VERSA NETWORKS

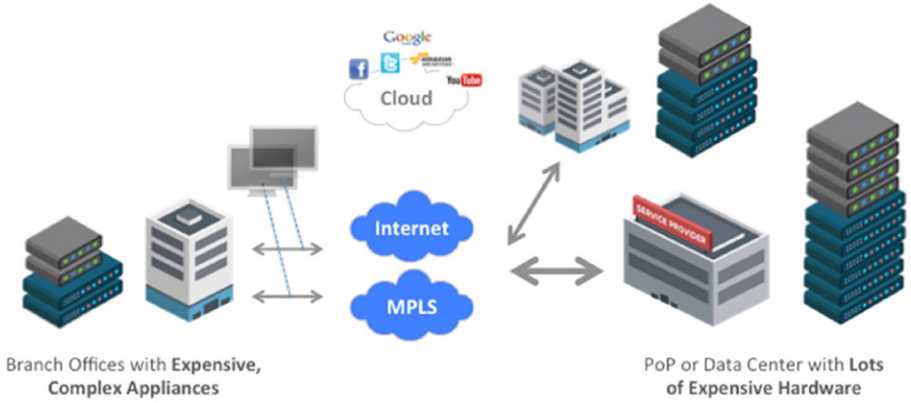
WHITE PAPER

The Benefits of SD-WAN with Integrated Branch Security

Branch Networking Today – More Bandwidth, More Complexity

Branch or remote office network architectures have barely changed for 15+ years. But the requirements for branch WANs have changed significantly. Most branch offices connect to the rest of the business through an MPLS circuit or VPN. This approach worked well for many years, but as traffic volumes have increased significantly due to video, cloud storage/collaboration and other high bandwidth applications, WAN bandwidth requirements have also increased. Options include adding more capacity to the existing WAN circuit or introducing an Internet connection to the branch WAN architecture.

The Internet approach can help mitigate the overall congestion of the WAN, but also increases the complexity, security requirements and cost of designing and managing the branch network, requiring additional infrastructure, policies and management/oversight. From a bandwidth management and allocation basis, traffic engineering to ensure available bandwidth for given applications requires time consuming manual mapping of specific traffic to specific circuits. From a security perspective, adding Internet connectivity requires additional security infrastructure, policy creation and management. Finally, when Internet connectivity is added, the ability to effectively monitor and obtain an overall view of the branch WAN becomes increasing complex, and ongoing issues are often difficult to mitigate.



Branch Network/WAN: Enterprise Challenges

Businesses with multiple branches today either manage their networking in-house or leverage a managed service provider. Either way, there are multiple (and growing) challenges that the network teams must address:

- **Applications deployed everywhere** – Today, applications not only run in corporate data centers, but also exist at cloud app providers (SaaS) and deployed in cloud infrastructure providers (IaaS). If all traffic to/from the cloud must be routed through the corporate data center for security functions, end user experience & response times will be negatively impacted. At the same time, additional security functions (e.g. firewall, access control & filtering, anti-virus/malware, DNS, etc.) are required if cloud resources are accessed directly from the branch office.

- **Bandwidth growth & application performance** – Video and cloud storage/collaboration continue to consume a growing amount of WAN traffic. Increasing the capacity of MPLS and leased lines can be expensive. The addition of direct Internet connections and broadband circuits provides lower cost bandwidth, but also increases operational complexity and security requirements. Additional challenges come with monitoring and troubleshooting network health across multiple circuits, communication service providers and an array of network & application performance tools.
- **Complexity and cost of ownership** – Adding bandwidth and Internet connections requires purchasing, deploying and managing point devices for different circuits and network functions (routing, WAN optimization, firewalls, etc.) at locations where there is generally little if any IT/security expertise locally. The result is a CapEx heavy investment and significant increases in ongoing OpEx.
- **Slow response to change and business needs** – Agility when facing unexpected events or line of business requirements at the branch allows companies to gain competitive advantage. Unfortunately, companies deploying new or upgraded branch network services experience long deployment times due to provisioning of new hardware devices, as well as scheduling consultants or integrators to install, configure, integrate and test equipment. This occurs both at initial deployments, but also when capacity upgrades are required (e.g. if a new or larger WAN circuit is provisioned, then a higher capacity router and/or firewall is required). Making a change to the branch WAN can take weeks and even months.

Branch Network/WAN: Service Provider Challenges

In addition to the enterprise problems associated with today's branch WANs noted above, service providers have an incremental set of challenges they must address as they build and scale managed network services for their business customers:

- **Lack of agility** – As noted above, the shipping, provisioning and configuration of branch networking (and security) devices is slow and expensive. Service provider customers expect rapid delivery of new WAN services, though it can take weeks to several months to properly deploy a branch office network and associated services. Providers need to rapidly launch new services using an automated/self-service approach whenever possible, and then quickly scale those services as business targets are reached.

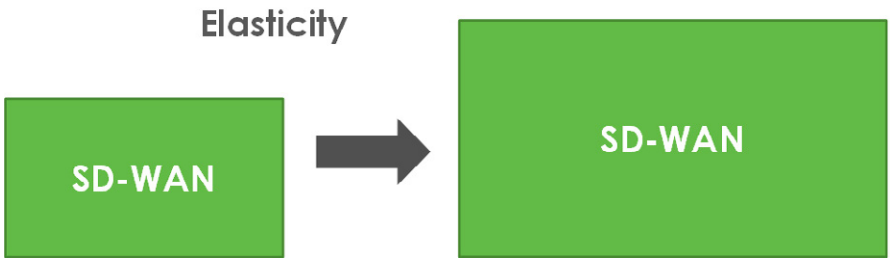
- **Cost of CPE** – Networking and security infrastructure is very expensive and labor intensive to manage. Add truck rolls, installation and support contract expenses and the costs associated with service rollouts can quickly cut into managed service revenue and profitability. Service providers need to deliver WAN services in a cost-effective way (without major hardware inventory costs), while decreasing the cost of equipment and operational expenses, to improve service margins and profits.
- **Added complexity at scale** – As a managed network service's customer and site volume grows, providers often find that complexity and operating costs grow radically after certain thresholds are reached – especially when the service is based on basic infrastructure like traditional routers or firewalls built for individual enterprises. Scaling managed services to 100s or 1000s of customers from a central PoP or data center requires both multi-tenancy and isolation of network, service and administration on a per-tenant basis.
- **Change and capacity management** – Regular changes to customer requirements like adding bandwidth and updating security policies, and the resulting updates to CPE, are an ongoing challenge. Service providers must efficiently and cost-effectively manage networking and security change requirements for branch WANs.
- **Systems expertise** – Network and security functions are increasingly specialized, and thus the requirement for service providers to provide technical support across a wide collection of managed devices is a huge challenge. Acquiring and retaining those resources, along with the support requirements associated with service management and change either remotely or on-site, can quickly erode margins and place significant pressure on the business model of a managed service.

Leveraging Software-Defined WAN (SD-WAN) and NFV

While the above issues with managed network services are very real, technology advances in the last few years can offset many of them. A software-defined approach can significantly improve the deployment and operation of managed network services like SD-WAN. A rapidly growing trend is the use of software abstracted from the underlying hardware used in the delivery of network services. This trend is called network function virtualization (NFV), evolving previously hardware-centric network and security technologies into software-based solutions running on commodity off-the-shelf (COTS) hardware and white-box appliances.

A core element of NFV is the virtualized network function (VNF), which is a software-based or virtualized version of a specific function like routing, CGNAT or next-generation firewall. Much more than just converting from point hardware or appliances to virtualized software instances, VNFs are centrally managed and policy orchestrated, zero-touch provisioned, and service-chained, addressing many of the operational challenges noted earlier.

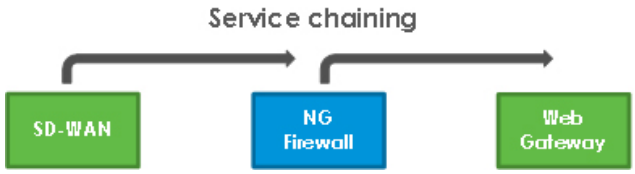
In essence, applying NFV (and VNFs) to enterprise WANs and managed WAN services results in the ability to "software-define" the WAN, not just in form-factor, but also in deployment & provisioning, initial configuration, ongoing management & operations. This is compounded by the fact that software-defined WAN created from NFV de-couples functions from proprietary hardware, enabling the use of network and security functions in software running on commodity x86 servers and white box appliances. It also de-couples the underlying WAN transport, enabling the use of any WAN circuit type including MPLS, leased line, broadband Internet and wireless 4G & LTE connections.



Taking an example of SD-WAN, imagine an enterprise with 400 branch offices that wants to utilize inexpensive, high throughput broadband connections as an element of its overall WAN architecture. Instead of purchasing legacy routers and firewall appliances and shipping them to branch sites, the enterprise or service provider can ship commodity white box appliances and zero-touch provision the equipment and underlying services at the branch. Using the legacy appliance-based approach and deploying them at the rate 20 per month (an aggressive schedule, at one installation per business day), it would take over 1.6 years to complete the project. Leveraging Versa's NFV-approach, the enterprise or service provider can ship commodity white box appliances to 100 branches per month, and simultaneously activate and test 25 devices per week remotely, yielding a total project time of 4 months. The result is a time reduction of nearly 80%, coupled with a significantly lower cost of deployment (as no on-site specialists are required).

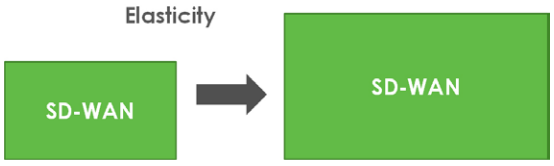
Another key aspect of Versa SD-WAN using NFV is the ability to service chain security functions to easily achieve an SD-WAN with on-premises security to meet compliance and data protection requirements. For example, specialized security functions like a secure web gateway can be service-chained to the

SD-WAN to enable secure direct Internet access from the branch. Service creation, service definition and service-chain rules utilize templates and provide programmable, API-driven delivery of the service via centralized orchestration and management tools. This automated approach enables each branch office SD-WAN to be deployed in hours, instead of days or even months.

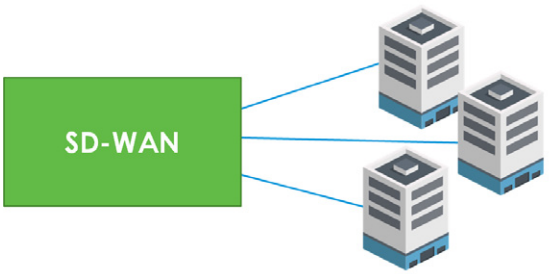


Other aspects of creating a SD-WAN managed service or enterprise deployment include:

- **Application intelligence** – Versa SD-WAN has the ability to identify over 2800 specific applications and use that knowledge to apply a range of network and security policies to the traffic carrying them. This includes mapping applications to particular WAN connections (e.g. core business applications to MPLS and consumer web traffic to broadband), application prioritization, per application security policy and enforcement (e.g. blocking certain types of web content), etc.
- **Elasticity** – When deploying SD-WAN through an NFV-based model, capacity can dynamically scale up or down without having to replace or add additional proprietary hardware. For example, branch bandwidth can be doubled in minutes either automatically or using commands from the central provisioning portal, with no truck roll or appliance swap-out. In the event that a branch needs more capacity due to a network traffic spike, the SD-WAN can automatically scale up to meet the demand. When the network spike subsides, the SD-WAN will scale down as needed.

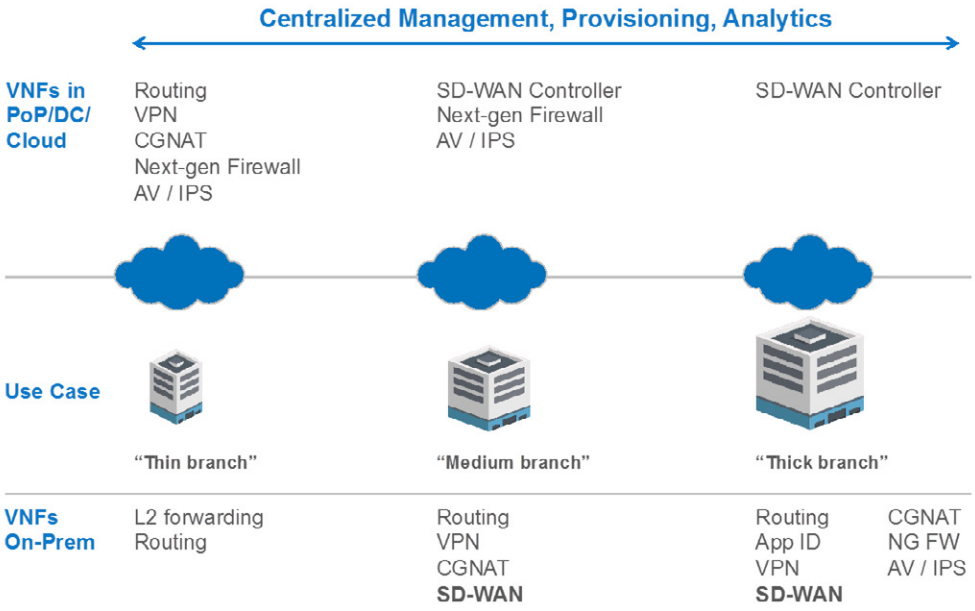


- **Multi-tenancy** – Versa SD-WAN is designed as a carrier-grade solution with full multi-tenancy at both the head-end and branch. Service providers operating SD-WAN managed services, as well as large enterprises operating different SD-WANs for separate business entities, can support up to 250 customers per single 1RU server running the Versa SD-WAN controller. Versa Director and Analytics also are fully multi-tenant. At the branch site, a single Versa FlexVNF instance can support multiple local tenants or business entities. The result is much lower infrastructure costs and more agile service delivery.



- **Multiple deployment options** – Versa SD-WAN is a software-based NFV solution, and has a broad set of deployment options. It can be deployed directly on bare metal x86 servers, white-box appliances, virtual machines (VMware ESXi, KVM) and containers. Customers can select the best infrastructure for their SD-WAN deployment at both the data center/PoP and branch offices without being constrained by SD-WAN vendor proprietary hardware options, resulting in significantly lower CapEx and design flexibility.

- **Flexible and distributed service architecture** – With the advent of NFV, service providers and large enterprise have the capability (and flexibility) to decide where to deploy and run each layer of network or security function – either on-premises in the branch office or centrally in the data center, at a provider's point-of-presence (PoP). For example, compute-intensive services such as anti-virus and IPS can run centrally, while services that are key in the branch, like application identification, SD-WAN, routing and firewall can be run locally. In addition, Versa SD-WAN can integrate critical network services using service chain definitions that include both local and remote functions, depending on the business need.



- **Centralized, automated operations** – A software-defined and NFV-based approach to the WAN also provides a way to provision SD-WAN equipment and deliver network and security services from a single point of control, avoiding the need for skilled personal available on-site to deploy and configure the solution. Instead, SD-WAN services can be deployed, bandwidth and service capacity increased or enhanced with additional functions automatically, all without requiring any on-site presence, hardware refreshes or manual interaction. Also, if a particular branch site(s) requires a unique set of network or security functions, the branch can be serviced individually and automatically from a single management portal, including role-based administration for flexible configuration and ongoing policy management.

In summary, enterprises and service providers looking to deploy a successful SD-WAN require a new approach to service delivery based on software-defined and NFV principles. These include next-generation network and security functions that make the WAN not only network-, but application-aware. These new SD-WAN capabilities must seamlessly integrate into a customer's routed network, but also have the ability to utilize any underlying WAN transport including MPLS, broadband and wireless connections. Internet security and control from the branch is a must-have to support the expanded use of Internet connectivity (e.g. direct Internet access) for business needs and ensuring end user experience.

Adopting a NFV-based approach to SD-WAN gives enterprises and managed service providers the added flexibility to easily integrate and scale the right security functions alongside advanced networking capabilities, maximizing the benefits provided by SD-WAN – agility, reduced TCO and better service levels & cloud application performance. Additionally, an NFV-based approach to SD-WAN greatly improves the operational efficiency and profitability of provider-delivered managed services through the use of multi-tenant software running on commodity hardware.

Versa Networks, Inc, 6001 America Center Dr, 4th floor, Suite 400, San Jose, CA 95002
+1 408.385.7660 | info@versa-networks.com | www.versa-networks.com