Next-Gen SD-WAN:
Charting a Path for the Next Five Years

John Burke

Principal Research Analyst
and CIO

Nemertes Research

Q2 2020

Table of Contents

Executive Summary 3

The Issue: Next-Generation WAN is a Journey, Not a Destination 4

Baseline Choice: Do-It-Yourself, Managed, or Co-Managed..... 4

DIY Overlay and Managed Solutions: Pros and Cons 5

A Middle Path: Co-Managed Solutions 5

Choosing: Touchpoints for Selecting a Model 6

Securing the Future in SD-WAN 6

SD-WAN Raises the Baseline of WAN Security 7

SD-WAN Security Functions 7

Branch Firewall 7

Fitting in: SD-WAN in a Security Ecosystem 8

Beyond SD-WAN: SCAPE as complementary solution 8

Choosing: Touchpoints for Security Decisions 9

Future-proofing: AI and the Future of Automation 10

AIOps and SD-WAN 10

Autonomous SD-WAN..... 10

Choosing: Touchpoints for Advanced Features 10

Conclusion..... 11

Executive Summary

SD-WAN is the basis of the current “next-gen” WAN, bringing with it the virtualization of wide area networks, centralized and holistic management, and improved performance and resilience in the WAN. It helps address this shift in use to encompass traffic touching the outside world, and the sharpening of focus on application performance for both cloud and in-house applications.

However, new SD-WAN options and new business requirements translate to more choices IT must make to zero in on the right solution; to best position the network to meet the next, higher-stakes round of needs.

At the base of it all, IT needs to choose among the deployment and management models: do-it-yourself overlay SD-WAN, or managed SD-WAN, or a new hybrid: co-managed. In choosing, they must balance their need for control against their need for reducing network staff management workloads, the risks of relying entirely on their own staff vs. those of relying on the service provider’s, and all with an eye on costs. DIY maximizes control and the risks that go with self-reliance; managed SD-WAN maximizes workload reduction and the risks that go with loss of complete control; co-managed balances the two.

IT leaders need to select a platform that meets their performance management and availability needs, but that is also ready to be a full partner in securing the WAN. Enterprises deploying SD-WAN expect to have three-quarters of their sites allowed direct access to the Internet by the end of 2021, and half to be connected solely via the Internet. They need an SD-WAN solution to help secure that, and moreover, 80% also want it to replace branch firewalls in most or all locations. In that context, the solution must play nicely with other security systems, feeding data into SIEMs and integrating with a Security Orchestration, Automation, and Response (SOAR) tool.

And, they need to keep an eye on the future of operations as they select solutions, aiming for an SD-WAN tool that will have, or integrate with, AI-driven operations automation capabilities.

IT professionals should:

- Evaluate managed, co-managed, and DIY SD-WAN solutions against their enterprise’s network needs and their own team’s skills and staffing levels
- Work with security teams to ensure a smooth integration of SD-WAN into the organization’s technological and operational security frameworks
- Define a roadmap for the integration of AI into network operations and specifically SD-WAN, with the goal of achieving more autonomous networking

The Issue: Next-Generation WAN is a Journey, Not a Destination

A simple truism about “next generation WANs” (or anything else) is that they are only next-gen until they are suddenly last-gen. New features and new technologies emerge regularly, so building a next-gen WAN isn’t a “once and done” exercise but rather an ongoing process of evaluation, adoption, and retirement.

At the same time, the business constantly requires new things of the network, as digital transformation efforts continue to remake operations, value propositions, and business models. The last few years have seen traditional WAN data flows (starting and ending inside enterprise locations) suddenly dropping to less than 40% of WAN traffic, with the rest starting and/or ending outside. They have also seen application performance rising to become the touchstone of WAN technology choices.

SD-WAN is the basis of the current “next-gen” WAN, bringing with it the virtualization of wide area networks, centralized and holistic management, and improved performance and resilience in the WAN. It helps address this shift in use to encompass traffic touching the outside world, and the sharpening of focus on performance. But new SD-WAN options and new business requirements translate to more choices IT must make to zero in on the right solution; to best position the network to meet the next, higher-stakes round of needs. This means in turn that IT will be faced with new complexity, and can use some guidance on how to make the right choice.

Baseline Choice: Do-It-Yourself, Managed, or Co-Managed

SD-WAN comes in two basic flavors: do-it-yourself overlay networks (DIY) and managed/in-net options. In the DIY model, the enterprise acquires and manages the solution, buying or leasing, installing, and managing the endpoints. Some solutions have a cloud-based management console, others on-premises, other both. In the managed option, a managed service provider can either install and manage an overlay solution on behalf of the enterprise, or combine an overlay solution with in-network services that provide some or all of the SD-WAN functionality.

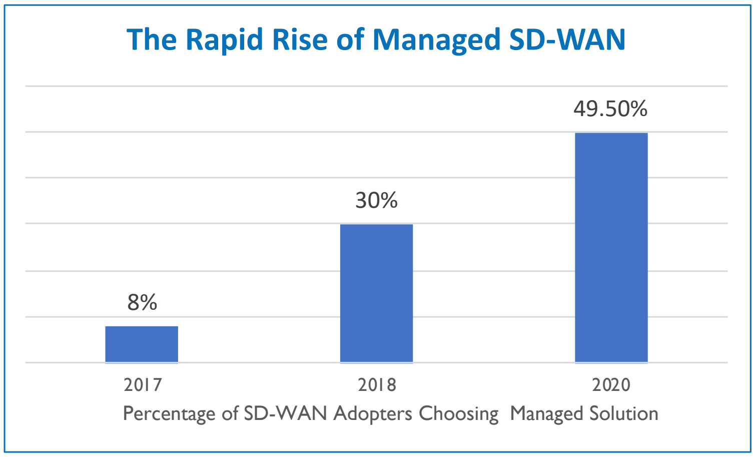

Figure 1: Managed SD-WAN Adoption Has Risen Quickly

In Nemertes Research’s 2020-2021 Next Generation Networking Research Study, 61% of organizations had begun to deploy SD-WAN, and of them 49.5% chose a managed solution, 51.5% DIY. This represents a dramatic shift in enterprise thinking towards adoption of managed options. In our 2017-2018 study, just 8% chose a managed offering, while in the 2018-2019 study only 30% did.

DIY Overlay and Managed Solutions: Pros and Cons

The first SD-WAN solutions in the market were overlay systems suitable to a DIY deployment. Among their strengths are technological maturity and broad install bases. They give IT maximum control of configuration, rollout, and connectivity. However, that completeness of control comes at the cost of complete responsibility. IT has to rely on its own resources for deployment and management, fine-tuning and troubleshooting configurations, and evaluating and rolling out patches and upgrades to the tool.

As with any managed solution, for managed SD-WAN the main trade-offs are on cost and control. On the one hand, the enterprise can rely on the expertise and staffing of the provider to handle deployment and management and the rest, a significant burden: on average, enterprises devote about 17% of their network staff's time to WAN management, roughly 4 full time staff out of an IT department of 100. Using a service provider also brings with it the benefit of a deep bench of network engineers, and of their having a broad experience of the solution as deployed in other networks. On the other hand, the enterprise loses some control over deployments, of who is assigned to the job or for how long, and of how quickly management actions are taken.

A Middle Path: Co-Managed Solutions

As the managed SD-WAN space has matured—and now, every major and most minor network services provider has one or more offerings—a middle way has emerged: co-managed SD-WAN. One of the defining virtues of SD-WAN technologies is simplified and centralized management of WAN behaviors separate from management of the underlying hardware and connectivity. They also tend to have role-based access controls, and multi-tenancy functionality. The nature of the solutions makes it easier for the service provider to share management with enterprise IT staff: they can open some or all provisioning and management tools to the customer, while putting guardrails on access to prevent disasters. Should a need for an emergency adjustment to segmentation or security policies arise, customer IT teams can potentially make those changes themselves, for example, with review post-facto by the provider.

Model	Pros	Cons
DIY	• Maturity, broader install bases • Complete control • Lower per-site cost	• Complete responsibility: deploy, manage, troubleshoot, update • Staff knows only this network • Only own staff to lean on
Managed	• Outsource responsibility: deploy, manage, troubleshoot, update • Deep bench and learnings across networks	• Loss of control of platform and management responsiveness • No control of who staffs or for how long
Co-Managed	• Retain as much responsibility as desired, outsource rest • Deep bench and learnings across networks	• Higher cost of managed with reduced staff time savings

Co-management allows the enterprise to develop and use expertise of its own as a hedge on staff rotation or responsiveness issues. It also allows customers that find no on-going need for hands-on access—that develop trust with their provider—to migrate to a fully managed service if they wish. (The tradeoff is a lesser reduction in staff hours to WAN management, of course.)

Choosing: Touchpoints for Selecting a Model

In making a choice as fundamental as DIY vs managed, IT needs to weigh a number of factors, including:

- **Overall appetite for managed solutions:** if the company is in an outsourcing and opex-leaning phase, managed options are obviously appropriate and DIY would need special justification.
- **Purchasing strategies:** If the organization is committed to a “big rock” strategy of acquiring as many solutions as possible from a strategic partner, that may push either way, depending on whether the partner sells an overlay solution of its own, or offers a managed SD-WAN service.
- **Strategic direction**: IT should carefully consider WAN needs and use cases known to be coming down the pike, as well as those already present. The more varied and unique they are, the more attractive a DIY solution will be, with the option to tailor precisely to each situation. The more an enterprise can achieve a templatized deployment model, the better served it would be by a managed option.
- **Staffing strategies:** If IT is facing a big generational loss of WAN expertise, or simply no longer sees WAN management as a core skill, it may want to buy the deep bench of the managed service provider, rather than gamble that the use of SD-WAN will “deskill” WAN management sufficiently for them to skate through.
- **Vendor sprawl:** The variety of last-mile vendors used represents another decision point. If IT wants to have complete control over connectivity options, DIY makes connectivity fungible, and some managed options allow the enterprise to bring its own. On the flipside, managing a network provider takes work and costs money, and SD-WAN creates the opportunity to vastly expand the number of last-mile providers in the mix. With a DIY system, IT has to either assume that cost, or seek to hand some of it off to an aggregator. With a managed system, IT may want to retain last mile management to retain an additional degree of independence from the SD-WAN provider; or it may want to hand off to a third party to aggregate in order to get that independence without the work; or it may want the SD-WAN provider to handle it. About 36% of enterprises hand off to an aggregator, while 18% have their SD-WAN provider manage the last mile.

Securing the Future in SD-WAN

Simply migrating to SD-WAN can improve security, and most SD-WAN tools incorporate multiple security features to protect WAN traffic. Ideally they also provide the kinds of data feed and integration functionality needed to fit into an enterprise’s security ecosystem.

SD-WAN Raises the Baseline of WAN Security

An SD-WAN solution provides a centralized, policy-based management console to manage the whole WAN, both the platform itself (software updates and patches) and the settings affecting traffic.

Stepping up to a truly centralized and heavily automated WAN platform raises the WAN security baseline for most organizations: the ability to know and control how the WAN is configured, and to use up-to-date software. Most legacy WANs are heavily manual in operation: engineers change device configurations manually, and patch or update the operating systems manually.

The cost in staff time, the interruption to services, and the risks (of further service interruptions or degradations, or of security vulnerabilities, due to misconfigurations or failed patching or upgrades) make most organizations minimize the number of times they update software. If traffic is flowing, they leave things be as much as they can. Branch network stacks, as a result, frequently harbor multiple versions of routing, firewall, and WAN optimizer operating systems, older ones that are also, often, unpatched or inconsistently patched or way behind on patching. SD-WAN's centralized management makes it simple to keep the platform itself up to date, and to ensure consistent configuration across sites. If an engineer pushes out bad settings, the platform also makes it easy to quickly propagate the fix.

SD-WAN Security Functions

From a security perspective, SD-WAN's key security function is to segment traffic in various ways: by application and protocol, by user/group, by region, etc. For example, SD-WANs can create virtual WAN overlays that route different categories of traffic according to the compliance requirements affecting each; for example, to keep flows in (or out) of specific geographies. Some solutions understand applications deeply enough to manage traffic generated by different functions differentially: to allow some functions (e.g. audio conferencing within a team collaboration app such as Zoom or Microsoft Teams) but not others (file sharing within the same application).

Nemertes Research's 2020-21 Next Generation WAN Research Study finds that SD-WAN users intend to have 50% of branches connected via Internet links only by the end of 2021, and to allow 75% direct access to Internet destinations.

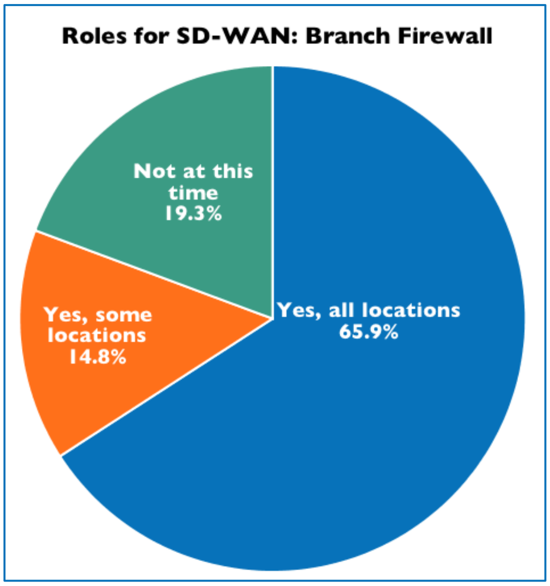

Figure 2: 80% of SD-WAN Users Want SD-WAN to Replace Some or All Branch Firewalls

Branch Firewall

Organizations wanting SD-WAN to be the branch firewall require a basic stateful firewall as bare minimum, but most want more: a full next-generation firewall (NGFW). These firewalls leverage the same kinds of context- and application-awareness that the SD-WAN needs for sophisticated traffic management, so it is a natural combination of functions. In the same vein, IT should also look for IDS/IPS functionality (often included in an NGFW), broader unified threat management (such as content filtering), and even secure web gateway features. If they are not folded directly into the SD-WAN endpoint itself, they should be available via service-chaining to another appliance, virtual network function module (VNF, or cloud service. A managed SD-WAN solution may offer these directly from the SD-WAN provider's own service cloud, or via partners. Where firewall functionality is to be pushed out to a cloud solution, enterprises must be careful to test and evaluate changes in latency and throughput that may result. More than 80% of SD-WAN users want their SD-WAN to replace branch firewalls.

> By the end of 2021 SD-WAN users intend to allow 75% of branches direct access to Internet destinations, and to have 50% of branches connect only via Internet links.

Fitting in: SD-WAN in a Security Ecosystem

An SD-WAN solution won't be the only security tool, so it should fit in with the rest. As a baseline feature, any SD-WAN should be able to feed logging data to a SIEM system. Better still, it should also provide secure API access to operational data. APIs are also central to integrating an SD-WAN into a security orchestration, automation, and response (SOAR) software. With SOAR, an SD-WAN can serve as flexible and powerful component in a broader software-defined perimeter and/or zero-trust security architecture.

Beyond SD-WAN: SCAPE as complementary solution

Nemertes 2019-2020 Cloud, Network, and Infrastructure Research Study found the average enterprise to be running more than half its IT workloads outside its own data centers. This continuing shift of enterprise IT into multiple cloud environments exacerbates the problem of securing use of them. After all, enterprise uses can be anywhere—not just in WAN-connected branches, but also in Internet-only branches, partner sites, telecommuting from home, or generally working untethered hotels, coffeeshops – anywhere.

The solution is SCAPE: Secure Cloud Access and Policy Enforcement, a new generation of multicloud-friendly, distributed-enterprise security offerings. SCAPE solutions provide

- a secure access layer that replaces a traditional VPN
- secure middle-mile connectivity to move traffic from access gateways to (or close to) its destination without traversing the public Internet
- centralized management and enforcement of security policies similar to a Cloud Access Security Broker (CASB).

SCAPE solutions can direct traffic into an enterprise's own data center, or through a cloud exchange to a cloud partner, or to an Internet egress point adjacent to a cloud service provider on-ramp. (Please see Figure 3.)

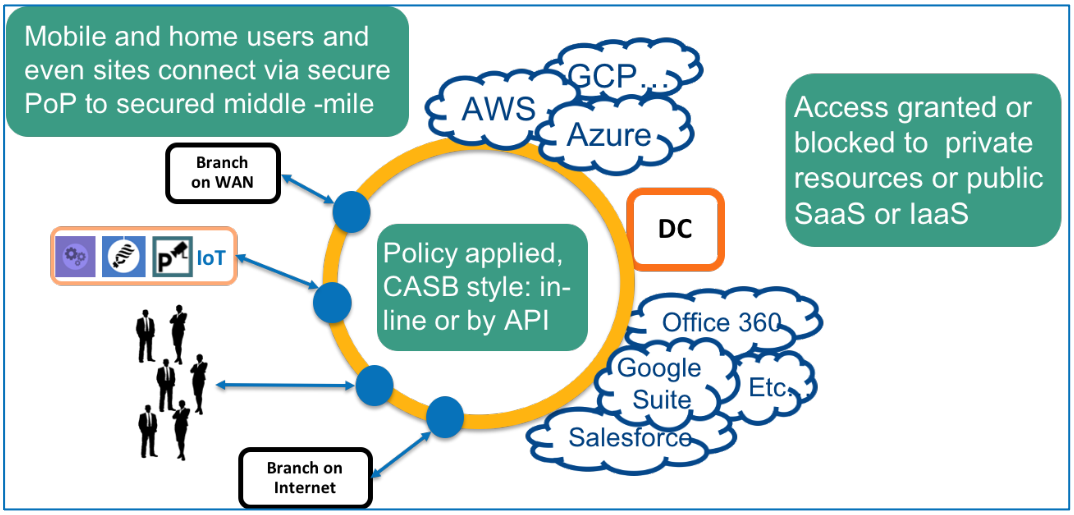
Mobile and home users and even sites connect via secure PoP to secured middle -mile
Branch on WAN
IoT
AWS
GCP…
Azure
DC
Access granted or blocked to private resources or public SaaS or IaaS
Policy applied, CASB style: in-line or by API
Office 360
Google Suite
Etc.
Salesforce
Branch on Internet

Figure 3: Secure Cloud Access and Policy Enforcement (SCAPE)

SCAPE solutions bring cloud scale and architecture to the VPN, and integrate cloud security with security of on-premises destinations. Given its architecture, it is able to play the role of both API-based CASB for known/sanctioned cloud destinations, and in-line CASB and secure web gateway for other cloud-bound traffic.

SD-WAN solutions are a natural adjunct to SCAPE. They provide the ability to selectively pass traffic from branches out through the SCAPE, or directly to sanctioned cloud partners, for example, and to provide flexible, dynamic allocation and prioritization of flows through the SCAPE. They can also help provide network analytics data, including user/identity-based network usage information, assist with "shadow IT" detection, and with threat monitoring and response generally.

Choosing: Touchpoints for Security Decisions

IT leaders should consider:

- **The current state of baseline WAN security:** how well is IT doing at keeping branch routers up-to-date on software and correctly configured? How much effort does it take to change configurations, patch software, or upgrade? Data on these points can support a move to SD-WAN and provide savings targets as well as security goals.
- **Firewall architecture and plans:** Is the security team ready to collaborate on a new generation of security at the branch using a merged endpoint approach? If not, are they ready to at least select a platform with separately manageable firewall endpoints (VNFs) sanctioned by the SD-WAN vendor or provider? Remember to work with them to ensure capacity as well as functionality, and application performance as well as security.
- **Ecosystems:** If there is a well-designed security architecture in place, IT should make every effort to ensure that the SD-WAN solution will fit into it, at the very least feeding data into a SIEM, and ideally providing API or other integration into a SOAR environment. Managed solutions should offer 24/7 threat monitoring and response.

Future-proofing: AI and the Future of Automation

IT needs to keep its eyes on the needs of the future, not just the present. The infusion of more, and more sophisticated, AI into IT will create new opportunities for SD-WAN to improve WAN performance and availability without staff intervention.

AIOps and SD-WAN

AIOps applies AI and analytics techniques to the problems of network operations. Its goal is to provide tools able to act on behalf of IT staff flexibly, reliably, and more correctly than previous generations of automation. The main idea is that they can bring a new level of contextual awareness to automation by using machine learning and other techniques to learn about the network as used. To do that, they harness some of the tools of big data analytics to ingest and learn from diverse streams of monitoring data, bringing to bear improved abilities to parse, understand, and correlate information across data streams.

To be successful managing future SD-WANs, IT teams will need to have an AIOps tool integrated into it directly, or to feed data from their SD-WAN into an AIOps tool and provide API access for control. If integrated, the tool should have the ability to see and process data from the underlay network (whether enterprise-owned or provider-owned) as well as from the SD-WAN's control plane. Monitoring the underlay can help spot potential future problems as well as provide accurate data for capacity planning and management.

Autonomous SD-WAN

An AIOps solution can track the evolving picture of what constitutes "normal" traffic for the organization, and learn how to solve problems automatically within that context: how to make small adjustments to tune performance, how to make large changes to handle an emergency. The ability act correctly in context without hands-on direction delivers autonomous networking. Creating an autonomous network is not a switch-flip, of course: it requires cycles of learning, feedback, and adaptation, and a close collaboration between network and security staff and the AIOps/SD-WAN software. Staff transfer knowledge of how to respond to a given set of performance or security monitoring data, teaching the software about context and meaning.

To facilitate fully autonomous operations, a future-proof SD-WAN should provide both pull and push APIs: simple, REST-based access to data needed by AIOps and other tools; simple, REST-based access to control functions for security and operations automation.

Choosing: Touchpoints for Advanced Features

IT leaders should look for tools that deliver now, or have a roadmap to deliver, whether directly or via a strategic partner, AIOps functionality:

- Deeper understanding of network traffic, security, usage, usage patterns, and trends
- Proactive advice on heading off problems and improving performance
- Root cause analysis for problems that occur, including insight on security events
- Process support and integration – the ability to integrate cleanly into IT processes

With respect to managed offerings, the provider should have a platform capable of providing AI-driven analytics and automation for its own underlay networks and infrastructure. AI-boosted SD-WAN should be a straightforward addition of functionality rather than require a complete retooling of the infrastructure.

Conclusion

In choosing an SD-WAN solution, IT staff should be looking not just at the needs of the moment but at the needs of the next five years or more. Consequently, they should be looking for SD-WAN solutions that provide more than core SD-WAN functionality; they should fit cleanly into a sophisticated security architecture, and the emerging AIOps space.

IT professionals should:

- Evaluate managed and DIY SD-WAN solutions against their enterprise's network needs and their own teams skills and staffing levels
- Work with security teams to ensure a smooth integration of SD-WAN into the organization's technological and operational security frameworks
- Define a roadmap for the integration of AI into network operations and specifically SD-WAN, with the goal of achieving more autonomous networking.

About Nemertes: Nemertes is a global research-based advisory and consulting firm that analyzes the business value of emerging technologies. Since 2002, we have provided strategic recommendations based on data-backed operational and business metrics to help enterprise organizations deliver successful technology transformation to employees and customers. Simply put: Nemertes' better data helps clients make better decisions.