E-Guide

SDN & SD-WAN: Transform Network Infrastructure and Security

TechTarget | SearchNetworking

In this E-Guide:

In this expert e-guide, CIO and principal analyst John Burke of Nemertes Research discusses what key considerations to keep in mind when updating your network infrastructure with SD-WAN. Plus, explore a Q&A with CIO Matt Minetola about how his teams over at Travelport Mindset underwent a digital transformation journey.

Don't forget SD-WAN during your next network infrastructure upgrade

Enabling digital transformation: CIO talks 3-phase journey

How has software-defined networking security evolved?

Don't forget SD-WAN during your next network infrastructure upgrade

John Burke, CIO and Principal Research Analyst

Software-defined WAN has many upsides for the typical organization with a WAN of sufficient size. The technology can reduce the amount of staff time required to manage the WAN, reduce WAN and site downtime, improve application performance and dramatically reduce costs incurred from increased WAN bandwidth. But IT can't just drop any product into a network infrastructure upgrade and expect it to succeed.

SD-WAN adoption is spreading surprisingly quickly for such a young technology. But in ongoing studies of WAN economics and SD-WAN, Nemertes Research has seen a familiar pattern: IT deploys SD-WAN when it comes time for a network infrastructure upgrade.

Sometimes, refresh is driven by the age of network components or by contract lifecycle. But when the time comes for a network infrastructure upgrade, IT has to decide whether to replace with do-it-yourself infrastructure, a traditional managed WAN or network as a service. No matter which way IT goes, SD-WAN will be central to nearly all plans.

Consider the branch stack when choosing DIY

If IT chooses to go the DIY route, it then has to decide whether to stick with its existing branch stack at each location. This stack usually is made up of three or four devices: the router and some mix of firewall, optimization and wireless LAN controller.

The branch stack may have design principles or security policies that dictate a separation of duties. If those policies can be dropped or relaxed, or if the stack grew over the years without such requirements, then SD-WAN and virtual customer premises equipment platforms allow IT teams the option of collapsing the stack onto a single device -- or, at most, a pair of devices in a failover or hot-hot configuration.

Managed SD-WAN benefits both enterprises and providers

If IT decides to hand off WAN management, substantially change how its existing managed WAN is delivered or look for a new provider, managed SD-WAN will likely be its No. 1 option. After all, SD-WAN offers enterprises new possibilities for connection paths and technology diversity, cheaper bandwidth and improved WAN performance.

On the flip side, SD-WAN offers managed SD-WAN providers lower marginal costs for managing customer WANs. This is, in large part, thanks to SD-WAN's centralized, policy-based management architecture and to the fact that service interruptions on a given link become less urgent to resolve when multiple paths are available and services can continue uninterrupted.

Don't forget SD-WAN during your next network infrastructure upgrade

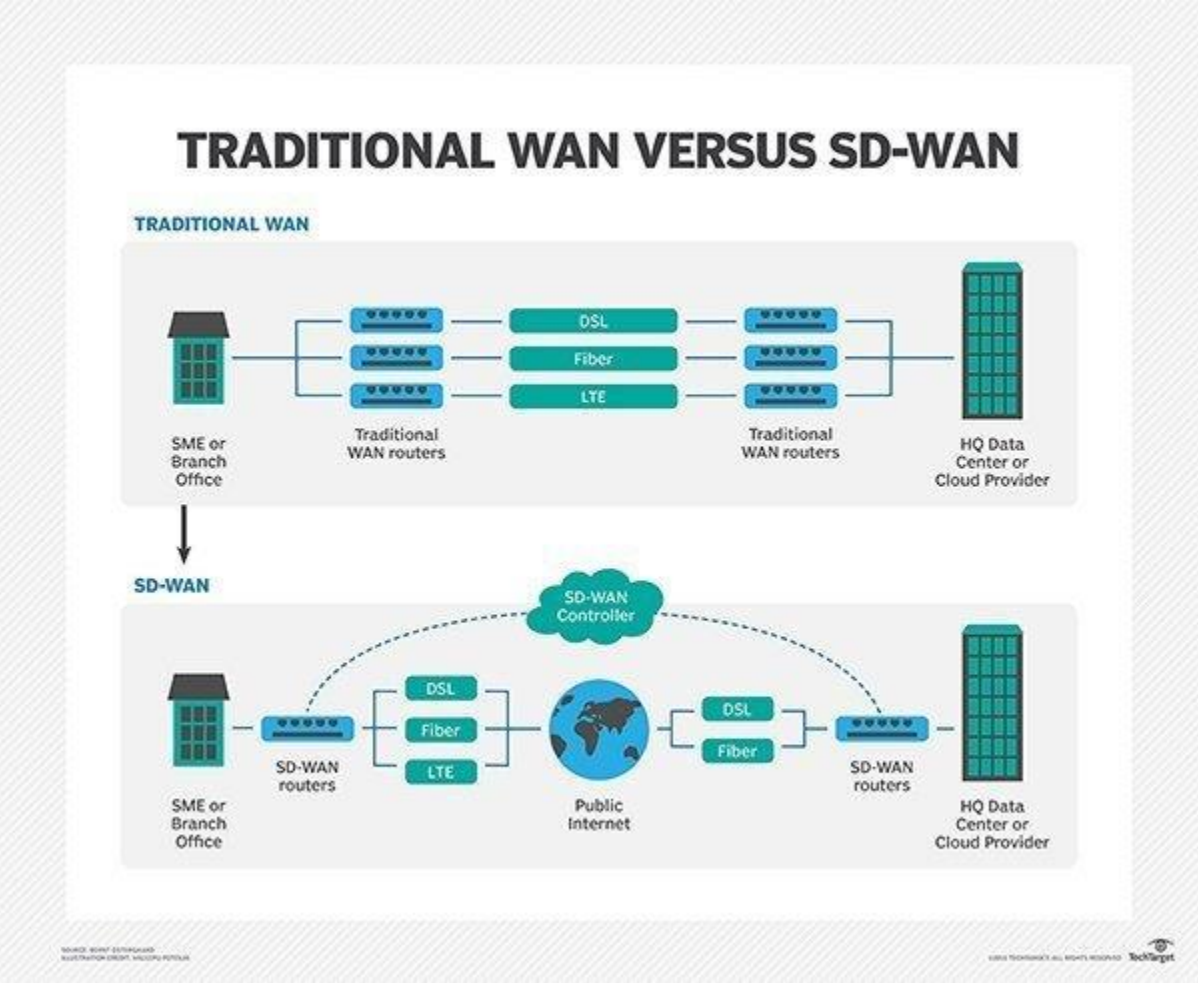
Enabling digital transformation: CIO talks 3-phase journey

How has software-defined networking security evolved?

Don't forget SD-WAN during your next network infrastructure upgrade

Enabling digital transformation: CIO talks 3-phase journey

How has software-defined networking security evolved?



Network infrastructure upgrade considerations

Don't forget SD-WAN during your next network infrastructure upgrade

Enabling digital transformation: CIO talks 3-phase journey

How has software-defined networking security evolved?

Some of the biggest considerations for an enterprise during a network infrastructure upgrade revolve around available connectivity for each specific location. Companies want SD-WAN to incorporate lower-cost internet connectivity as a primary WAN transport, even though most that have MPLS or Carrier Ethernet plan to retain it within SD-WAN. SD-WAN adopters also want the ability to have diverse connectivity providers in order to improve resilience and stabilize performance.

In some locations, business internet services may not be significantly cheaper than MPLS, however, and consumer broadband might not perform well enough or have enough support to be viable options. IT teams might not be able to achieve path diversity, as there might be only one physical route to a building, for example. Additionally, there could be only one provider in an area, making it difficult to achieve provider diversity. This is often a significant concern for companies with locations in remote or rural locations, such as manufacturers.

Some enterprises plan to keep management of last-mile relationships -- and the need to deal with all these issues -- in-house. Others plan to outsource it through a managed service provider or connectivity aggregator, even if they intend to deploy SD-WAN in-house.

IT shops on the cusp of a network infrastructure upgrade should plan for SD-WAN deployment -- if not now, then the next time around.

When incorporating existing connectivity into the transport mix, IT also has to deal with the question of the medium. If the existing link isn't handed off as Ethernet, they will need to adapt it for SD-WAN services that don't accept other connection types -- which are most of them. Some enterprises retain their routers in

this capacity, essentially using them as media converters; others look for more compact and energy-efficient boxes to drop in line. Others will instead require an SD-WAN option that can accommodate the older link interfaces, of which there are a few.

As it is with connectivity, so it is with protocols. An SD-WAN appliance may or may not speak all the protocols an organization requires in a branch box. The overall architecture will determine which protocols the appliance needs to understand. If the SD-WAN appliance has to interoperate with conventional routers, for example, it should speak Border Gateway Protocol (BGP). SD-WAN products meant to replace routers generally support current open routing standards like BGP. But if an organization's network has vendor-specific or older standards in place, it will need to carefully evaluate an SD-WAN product's ability to interoperate.

IT shops on the cusp of a network infrastructure upgrade should plan for SD-WAN deployment -- if not now, then the next time around. Either way, they should be thinking ahead to the collapse of branch stacks, the primacy of Ethernet as a link handoff and the need to get rid of any lingering remnants of routing protocols past. They should also be actively reviewing connectivity options in all their locations or finding someone -- a managed service provider or a connectivity aggregator -- who can do that on their behalf.

Don't forget SD-WAN during your next network infrastructure upgrade

Enabling digital transformation: CIO talks 3-phase journey

How has software-defined networking security evolved?

Enabling digital transformation: CIO talks 3-phase journey

Brian Holak, Associate Site Editor

Enabling digital transformation with the necessary technology is just the first step, according to Matt Minetola, CIO at Travelport. Mindset and talent are just as important.

Travelport, a $2.4 billion travel commerce platform that provides technology offerings for the global travel and tourism industry, has more than 4,000 employees and has operations in 180 countries. With a company of that size -- seeped in legacy processes -- enabling digital transformation was no walk in the park.

In this Q&A, Minetola *recounts the ongoing journey and the challenges Travelport has faced as it rethought its original, global distribution systems-centered business model, implemented new technology, retooled internal company processes and hired the right end-to-end talent. Minetola's goal: to continuously evolve and build out capabilities that improve the customer experience. In part two, Minetola discusses the technologies that make up Travelport's "digital spine."*

Editor's note: *This transcript has been edited for clarity and length.*

Don't forget SD-WAN during your next network infrastructure upgrade

Enabling digital transformation: CIO talks 3-phase journey

How has software-defined networking security evolved?

Describe Travelport's digital transformation journey: How far has the company come and where is it now?

Matt Minetola: We're probably like everyone else -- right in the midst of it. I think digital transformation is about [building] the capability, less than it is about going from point A to B. We started this probably three to four years ago, maybe longer. I'll talk about it in phases.

The first phase is the [technology] enablement piece. Are you understanding and implementing the right technologies, and are you working through the organization to try to change the skills and the knowledge base of how things get done? I would say we've done a really good job of getting through that stage.

Don't forget SD-WAN during your next network infrastructure upgrade

Enabling digital transformation: CIO talks 3-phase journey

How has software-defined networking security evolved?

Right now, we are probably working our way toward the end of the ongoing middle phase, which is really figuring out how to take these technology enablers and change the way that you deliver your business products, the experiences that you create for your customers, and how you do work across the organization. I think it is those three that must continually change. What I mean by that is you start to take the technology that you built out and have acquired solid capabilities in the first stage in order to start to change legacy processes and legacy capabilities and replace them with digital- or technology-based services, which fundamentally changes your go-to-market as well how your customers absorb and digest what you offer them.

The third phase is the capturing of that information and the learnings they provide and feeding that information and knowledge back in and asking, 'Are there new technology enablers that I need to start to reinvent in phase one?' or, 'Do the processes that I'm doing in phase two need to go faster?' It is just that constant evolution. I would say we're right in the middle of it and having a ball.

How has internal company culture helped in enabling digital transformation at Travelport?

Minetola: It starts from the top. I think, as an organization, you've got to commit to the fact that the business that you had and the way that you do things has to change. We've done a really good job of that. Our CEO, our commercial folks and all our technology folks from day one knew this is where we needed to be. Five years ago, we were a travel company that did technology and, today, we're a technology company that does travel -- and that mindset comes from the top.

What then has to happen is you've got to start to move that [mindset] down throughout the organization. On the technology side, it's about building around the technologies and

Don't forget SD-WAN during your next network infrastructure upgrade

Enabling digital transformation: CIO talks 3-phase journey

How has software-defined networking security evolved?

thinking differently about how you look at technologies. The example I would give you is 10 years ago, it was all about ERPs and optimization. In today's world, you're looking at customer experience and figuring out what technologies could enable and enhance that. That changes how you look at technology products, how you bring them on board and, most importantly, how you integrate them and start to build them out.

In the digital world, and what we [at Travelport] had full support on was really changing our skill sets and our processes and saying that everybody in the organization has to understand their larger role. It's not, 'I'm a salesperson and I'm only trying to do this one thing.' Everybody along the way is trying to understand the process and experience. I call that 'evergreen requirements building' and everybody in the organization is constantly building those.

So, on the technology side, I think we've done a good job of getting our people to think differently and implement differently. And on the business side, we've done a good job of changing the expectation of what your role is, and those two things really just fuel the transformation.

Talk about some of the challenges you faced in enabling digital transformation at Travelport?

Minetola: Talent is a key one. In today's world, you have to constantly be out there mining for the talent. Everybody is looking for the same folks and the same skills. If you ask me one of the things that I've been most pleasantly surprised with, it's our ability to attract talent. We're in the travel space. Although we're doing some really cool technology, we're not a startup. We are at a large scale. So, we have the best of both worlds [for talent]. You have the newer technology, but you can scale it. The travel industry is going through such change and it's really pushing the envelope. The most important thing that we did in this

organization was we hired in the right people early on. When you hire the right people, they then hire the right people and it starts to build on itself.

The other thing I would say is in the old world, you had experts of one, and now you need end-to-end solutions people. In the old days, you had the network expert, the database expert, the application expert, etc. In today's world, you need the person who understands the application, understands the network, understands the storage and understands the database. It's those end-to-end people who really become valuable, because the world is changing so fast that you don't want anybody to get locked down into a specific technology. At the end of the day, the solution is the integrated stack. So, the more of those people you can get, the better off you can be.

Don't forget SD-WAN during your next network infrastructure upgrade

Enabling digital transformation: CIO talks 3-phase journey

How has software-defined networking security evolved?

How has software-defined networking security evolved?

John Burke, CIO and Principal Research Analyst

Software-defined networking security, specifically microsegmentation, continues to be the No. 1 reason organizations deploy SDN in their data centers.

When actually putting SDN into production for security purposes, however, IT teams can face significant challenges. One reason for this is because SDN platforms often presuppose that IT knows what the microsegments in their network should be, even when they often don't.

In actuality, many IT teams end up deploying an SDN platform like Cisco Application Centric Infrastructure or VMware NSX to replicate their existing security zoning strategy and granular segmentation. These deployments benefit organizations by moving them into production with a new tool, and without extensively disrupting operations. On the other hand, IT teams can fail to realize the full benefits of the tools at hand.

IT teams often face the stumbling block of developing the level of knowledge about their networks required for successful microsegmentation. Organizations lucky enough to have robust network analytics already in place hold an advantage, as such analytics platforms make acquiring this knowledge a nonissue. These platforms can rapidly map out which systems talk to which, when they do so and how (e.g., what protocols or transaction types are used).

Given such a map, IT can then more easily assess where to draw tighter boundaries around system groups and how narrowly to squeeze the range of communications. Smaller groups and more restricted ranges of communications translate into improved security with reduced threat surfaces and risk of compromise. Indeed, gaining this kind of insight can be a major driver of network analytics deployments.

SDN tools are continuing to mature in scope, scalability and ease of use, while becoming more affordable.

In organizations without robust network analytics tools, IT teams should prepare to invest significant time into mapping the network manually and maintaining accurate network maps. Another option is to invest in automation and analytics platforms that keep such knowledge up to date.

How software-defined networking security has advanced

Other ways in which software-defined networking security can specifically benefit organizations include improved monitoring, establishment of security demilitarized zones and automation of network configuration.

Improved monitoring. An enterprise can use a software-defined network alongside its production network to provide a parallel network that handles monitoring and management.

This parallel network can pull replicated packet traffic from the production network using inexpensive white box switching and, perhaps, even open source software.

Security zones. An enterprise can similarly use a software-defined network to route traffic through a gauntlet of security appliances at the same time it flows from one part of the network to another. This can improve throughput and reduce costs.

Automation. By integrating network provisioning and configuration auditing into system deployments -- using infrastructure-as-code tools like Ansible or Salt -- IT can reduce the rate of misconfigurations that result in security problems and improve the rate of remediation of any problems that creep in.

The end goal for software-defined networking security

Of course, the ultimate end state of software-defined networking security in full production is what Nemertes Research calls *deep segmentation.* This is the ability to control, to as fine a degree as desired, which entities can see and communicate with which -- and how they do so -- end to end across the enterprise network.

Security compromises can be tightly constrained when every edge switch -- physical or virtual -- and every other packet-handling device can enforce security policies in a fully software-defined perimeter. In this environment, land-and-expand attacks can be slowed or potentially stopped before they get to another system.

Don't forget SD-WAN during your next network infrastructure upgrade

Enabling digital transformation: CIO talks 3-phase journey

How has software-defined networking security evolved?

The typical enterprise has a long way to go before achieving this end-state architecture, but SDN tools are continuing to mature in scope, scalability and ease of use, while becoming more affordable.

Don't forget SD-WAN during your next network infrastructure upgrade

Enabling digital transformation: CIO talks 3-phase journey

How has software-defined networking security evolved?