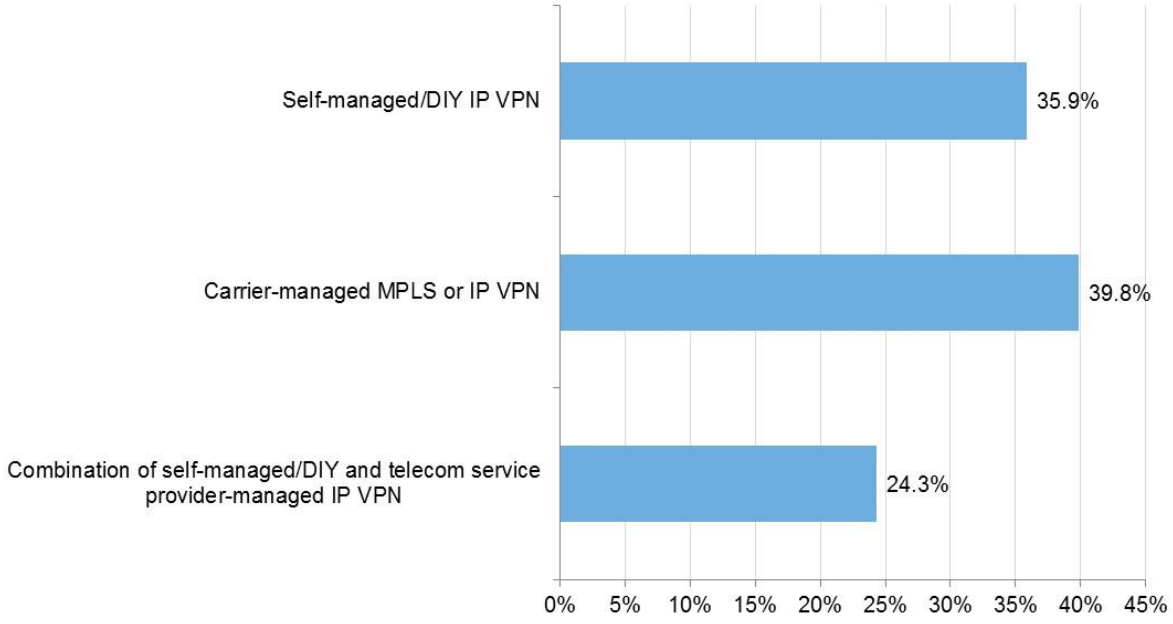
As enterprise IT becomes more comfortable with cloud and software-defined IT architectures, the stage is set for the SD-Branch to be embraced. A good indicator of this trend is the burgeoning interest in SD-WAN. In IDC's *Software-Defined WAN (SD-WAN) Survey*, over two-thirds of respondents said that they either plan to deploy SD-WAN in 12-18 months or have done so already. Given this interest and the rapidly growing market, many service providers have already launched SD-WAN offerings.

IDC data reveals a divide in the market between "DIY" and MSP-supported WAN. A slightly higher percentage of surveyed enterprises prefer CPE-based IP VPN (the dominant SD-WAN deployment scenario) that is MSP supported (see Figure 1). Moreover, the survey also revealed that 57% of DIY enterprises plan to shift to a carrier-supported solution within two years. IDC believes this trend will extend to the greater SD-Branch.

FIGURE 1

Self-Managed Versus Carrier-Managed IP VPNs

Q. What type of premises/CPE-based IP VPN do you have?



n = 605

Base = all respondents

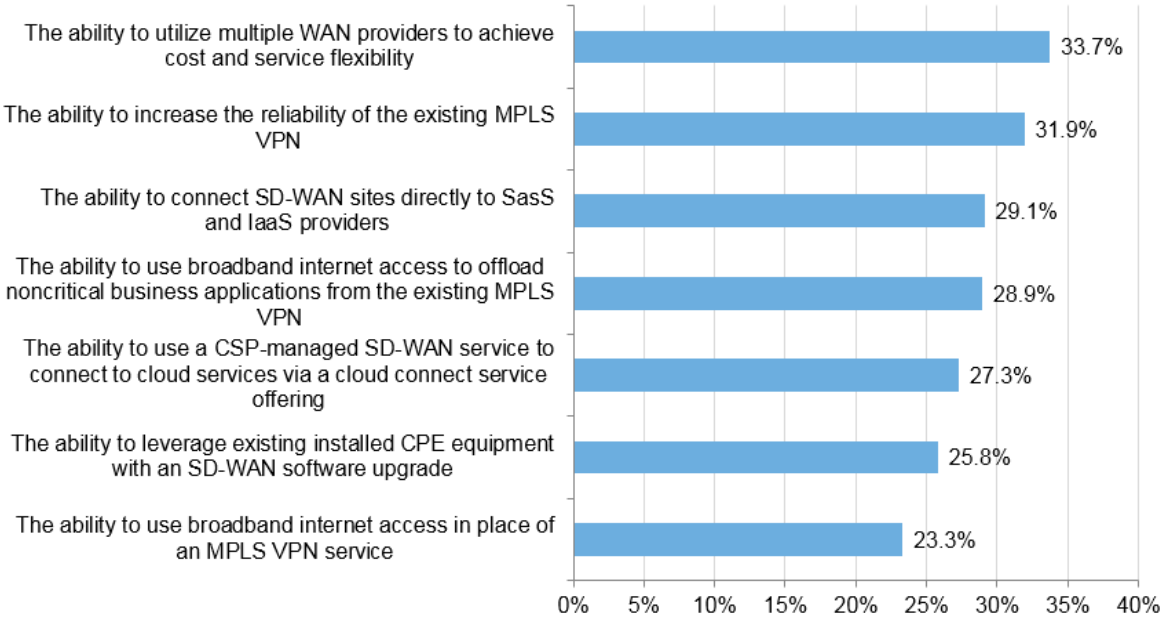
Source: IDC's *Software-Defined WAN (SD-WAN) Survey,* May 2016

When enterprises were asked to name their top 2 use case criteria for adopting SD-WAN technology solutions, there were several criteria that were important to a critical mass of those surveyed. Among the criteria that featured prominently were the ability to leverage multiple WAN connectivity methods and optimizing access to SaaS and IaaS applications (see Figure 2).

FIGURE 2

Top 2 Use Case Criteria for Adopting SD-WAN Technology Solutions

Q. Which are the top 2 use case criteria for adopting an SD-WAN technology solution?



n = 605

Base = all respondents

Source: IDC's *Software-Defined WAN (SD-WAN) Survey,* May 2016

However, what if SD-WAN is only the first step toward preparing the branch for the digital era? What if software-defined architectures for IT infrastructure and security can be converged with the network for a truly evolutionary branch IT solution?

Choosing the Right Underlying Branch IT Platform

The rapid growth of SD-WAN highlights the need for a streamlined, single-platform networking solution for the branch. However, the IT needs of the enterprise branch extend beyond networking. As organizations seek to converge different elements of IT infrastructure, it follows that many branches would benefit from a converged "services platform" that delivers a range of necessary IT functions in the branch, including networking and security services.

Advancements made with server virtualization, in conjunction with improved compute performance, and with NFV mean that traditional hardware-based IT functions can now be migrated onto a commodity x86-based appliance that takes the form of customer premises equipment (CPE). This CPE can provide fully open and programmable IT services and functions through software-based virtual network functions (VNFs). When multiple VNFs are provisioned with service chaining onto an industry-standard x86 appliance, these VNFs constitute what is termed as a "vCPE." Ideally, service providers should support a catalog of services at the branch to offer a complete solution. Today, these services are only available via dedicated physical appliances or via multiple VNF platforms that increase complexity. In response, many service providers strategies include deploying a vCPE

offering that supports a catalogue of third-party VNFs so that end customers (enterprises) have the flexibility to build the service that best supports their business needs.

While SD-WAN addresses pain points related to the performance and complexity associated with provisioning and operating multibranch enterprise WANs, in the process, it has also garnered a lot of hype for what it promises. Any SD-Branch function/service or platform should prominently feature robust SD-WAN functionality. But SD-WAN is not the "be all, end all" of the SD-Branch. The SD-Branch is most effective when utilized to its full potential across multiple network and security services such as full Layer 3 routing, SD-WAN, WAN optimization, firewall/VPN, unified threat management (UTM), secure web gateway, and DDoS protection. Key requirements of a fully integrated, enterprise-grade SD-Branch platform include multiservice support including local networking (wired/wireless), multitenancy, orchestration, the ability to support third-party VNFs via a vCPE, APIs and DevOps compatibility, and OSS/BSS integration. These features should be set against a backdrop of integrated security.

Benefits of SD-Branch Architecture

The SD-Branch promises many benefits to both enterprises and service providers alike.

Enterprises note the following benefits:

- **Application (and thus business) alignment.** Optimization of cloud connectivity, management, and visibility inherent in SD-Branch allows enterprises to better measure the effectiveness of an application versus its business objectives and its ROI. It also allows for more flexible scalability. SD-Branch facilitates more granular policy setting, with connectivity optimization reducing latency, so that mission-critical applications perform well, thereby allowing the business to run effectively.
- **Integration of security (software-defined security).** SD-Branch heavily leverages the internet in optimizing application connectivity. However, this creates new challenges for security and heightened requirements that come at additional cost. For the enterprise, this means the perimeter to the internet now goes from a few sites to potentially every enterprise location. This increases security infrastructure needs along with orchestration, management, and improved visibility for policy enforcement. The enterprise needs visibility and control of user, device, location, path, destination (URL), and application context combined with a dynamic policy-based capability. SD-Security addresses these requirements through Direct Internet Access (DIA) hardening to mitigate any IT concerns about a lack of protection. SD-WAN's foundation of encryption and topology flexibility also help to make the network inherently more secure.
- **Simplified provisioning and management of incremental network and IT functions in the branch (WiFi, LAN, other security).** A major promise of any converged infrastructure is streamlined, single-pane-of-glass management. With branch IT frequently asked to manage a more robust infrastructure without additional staffing, this is becoming more necessary. Single-touch provisioning and management across branch functions reduces operator error and inefficiencies, reduces silos, improves visibility, and allows enterprise IT to deliver a more consistent user experience through standardized policies and quality of service. Additional benefits include the improved ease of compliance adherence due to ubiquitous deployment of services and the standardized approach to infrastructure policies with automation. Workflow automation reduces the amount of time spent on network configuration and maintenance, allowing IT to spend more time on strategic tasks instead of "keeping the lights on."
- **Reduced TCO.** According to IDC's April 2016 *Software-Defined WAN (SD-WAN) Survey,* respondents initially expect to see, on average, 20% cost savings over traditional WANs. IDC

believes this cost savings extends to the greater SD-Branch and should rise with additional functions, such as security, getting software defined.

- **Better agility.** SD architecture allows branches to more dynamically and efficiently provision new IT services, reducing the time to roll out new business initiatives. This is important in that the digital enterprise has no time to spare when responding to competitive forces and changing business conditions. Ongoing digitization will only intensify the agility requirement.

Benefits for service providers include the ability to:

- **Increase top-line and bottom-line managed service revenue.** IDC forecasts that the market for SD-WAN will grow to $6 billion by 2020, representing a five-year CAGR of more than 90%. This growth demonstrates that there is near-term demand for software-defined branch technology and that SD-Branch services beyond WAN increase that opportunity. While delivering incremental value to the enterprise, SD technology can also improve MSPs' bottom line, given its reliance on low-cost CPE and the reduced cost of labor given the streamlining accomplished by single-touch management and the integration of network and security.
- **Offer differentiated services.** Many service providers are introducing offers into the SD-WAN market. By offering a more complete SD-Branch solution that includes SD-WAN and SD-Security, service providers position themselves ahead of the technology curve and quite possibly ahead of their competitors.
- **Deploy a flexible services-oriented platform in the branch.** Adopting this approach will enable ongoing upselling of services from SD-WAN to SD-Security to full SD-Branch. Similarly, offering a full stack of SD-Branch functionalities allows customers to achieve a high degree of customization, choosing the VNFs most relevant to their business needs. Of course, business needs change and the vCPE model allows for the upselling of new and expanded services as customer needs evolve.

Considering Versa

Versa leverages innovation in SDN, NFV, programmability, and agile provisioning integrated with proven networking and security technologies to create an integrated and system-level solution for managed services to provide a flexible SD-Branch offering for the enterprise.

By transitioning from hardware-based managed services to a software-based and more DevOps-oriented approach, service providers can harness the power of SDN and NFV to provide greater service agility and time to revenue, combined with lower capex and opex. Enterprises benefit directly by simplifying their WAN and overall branch architecture and gaining the cost savings and efficiency that comes with SD-Branch. To make this transition achievable, Versa has developed a cloud-native, multitenant, multiservice software platform that provides multiple functions that run on low-cost x86-based servers and appliances that are open and programmable and operate in a private cloud or public cloud environment.

The Versa solution consists of three software components that work together to deliver highly flexible VNF-based network and security services:

- **Versa FlexVNF:** The core building block for Versa's solution, which includes a broad set of network and security functions with full multitenancy, programmability, service chaining, service elasticity, support for hosting of non-Versa VNFs, and cost-effective deployment choices
- **Versa Director:** Single point of centralized control and management for both connectivity and services

- **Versa Analytics:** A real-time analytics engine that provides historical visibility, prediction, and a feedback loop for adaptability and control

The company's system-level approach can be used to enable several use cases and diverse managed service offerings, among them:

- **Managed SD-Branch:** For customers looking to maximize the business agility of their branch offices while reducing appliance sprawl and overall IT costs, service providers can leverage the Versa SD-Branch solution to software define and virtualize a broad set of WAN, networking, and security functions. Versa SD-Branch integrates a highly flexible and high-performance SD-WAN with multilayer security and local networking, combined with automated service provisioning across all functions and full multitenancy. Target customers for SD-Branch services include midmarket to enterprise businesses, as well as those industries requiring maximum control of IT resources (e.g., financial services).
- **Managed SD-WAN:** For customers that require an on-premise deployment of connectivity services and/or are interested in the benefits of SD-WAN, Versa enables providers to deliver a highly scalable and cost-effective managed SD-WAN service. While some SD-WAN products were developed for single customer enterprise deployments and connectivity only, the Versa solution is multitenant and multiservice, enabling both economy of scale as deployments grow and the ability to integrate on-premise security services with SD-WAN connectivity for unique, feature-rich service offerings. Target customers for managed SD-WAN services include midmarket to enterprise businesses.
- **Managed SD-Security:** For customers looking to deploy a cloud managed security capability at their branches to provide visibility and control, service providers can create managed security services using the Versa solution with multiple security capabilities. Service offerings can be built with security functions on-premises (e.g., next-generation firewall and URL filtering to enable direct internet access) or located at the provider's premises (e.g., a "virtual UTM" with next-generation firewall, antivirus, and IPS in the POP or datacenter), or a combination. Target customers for managed security services include small, midmarket, and enterprise customers, depending on branch architecture and security/compliance requirements.
- **Managed SD-Router:** For creating a managed router service, the Versa managed SD-Router solution provides a flexible and lightweight zero-touch deployment model. Connectivity options can range from simple Layer 2 forwarding to full routing and are achieved with an on-premises VNF on a local server or dedicated appliance. Versa's multi-VNF capability and service chaining enables additional network and security services to be easily added to the managed service and delivered from provider premises to create a full-featured offering. Target end customers for managed SD-Router services are small to medium-sized businesses (SMBs).

Challenges

While these offerings demonstrate tremendous potential to create new opportunities for service providers and enterprises alike, there are some challenges to consider. First, Versa is a newer vendor in the WAN infrastructure and services market that is replete with incumbent vendors. It is important to seek proof points as to Versa's value proposition from preexisting service provider deployments to assuage the concerns of WAN buyers that are possibly overwhelmed with messaging about new SD technologies.

Another key challenge pertains to how quickly enterprises can embrace the transformation toward SD-Branch. Deploying an SD-WAN solution itself breaks new ground for enterprise IT, adopting a more holistic, virtualized architecture for SD-Branch involves a completely new and innovative approach, and a mindset change that will require extensive education from Versa and its SP partners.

Also, one needs to consider the disconnect between the centralized branch IT buyer versus the remote branch IT user. It is important to meet the needs of both stakeholders, and marketing must speak to both. IDC believes that, if Versa and its service provider partners address these challenges collaboratively, it will improve their collective chances for success.

Conclusion

The emergence of software-defined branch infrastructure represents tremendous opportunities for service providers to meet evolving enterprise needs, as well as a key resource for large enterprises directly. Software-defined branch allows for flexibility in WAN connectivity, alignment of the WAN with mission-critical cloud-based business applications, simplified single-platform management, better security across the WAN and branch, and the opportunity for decreased TCO. By moving beyond SD-WAN and offering a more fully featured SD-Branch that includes SD-Security, analytics, and VNF flexibility, service providers can distinguish themselves in an ever-crowded SD-WAN services market and stay ahead of rapidly changing technology. A solution such as that offered by Versa Networks has good potential to equip service providers, as well as large enterprises, to respond to the needs and opportunities of the SD-Branch.