ComputerWeekly.com | TechTarget

E-guide

CW+ Content

SD-WAN: Hitting the mainstream

In this e-guide

In this e-guide:

For the networking industry, 2018 was the year in which interest in software-defined wide area network (SD-WAN) started to ramp up in earnest, as more and more enterprises started to assess the benefits (and pitfalls) of the technology, and more early adopters started to make concrete purchasing decisions.

For the uninitiated, an SD-WAN uses software-defined networking (SDN) technology to automate and prioritise traffic routing between distributed enterprise sites and datacentres, either by creating a transport-agnostic virtual overlay that sits on top of your preferred network infrastructure, or running as a network-as-a-service option. Centrally provisioned and controlled, SD-WAN technology is supposed to make life much easier for the IT department. That's the theory, at any rate, but what's the reality?

In this e-guide, our team of experts explore the current state of play in the SD-WAN market. As the technology moves towards

In this e-guide

the mainstream, Christian Annesley provides an overview, while Rene Millman looks at some of the supplier options for buyers.

Moving on, we take a look at some of the misconceptions that still surround SD-WAN, and maybe explode a few myths, and of course as with any network deployment, there are security concerns to consider.

Finally, we assess some aspects of migrating to SD-WAN from MPLS, first with a compare-and-contrast exercise, followed by a look at how to start a successful transition.

Alex Scroxton, networking editor

In this e-guide

Intelligent automation and the WAN: Is SD-WAN moving mainstream?

Christian Annesley, guest contributor

Sometimes in the modern era, a new technology sweeps in and adoption by business is swift because it's a certified game-changer – desktop PCs, email or word processors, say. But history also tells us this kind of step-change is the exception.

Running large, complex businesses is multifaceted, with thousands of moving parts – people, process, technology, data analytics – to consider. It means most change that we see is incremental in how it unfolds – and even more so if the benefits and scope of a technology are not that easy to pin down.

When it comes to networks, and particularly wide area networks, the shift to enterprises taking control with a software-defined approach, through software-defined wide area networking (SD-WAN), is happening more and more, for sure, but it's also not sweeping through as some predicted.

What's the story behind the journey so far? And if the cost-savings of running SD-WANs versus traditional networks aren't quite there in many cases, are

In this e-guide

network managers still missing the point that SD-WAN can deliver other benefits right now?

What's happening in the WAN?

First, let's briefly take a step back. Software-defined networks (SDN) are the future; of that there is surely little argument. In the next 10 years and beyond, SDN – and especially SD-WAN, using multiple carriers' infrastructure – will become the norm as the benefits in agility and function come through and proliferate across everything that goes on in networks.

But what about the here and now? It turns out the transition is hard for many IT buyers to rationalise because the benefit of an investment in SD-WAN is often not clear-cut when weighing resilience, flexibility and value.

This is partly because there are lots of variables in different markets in relation to SD-WAN for enterprises to ponder – and variables that give the lie to baseline justifications about what SD-WAN delivers.

Most can be disputed, but some of the arguments, let's remind ourselves, are that SD-WAN will usurp current networks.

Advantages of SD-WAN

It's cheaper to run day-to-day: SD-WAN will deliver cost reductions as internet access is cheaper than MPLS, the argument goes. The thing is, that's

In this e-guide

just not true across the board. In Europe, and especially in the UK, internet access costs are far closer to MPLS and in many customer networks the cost of MPLS is lower than that of providing internet. When you add in security considerations and firewall costs, the internet can look less attractive.

It lets you cut bandwidth and circuits: However, in reality the cost of SD-WAN cannot usually be justified on the grounds of cost savings by reducing bandwidth or the number of circuits. SD-WAN can, however, maintain business continuity at times of congestion or failure so is best viewed as an investment in productivity and customer service, more than a route to making savings.

It speeds up applications and cuts network data: Control of an applications layer is part of SD-WAN's promise, but application acceleration is around in different guises and there is scope to cut latency and traffic in various ways, so it's not quite a game-changer.

It speeds up future network deployments: That's the theory, and it will happen, but for now networks are often made of copper and coaxial cables with engineers working in holes and up poles for connectivity by hand, with some form of device being deployed before circuits can be used. In time, carriers will be able to deploy and light services faster than they do today, with most places pre-fibred and ready for central deployment, but for now that vision isn't a widespread reality.

In this e-guide

How enterprises buy SD-WAN today

If the headlines don't always quite deliver, what is the trigger for businesses to roll out SD-WAN today?

"We think this is a really interesting time in the market," says Nick Johnson, chief executive of UK-based SD-WAN specialist Evolving Networks. "Acceptance of SD-WAN as a product is growing, but every conversation we have with a company weighing up SD-WAN is naturally unique. Not surprisingly, many approach us with immediate issues to resolve rather than a strategic vision to invest in a next-gen network."

What Johnson says is true of many enterprises today is that their networks have organically expanded and become more complex, so a fix that layers in SD-WAN often looks a good value-add, but the opportunity to look at a WAN in the round is often worth taking.

"Many will have a core corporate MPLS plus extras like internet breakout. It's common for CIOs and network managers to be unhappy with their ISPs, too. One thing with the UK market is that some SD-WAN offers out there don't really address the risks around connectivity, even though it's fundamental.

"Companies need an integrated SD-WAN platform, really, with no disconnect between the software and infrastructure. When you take US-developed software and apply it with a UK ISP, we think that's a risk. UK broadband is cheap but

doesn't always compete on quality and service levels in the same way as in the US."

SD-WAN in practice – Vindis

In practice, of course, every SD-WAN roll-out is down to the fit with business processes and what needs to be upgraded. As more and more core business applications move to the cloud, for example, that's a part of the picture for many enterprises – on-premises servers can be retired when a resilient SD-WAN goes in.

If a root-and-branch WAN overhaul or roll-out isn't the most common place to start with SD-WAN, for Vindis Group – a family-owned car dealerships business with 19 vehicle dealerships and five other sites supporting its commercial operations – it was a much-needed investment in 2016.

"The business had 24 sites with some ADSL services, no real WAN and local systems at each site relying heavily on ISDN lines," says Nic Elliot, Evolving Networks' CTO. "When we came in there was inadequate resilience in the branches' external connectivity and no internet access management or control, plus no infrastructure to support VoIP. There were also no network connections between sites or between branch offices and HQ."

With servers at every branch office, with all the attendant management costs and complexity that can bring with it, Elliot says increasing bandwidth and resilience at all sites with a managed WAN was a clear business priority.

“Centralising business systems at Vindis Group HQ, including group-wide adoption of a new centralised dealer management system and Microsoft Exchange, was part of the overhaul,” says Elliot.

“An SD-WAN running over bonded ADSL, FTTC [fibre-to-the-cabinet] and Ethernet connections was implemented for all sites. The SD-WAN uses connectivity provided by us including a cross-carrier network, with a mix of Ethernet services from Virgin, BT and TalkTalk, and bonded ADSL and FTTC at sites for which Ethernet was either non-viable or not cost effective. It’s a robust set-up that means key business systems are now hosted at Vindis HQ, which is real step-change.”

To manage this complexity, the SD-WAN is making automatic, intelligent policy-based routing decisions for all data transfers. As well as allowing for the automation of routing and quality decisions, this abstracting of network control to the WAN also enables transparent failover in the event of circuit failure.

Elliot says for Vindis the SD-WAN has allowed the group to make cost savings by using VoIP in place of traditional telephony, as well as seeing savings arising from central monitoring and management of all internet usage.

"As you would expect, there are also savings arising from eliminating branch office servers and relocating central business systems to the HQ," he adds.

This long list of benefits from a big-bang SD-WAN upgrade is unusual in that most businesses take a far more incremental approach to a networks investment, but it certainly showcases some of the potential in software-defined networking.

The analyst view – pilots and process

If some suppliers offering SD-WAN emphasise how the renewal of contracts on MPLS circuits is often the trigger for enterprises to start a conversation about SD-WAN, Gartner analyst Neil Rickard makes the essential point that an SD-WAN set-up most likely makes use of MPLS rather than replacing it.

"You don't swap one for the other. Any rethink in relation to a WAN is premised on building better, more agile networks. You might cut back on MPLS but it would be odd to look to escape it altogether. In essence, SD-WAN is a new generation of edge device, and it gives you any connectivity – not just broadband internet but whatever is fit for purpose."

Rickard makes the point that adoption of SD-WAN has to be approached with the right critical mindset to make the most of what is still a relatively immature proposition in some respects.

“This is a market historically characterised, until quite recently, by the purchase of reliable routers from large suppliers. With SD-WAN today there are already over 40 viable vendors in the marketplace with products, but all have different approaches and different feature benefits. To that extent, it always makes sense for an enterprise to be quite process-driven and granular and analytical when weighing up SD-WAN – and that includes doing a small-scale pilot to understand the risks and the benefits.”

Rickard adds that the rise of SD-WAN as a managed service is also changing the landscape again.

“How do enterprises source SD-WAN? Once there were no managed providers offering it – you had to buy the boxes and run your network. Now, though, we do have managed SD-WAN service providers from network-owning telcos and more. Many organisations will like it as a managed service, in fact, but it’s not a cure-all.

“The temptation with SD-WAN is to believe the devices are all self-learning and adaptable and it will make running the network easy. But that is false because most networking is still defined by the underlying links. Troubleshooting should get easier with SD-WAN, for sure, but the problems to be fixed won’t just go away. The savings story with SD-WAN is not so much to do with the underlying network but more about the promise of better controls.”

Culture change and automation

The human element when it comes to any SD-WAN roll-out is also fundamental, as Patrick Hubbard, head geek at IT monitoring outfit SolarWinds, is keen to emphasise.

“There are two sides to this. There is the caution that many network managers might naturally feel about backing an automation technology that should in theory cut network roles in an organisation. And there is the way that any learning to make the full use of SD-WAN should deliver real transformation to an enterprise,” he says.

“In other words, there is lots to chew on when it comes SD-WAN. It shouldn’t just be approached as an upgrade on the wide area network but for the transformative potential of the control and analytics it offers,” says Hubbard.

“Of course existing networks are business-critical and often bespoke and manually configured – that’s the usual context. It means it is usually too risky to just jump in and undertake a big overhaul, as in your unusual example, but that doesn’t mean that a sensitive, small-scale upgrade shouldn’t also be a jumping off point for long-term strategic change.”

Hubbard argues that the range of issues to consider with SD-WAN and wide area networks generally is extensive in technical terms, but the cultural shift mustn’t be ignored by network managers.

"Yes, you need to look at every element of a network and what tools will work – 4G wireless, whatever – but there are so many other aspects to understand when automation, machine learning and the software layer is added.

"Those working on the network need to adopt more of a DevOps mentality in relation to SD-WAN and recognise that you can automate yourself into a new skillset and a new career. It's a big step away from trying to keep the lights with a traditional network – but exciting, too.

Troubleshooting or transformation?

In a sense, what Hubbard and others are arguing is that SD-WAN, whatever its current substantial shortcomings and ROI gaps, does offer the promise of a way ahead that's properly transformative: a single view of the network, with controls and analytics that are more like programming in their functionality and scope.

"The days of reactive networks firefighting have to be consigned to history soon. SD-WAN is at least about being proactive and taking control with software. It needs to be measured for that potential just as much as for any projected hardware cost-savings.

"We are still getting used to the transformative potential of automation – still adapting to what it means in practice. It does often mean you can do things that just weren't possible previously, and that means you have to recalibrate as an organisation. What's the real bottom-line advantage to making this step?"

In this e-guide

What are the current SD-WAN options for enterprises?

Rene Millman, guest contributor

One of the biggest developments in enterprise networking at the moment is the emergence of the software-defined wide area network (SD-WAN).

This next generation wide area network (WAN) technology is being touted as a means of moving away from proprietary or specialised WAN technologies to something more open, flexible and cloud-based.

According to Gartner, by 2020, SD-WAN will be a $1.1bn market, while IDC predicts this market will be closer to $8 billion in size by 2021.

Frost & Sullivan recently revealed that 94% of businesses have deployed, are deploying or will deploy an SD-WAN in the next two years. So, it looks like SD-WAN is gaining traction, but what is SD-WAN and how will it change the humble enterprise WAN?

Simply put, SD-WAN streamlines enterprise connectivity between remote locations and branch offices, using software to create encrypted network tunnels between endpoint devices to produce a private WAN over simple circuits.

It uses broadband internet, 4G Long Term Evolution (LTE), or multiprotocol label switching (MPLS) access and centralises control in the cloud.

The upshot of all of this is the enterprises should, in theory, gain greater flexibility and performance in their corporate network as well as better economics.

Benefits of SD-WAN

How is SD-WAN going to make IT operations more effective? Gina Nomellini, chief marketing officer at network provider GTT, says that as IT and applications today are often more geographically diverse than their user base, SD-WAN is helping make the network simpler to configure and control centrally.

“SD-WAN allows you to consolidate your network assets – old and new – and extend control all the way to the edge for more efficient branch networking and secure connectivity to cloud applications,” she says.

She adds that using split-path routing and dynamic-path control, SD-WAN lets enterprises route their internet traffic locally, without having to re-route through the WAN and squeeze through the datacentre-hosted security appliance. It improves cost efficiencies and enhances networking flexibility, without sacrificing one of the most important business drivers, performance.

Richard Kitney, hybrid connectivity specialist at Orange Business Services, says that a compelling initial benefit will be in switching on application visibility before

any business goes headlong into delivering services to the cloud or re-architecting to a hybrid network topology.

“That level of visibility gives a lot of usage detail about what applications are running on the network, how much bandwidth is being consumed and where any problems lie. This in turn enables the business to have an informed discussion about current applications and how they can be improved,” he says.

Fitting in with existing technology

If a business already has inter-site connectivity, either through site-to-site VPN, or MPLS, then it will probably already have technologies in place on the network to support multi-site implementation of SD-WAN, according to network infrastructure design firm LAN3’s SD-WAN team manager, Roger Collins.

“SD-WAN solutions, that include a dedicated backbone, will provide the benefits of MPLS at significantly reduced cost while providing reduced complexity and ease of administration (when compared with site-to-site VPN solutions). The technical prerequisites will be similar to these existing technologies and will include ensuring non-overlapping subnets between locations,” he says.

Donna Johnson, vice-president of product and solution marketing at Cradlepoint, says that the main thing an organisation should think about before implementing SD-WAN is to really understand their use case – what are

the primary problems they're trying to solve or what do they think they'll accomplish with SD-WAN?

“Because the technology itself is so broad, it's important to go into a project with a definite idea of their end goal. Without that, it's easy to get lost in the very many different options and technologies that are included in SD-WAN,” she says.

Finding the right SD-WAN

Marc Sollars, CTO at integrator Teneo, emphasises the need for education on SD-WAN capabilities and risks.

“Vendors need to help prospects identify potential SD-WAN risks and what outcomes they need because each vendor goes about this discussion differently,” he says. “It’s possible to have some zero-touch SD-WAN deployments, because of a rapid go-to-market plan or a tough deadline, but I know of roll-outs where networks fell over because the risks were still not fully assessed.”

He adds that the corporate decision-making unit is broad and advocates a workshop approach, ensuring that all stakeholders – CIO, CISO, etc. – are on the same page, in terms of knowledge and business outcomes.

“I know of a transportation company that thought they had every risk covered, but we showed its team additional capabilities that needed further discussion. I

know quite a few SD-WAN experts that are saying prospects have had some Kool-Aid from vendors but not the truth," says Sollars.

Kitney says that enterprises should look out for end-to-end technology. "For example, for quality of service, you really want that to be delivered across the board".

From branch site, to HQ, to cloud, enterprises should ensure the quality of service can be maintained across the infrastructure.

"It makes things problematic when you're crossing boundaries from SD-WAN to mixed connectivity environments to cloud and have to translate everything and make it work in an ad-hoc fashion. There needs to be a ubiquitous infrastructure end-to-end," he adds.

The options for SD-WAN

There are a few approaches on how to adopt SD-WAN technologies. Whilst all SD-WAN vendors will help reduce the costs associated with MPLS, most will achieve this by reducing the volume of traffic which is sent down the MPLS circuit, according to Collins.

"Most appliance-based SD-WAN solutions use the 'public internet', where latency is unpredictable, so MPLS is still a necessity for latency-sensitive applications," he says.

Collins adds that this often requires the maintenance of existing routing devices and an additional 'overlay' SD-WAN router/firewall. "This means that budget needs to be sought to purchase these additional devices and resources required to manage the devices," he says.

Collins says that for companies with several office locations dotted around the globe, latency is a significant challenge and MPLS has, up to now, been the only answer (but at a price!).

"However, there are now viable alternatives, where the savings can be substantial, and little compromise to latency. These approaches hinge on the provision of an affordable, SLA-backed global backbone, where latency is minimised," he adds.

Deploying SD-WAN

Sollars says that when it comes deploying SD-WAN, phasing of migrations is essential.

"Many companies want better performance from existing applications in a particular region or division, or they want greater reliability from an enterprise-wide application – such as video, collaboration tools, Office 365, and so on," he says.

"We have a customer considering SD-WAN for 1000+ locations and we're carrying out phase one deployment to a few sites. Global-level deployment only

will follow when the customer's IT team is comfortable with application performance."

He adds that as an alternative, companies that target particular outcomes from SD-WAN, mitigate risks and keep implementation simple, are more likely to be successful. "Some firms only do cover one area of the business to see a clear benefit. One firm switched off its MPLS circuits and moved to public internet circuits to save costs and it's on target to save $750K a year."

When deploying SD-WAN the network underlay is a key part of the SD-WAN architecture. It's complex and often underestimated, according to Mark Weait, VP and head of Europe at Tata Communications.

He says that networks are far more complex than they were a decade ago, with infinitely more applications to consider: some on-premise, some in the cloud, some transitioning between, and many of these are mission-critical.

"These applications need to be secure and free of congestion to avoid QoS issues arising. Businesses starting to implement SD-WAN need clear visibility of all applications, as well as a clear understanding of what should go in which queue and, when congestion occurs, what should take priority," he says.

He adds that more importantly, where does the low-priority traffic go during busy periods? "When it comes to optimising voice for SD-WAN, architectural underlay is vital for the overlay to work efficiently. This is especially important for

businesses looking to reap the benefits of unified communications (UC) and cloud-enabled services such as SIP trunking."

SD-WAN evolution

There will be significant developments and challenges for next generation SD-WAN deployments over the next 12 to 18 months.

According to Manish Aggarwal, the AVP of technology at design and engineering firm Aricent, there are interoperability challenges that need to be overcome.

"The industry requires a set of agreed, uniform interfaces so multiple-vendor components in overall SD-WAN ecosystems can interoperate via standard protocols and APIs," he says, adding that the MEF industry association has started working on this.

Aggarwal also expects the development of intent-based SD-WANs as this will allow rapid and automatic provisioning of required network elements. "It will use capabilities like AI (Artificial Intelligence), ML (Machine Learning) & Cognitive Analytics to learn the characteristics and performance of network flows/applications and configure the best possible automated paths and policies."

Next Article

In this e-guide

Four misconceptions regarding the benefits of SD-WAN

Robert Sturt, guest contributor

When any technology or service is marketed heavily, a number of common misconceptions and concerns may arise. In the context of software-defined WAN, vendors market IT management features in a way that loses the original benefits of SD-WAN, in some respect.

SD-WAN is frequently touted as the savior of WAN pricing, flexibility and performance. But, as with every technology, unlocking the benefits of SD-WAN requires thought and attention. This article addresses common concerns and misconceptions IT teams have when considering SD-WAN technology.

Misconception No. 1: Internet connectivity as the panacea

The first misconception is SD-WAN is an internet-based technology that's unable to use other types of WAN interfaces.

The overall SD-WAN vision is one of an agnostic WAN technology positioned to use any network connectivity type, coupled with security and traffic prioritization. The product development reality for SD-WAN is somewhat different, however,

as marketing often defines the feature sets with internet backbones as the basis for achieving cost savings.

SD-WAN does offer cost savings, especially when compared with Layer 3 virtual private routed networks like MPLS. In order to achieve those savings, SD-WAN architecture uses lower-cost connectivity in the form of internet connectivity. But with the abundance of "internet cost saving" marketing, IT teams are led to believe SD-WAN *only* supports internet-based connectivity -- note that SD-WAN vendors or providers can position their offerings as they see fit.

The architecture of most current networks, however, is based on a hybrid of broadband circuits that use different combinations of MPLS, virtual private LAN service and optical point-to-point or multipoint connectivity. This hybrid network architecture helps enterprises align their business requirements to the right design.

In addition to cost savings, the benefits of SD-WAN exist as byproducts of software feature sets. These benefits include granular security, quality of service (QoS) based on connectivity state and management simplicity. In short, internet connectivity is only one benefit to drive cost savings with SD-WAN.

Misconception No. 2: SD-WAN replaces MPLS

From the beginning, SD-WAN was positioned as a replacement technology for MPLS. While there is a certain truth in the adoption of SD-WAN as a replacement for MPLS, private networking remains a component of both hybrid architectures and software-defined networks.

The drivers behind internet-based SD-WAN are created out of mobility, public cloud-based access and agility. Where guaranteed end-to-end global performance is required, however, private IP continues to be the prevalent technology. The internet as a VPN with added SD-WAN functionality may be a capability that's *good enough*, but private IP circuits are the way forward when it comes to key corporate global locations.

SD-WAN benefits businesses where multiple branch offices require a standardized low-cost capability. In contrast, MPLS suits headquarters or hub locations where predictable application performance is a must-have.

Misconception No. 3: One is better than the other

In short, internet connectivity is only one benefit to drive cost savings with SD-WAN.

Agility is a significant benefit of SD-WAN, as the technology presents a setup that can be quick and relatively easy to deploy. It is a misconception, however, to think SD-WAN technology can solve application performance issues in all

scenarios. In all instances, IT teams should carefully pay attention to connectivity elements, including support and path performance.

The internet offers multiple connection options, including wireless 3G and 4G and copper or fiber broadband, which allows any business to quickly establish connections. But if the cellular signal is degraded and broadband performance is limited, applications may perform in an unpredictable manner. While it is true SD-WAN offers effective feature sets, it is a misconception to think all problems may be solved using the technology.

Remember that SD-WAN is an edge technology in terms of how it treats applications, which is why MPLS still acts as a component of architectural design. With any internet-based technology, QoS is only applicable locally and not end to end.

Misconception No. 4: SD-WAN replaces WAN optimization

SD-WAN and WAN optimization complement each other in respect of their feature sets. With WAN optimization, the focus is on caching, TCP optimization and compression. SD-WAN services offer a more direct traffic treatment, with added benefits of sensing path condition in terms of bandwidth, loss and delay. The two technologies are not the same, although SD-WAN services are gradually incorporating WAN optimization techniques.

In this e-guide

IT teams need to evaluate SD-WAN technology

To conclude, the hype and marketing around SD-WAN cause many of the misconceptions and concerns. As with any new technology, the SD-WAN buzz often distracts from the need for IT teams to conduct thorough network architecture research with due diligence.

We've witnessed telecom services adapt and grow to meet business demands over the years. The changes brought about by SD-WAN services are perhaps the most significant due to the shift in the way we use connectivity. As Layer 3 VPNs moved customers from limited private IP, SD-WAN is moving customers into a world of bring your own device and cloud-based accessibility, with network performance and security. Enterprise users need more from connectivity, along with the ability to seamlessly work, collaborate and access resources from wherever they're located.

The benefits of SD-WAN are promising. But IT teams should consider SD-WAN from a technical product ability viewpoint, rather than from marketing statements about it, which often mask the required detail to make an informed procurement decision.

Next Article

In this e-guide

Securing the SD-WAN: The next network challenge

Christian Annesley, guest contributor

The arguments for deploying a software-defined wide area network (SD-WAN) are becoming better known as the technology continues its journey into the enterprise mainstream, even if there remains a bewildering plethora of networking setups that take the name.

But perhaps the essential question that arises when an enterprise is transitioning from traditional branch-and-datacentre connectivity, using multiprotocol label switching (MPLS) circuits most likely, and towards direct internet access and SD-WAN technologies is how to navigate the security risks. There's a need for visibility, in particular, into all those service dependencies spread across the internet.

Alexander Anoufriev is CISO of network intelligence cloud platform ThousandEyes. He said SD-WAN adoption is frequently viewed as an easy way to take the sting out of the inherent unpredictability of internet transit because it uses metrics, such as overall latency, to execute defined policies.

“But while these metrics give SD-WAN a certain level of ‘internet awareness’ and enable it to make decisions based on path performance, it’s important to remind ourselves that an SD-WAN doesn’t control the internet,” Anoufriev. “If something goes wrong, SD-WAN can’t tell you what the problem is or who’s responsible.

“It can’t tell you if an upstream ISP is dropping packets, or if a Border Gateway Protocol (BGP) hijacking has put your users at risk. It can’t even tell you if your performance is in line with area norms.”

It’s a good point. And remember, too, all the external dependencies that are needed to reach applications and services. These include BGP routing, a variety of internet service providers (ISPs), DNS service, cloud security proxies, content delivery networks (CDNs), DDoS protectors, and others – so you need to see every hop in the network path, along with detailed loss, latency and jitter metrics.

“Relying on SD-WAN as your sole source of internet visibility is like relying on sunglasses as your sole source of sun protection,” said Anoufriev. “Sure, you have some limited coverage, and it will undoubtedly influence your perspective. But you’re in for a nasty burn if you’re going outside the shade of your datacentre or branch office unprotected.”

SD-WAN as a service

While we might expect Anoufriev, who works for a security-of-networks cloud platform, to emphasise the need for constant monitoring of the SD-WAN, he's clearly not wrong that many flavours of SD-WAN seem to land with a certain amount of baggage in security terms.

Jan Hein Bakkers is a networks research manager for the analyst group IDC and said the immaturity of a fragmented marketplace shouldn't be overlooked.

"There are so many products, propositions and players out there – DIY, managed services from different telcos, SD-WAN startups, networking companies that have moved into the space, and so on," he said. "They are far from all being the same and there is no SD-WAN standard.

"In fact, I would go so far as to say interoperability and standardisation in the space is non-existent. Buyers need to understand that, and therefore take the trouble to understand fully just what they are tying themselves to when they do make a pick. Because they all have a different story to solve a familiar problem of networks reliability, performance and bandwidth."

So these different plays in the SD-WAN marketplace need to navigated, for sure, and it's this that will or should govern the security approach taken by an enterprise CISO or CIO.

In this e-guide

Security proposition

We should recognise, too, that some parts of the marketplace for SD-WAN are heavily focused on the security proposition and are effectively selling secure SD-WAN as a service. The push is being made on the basis that the rise in cloud services has introduced complexity to the network that needs a security-related response to protect internet traffic.

The likes of Cato Networks, Zscaler, VeloCloud from VMware and Cisco's SD-WAN offer are all offering a version of this kind of protection proposition, one way or another, and for some network buyers one of these offers could well deliver a drop-in solution to an otherwise knotty problem.

Zscaler's proposition, for example, still requires an SD-WAN partner in the mix but has been set up to make it easy to migrate from hub-and-spoke to a cloud-enabled architecture by enabling secure local internet breakouts for branches.

"Simply route internet-bound traffic to Zscaler and immediately begin inspecting all traffic – all ports and protocols, including SSL," it said. "You can define and immediately enforce access and security policies across all locations from a single console."

Cato Networks, to take one more use case, posits the argument that SD-WAN's introduction of internet transports into MPLS WAN expands capacity and

offloads internet-bound traffic at the branch, but fails to address the network security requirements of accessing internet and cloud resources.

Its proposition to make this safer is “a fully converged global SD-WAN with built-in network security, delivered as a cloud service”.

“SD-WAN edge device is the enabling network infrastructure and core capabilities, such as policy-based routing and transport-agnostic overlay, are extended to address problems with traditional SD-WAN.”

It’s complicated

Yet, these end-to-end, embedded-secure-SD-WAN-in-the-cloud offers are only a part of the picture, of course – and most CISOs would be wise to remind themselves of this.

Donna Johnson, vice-president of product marketing at 4G networks business Cradlepoint, said: “One thing SD-WAN has done poorly has been overselling the simplicity of SD-WAN insertion.

“While it might be straightforward for some, there’s lots to think about and many companies don’t have a good understanding even of the applications in their setup. For a more traditional SD-WAN deployment, that’s something that matters”

In terms of security, Johnson makes the point that SD-WAN projects should always be coordinated jointly by networks and security functions.

“For example, you might find that a firewall rule stops SD-WAN in its tracks, and many companies don’t understand their router set-ups, which can get quite complicated over several years of network changes and additions.”

Securing the network

What other kinds of SD-WAN security might be reviewed by an enterprise considering a deployment?

Paul Dawes is chief executive of Mode, which has a particular offer in the SD-WAN market – offering a “global overlay” for carrier-grade networks like Microsoft Azure to ensure a high-performing cloud private network. He said the starting point has to be deciding what kind of SD-WAN proposition is in the frame.

“Are you going to opt for a more traditional network deployment, with firewalls and web gateways, but with software delivering a new level of control and strategic visibility, or go down the outsourced model offered by Zscaler and the like? These two options are two among many, yes, but the point is they are worlds apart in terms of architecture and worlds apart in terms of the kind of attentions that will be needed for the new WAN to deliver and be secure.”

Mode itself is focused on the middle-mile of the network, and Dawes said its offer is important in the space in security terms because it offers a third way – a private core backbone – that's an alternative to MPLS and the internet, delivering encryption and quality of service.

"The big question with security and network architecture is whether you can deliver end-to-end encryption of traffic? Are your keys exposed anywhere? You have to be able to trust the carrier when it comes to encryption."

Attitudes to security will also vary a lot based on context. Where a really large enterprise (or perhaps a company working in a highly regulated space) will have a CISO conducting security audits and asking about vulnerabilities in a systematic way, including decrypted traffic, in many organisations there won't be this kind of detailed scrutiny and red lines that cannot be crossed.

But enough theory. Let's look at a couple of companies deploying SD-WAN in practice.

SD-WAN and the global law firm

Mode has been working on an SD-WAN deployment with a large law firm with a global footprint. The firm has a sophisticated document management system, high-billing staff and demanding clients – and it needs a reliable and secure network to match, with a 15Gbps backbone and end-to-end encryption.

"With SD-WAN, their quality bar does not change," said Dawes. "In this case, the firm ruled out the cloud-based SD-WAN security options because the way that encryption works in those contexts wasn't quite right for their needs, with data being decrypted in another's infrastructure."

Instead, the firm opted for Mode's private backbone allied to orchestration using SD-WAN.

"Once their CISO understood our private core offer it sped things up," he said. "We have to show how we handle a DDoS or a compromised POP [point of presence], but the combination of SD-WAN and private core means that, for the firm, even in the worst case scenario, traffic just routes over the internet."

Like most SD-WAN deployments, a phased roll-out is also an important part of the security picture, with trials before wider adoption.

"One nice thing about SD-WAN is the way the orchestration means you can selectively implement changes," said Dawes. "That's essential for a big enterprise, and over time, bandwidth growth can be managed dynamically, too."

How Everyday Loans deployed SD-WAN

Another who has been on a journey with SD-WAN and security is Tony Sheehan, technology and infrastructure manager at UK-wide bad-credit loans provider Everyday Loans.

"The company is 12 years old, is a Citrix user and is a branch-based business with a head office and 40 branches," said Sheehan. "The impetus for adoption of SD-WAN was reliability and the need for more bandwidth, even if our need in the branches isn't that great, with just a few users in each location."

The company was using MPLS over EFM copper, with apps delivered from a central datacentre. When an upgrade was on the cards, about 18 months ago, he said Cato Networks' cloud-based SD-WAN was a good fit once he explored the service.

"We are quite a simple business and wanted a simple deployment. We don't have the security dilemmas of some others, either. We are committed Citrix users, too, and ease-of-adoption without a big investment was very appealing. The IT networking integrator LAN3 has supported us on the journey at every step, and made it simple."

Everyday Loans' locations are in town centres, where the most reliable option is fibre in theory but there isn't universal availability, said Sheehan.

"Our copper connections work for our needs, backed up by a 4G router, and with Cato providing secure tunnelling to Cato Cloud with its Cato Socket SD-WAN device," he said. "Cloud datacentres are integrated via a tunnel from the Cato Cloud to the VPN Gateway, which is agent-less."

When it comes to security, Sheehan said there was the potential for increased attack exposure with internet into the branches, but Cato's services such as firewall-as-a-service and other security offers gives the protection that's needed. "Our security before was quite traditional, with everything coming back to the datacentres and with a tightly controlled perimeter," he said. "That's still there, but the SD-WAN setup has introduced different parameters that Cato's services are able to cover off."

Now the branches are using web interfaces, and Office365 and other cloud apps either back into the datacentre over private links or by using internet breakout that's protected.

"We've moved from hub-and-spoke to a multi-breakout network with a single admin interface," said Sheehan. "It's working well, though it is still relatively early days. There's a security audit we've started, to establish some new baselines and some new exposures we need to fully understand as we embrace cloud more and more. We are using analytics to keep track of our connection reliability, too."

As for encryption, he said he trusts Cato encrypts between points, with site-to-site standard tunnelling and internet breakout as per the browser request.

"I'm really pleased so far," said Sheehan. "We're not a fintech but a fairly traditional financial services company, so having a simple-to-manage infrastructure remains the key.

"We don't want to have to employ an admin team to run a 100-point network, so easy administration and deployment is just the ticket," he said. "Making better use of new network analytics capabilities from here is also on my to-do list."

Next Article

What are the benefits of SD-WAN services vs. MPLS?

Carrie Higbie Goetz, guest contributor

When comparing the benefits of SD-WAN services vs. MPLS for unified communications, organizations probably won't find many tradeoffs. Software-defined WAN is poised to make a difference in the wide-area space because of its simplicity and ease of use. It also provides more broadband connections, which are less expensive than MPLS connections to carriers in many geographic markets.

It's simply better to look at UC network enhancements from an SD-WAN perspective. SD-WAN services manage UC traffic by increasing bandwidth for high-volume data, such as voice and video. The WAN will be easier to administer and is open to more types of circuits than a traditional MPLS-to-MPLS circuit, which may not be available or affordable in all locations.

In fact, software-defined services, both local and wide-area, boast ease of use as a key feature. They do not require the advanced specialists for configuration and administration like traditional MPLS and other admin-heavy equipment require.

The benefits of SD-WAN services can be especially helpful for remote and home offices where broadband services are available, but MPLS may not be. In the past, gateways have been required to connect those locations, or the administration has required multiple protocols and profiles for those locations to work.

SD-WAN services also offer an overlay of security, as open internet circuits have not always been the most secure. One final advantage SD-WAN has over MPLS is the ability to manage all circuits in one place at the same time, allowing for easier expansion.

Next Article

In this e-guide

4 steps to start a successful migration from MPLS to SD-WAN

Steve Garson, guest contributor

Over the past several years of deploying software-defined WAN, there's been a shift in the way enterprises move from MPLS to SD-WAN technology. Increasingly, the question has become less about *if* SD-WAN will be adopted and more about *how* to shift to SD-WAN.

After assessing the SD-WAN options -- preferably with input from consultants -- organizations must still go through the practical steps of moving off MPLS. Here are some of the less obvious actions to take to ensure a smooth transition from MPLS to SD-WAN.

1. Read your MPLS contract

For starters, when migrating from MPLS to SD-WAN, you need to understand some basics about MPLS contracts. MPLS contracts are normally structured on

a multiyear basis -- typically three years. Service pricing includes an MPLS port charge and a local loop charge. The MPLS port charge will be for the actual MPLS services, while the local loop charge is for leasing the infrastructure from the local carriers. Service-level agreements and break terms will be spelled out in the contract.

Your contract should clearly describe how quickly and easily you can break away from MPLS. Carriers know this, so they may be reluctant to provide a copy of the contract if you don't have one. This is a problem, particularly for companies that have gone through mergers and acquisitions in which the people who negotiated the service are longer be with the firm.

At other times, foreign carriers might provide only a native-language version of the contract. If that's the case, hire a professional translator, if necessary; it's well worth it. Bottom line: Do whatever you need to do to get hold of that MPLS contract early.

2. Termination charge and minimum commitment

When moving from MPLS to SD-WAN, the moment you know you'll need internet lines, order them.

Once you get a version of the contract, you'll need to understand a few things. The first is the termination charge. Most MPLS contracts will penalize you for early termination. The provider might say you can break the contract, but you'll

have to continue paying a charge for the contract term as if you were still using the network.

MPLS providers need the termination charge, in part, to protect them against local loop costs. They lease the local loops from the carrier and are locked into them for the duration of the contract. Understanding this fact might give you some negotiation leverage. You can look into paying the local loop charge, for example, and save on the MPLS port costs, which constitute about 30% of the overall costs.

Next, investigate the clause laying out the minimum commitment. MPLS contracts will often commit you to annually spend 70% to 80% of your actual annual spend. If you've increased your MPLS usage for any reason during the terms -- due to new locations or traffic surges on variable rate ports, for example -- you could find that you've met the minimum break requirements well before the term completion.

3. Move to month-to-month MPLS services

Ideally, you'll be able to schedule your transition from MPLS to SD-WAN when the MPLS contract is up for term. If that's not possible, or if you need the flexibility -- to give you time to install internet lines, for example -- you might have other options. MPLS providers often will permit you to go month to month if you negotiated this at the start of the contract.

Keep in mind that monthly MPLS contracts can be very expensive. Carriers will discount MPLS port prices on multiyear contracts by as much as 60%. Once you go month by month, you'll often lose those discounts.

4. Order internet lines ASAP

This can't be said this enough: When moving from MPLS to SD-WAN, the moment you know you'll need internet lines, order them. Yes, SD-WAN can deploy faster than MPLS, but don't be fooled -- that's when compared against low-cost broadband circuits. For high-quality, dedicated internet access, you'll need the right fiber plant, and that can take nearly as long as getting MPLS in place.

The consequence of waiting can catch enterprises by surprise. At one Fortune 100 customer of mine, I advised early on to start their internet service provider installations. They waited, and when they wanted to cut over from MPLS, internet access wasn't available. The result: They ended up paying $250,000 more in MPLS charges as they waited for internet fibers to be pulled to their various premises.

Once you've made your decision to go with internet, place the order. Leave at least 10 to 12 weeks to get internet circuits installed. You'll need to identify the minimum point of entry (MPOE) for each location, which is the point at which a telecommunications provider's wiring crosses or enters a building.

This often occurs in a box on the outside of the building or possibly in the basement. It's an area in your building that usually looks like a closet or a box. Here are some sample photos to send to your branch offices to identify the MPOE.

Getting more CW+ exclusive content

As a CW+ member, you have access to TechTarget's entire portfolio of 140+ websites. CW+ access directs you to previously unavailable "platinum members-only resources" that are guaranteed to save you the time and effort of having to track such premium content down on your own, ultimately helping you to solve your toughest IT challenges more effectively—and faster—than ever before.

Take full advantage of your membership by visiting www.computerweekly.com/eproducts

Images; stock.adobe.com