SD-WAN as a Managed Service

Your complete guide

Cisco Powered | zen

Contents

Introduction

2020 accelerated many pre-existing trends in technology, from the rapid shift of workloads and data to the cloud, to the migration of many workers from densely packed offices to remote locations, including their own homes.

This has raised questions as to whether traditional approaches to wide area networking offer the sort of flexibility that organisations need today, as they increasingly embrace digital transformation.

Networks designed five to ten years ago were often built for a world that still assumed key business workloads and applications would largely exist in the corporate data centre, and where meetings tended to take place face to face.

However, digital transformation means companies increasingly demand secure access to enterprise applications and data that exist partly or entirely in the cloud.

At the same time, the Covid pandemic has highlighted the need for remote and mobile workers to have full access to corporate networks, both in terms of access to data and applications, and to support more robust communications, for example via video conferencing platforms.

A further consideration is how these changes affect the organisation's security posture, whether that means accommodating flexible, mobile and remote working or ensuring the integrity of the increasing volume of traffic heading to and from the cloud.

So as legacy networks - and the contracts associated with them - come to the end of their lives, enterprises and other organisations are considering whether other WAN architectures are better able to support their changing business ambitions.

Increasingly, organisations are considering whether Software Defined Wide Area Networking (SD-WAN) gives them the flexibility and security they need.

This whitepaper will give an overview of SD-WAN, with a particular focus on managed SD-WAN, highlighting how it resolves the limitations of conventional enterprise WAN approaches, addresses modern security concerns, and how it both parallels and supports companies' digital transformation efforts.

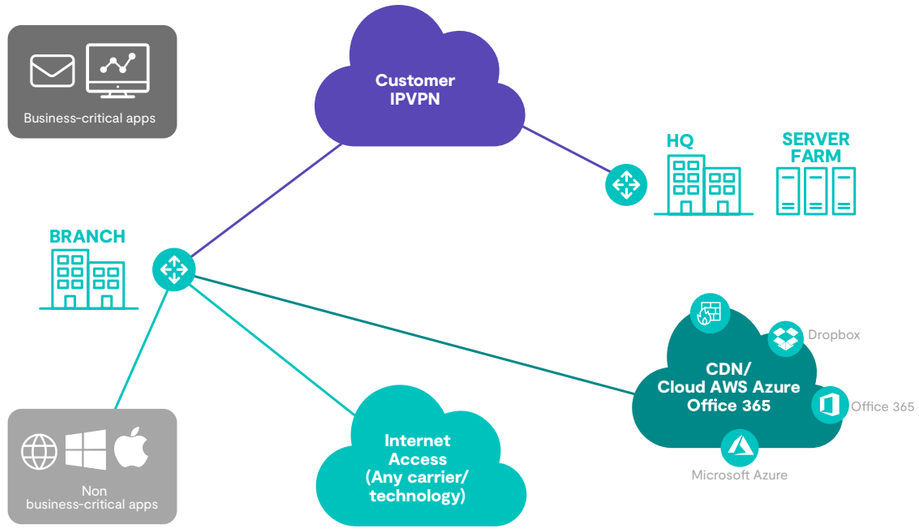
A brief definition of SD-WAN

For the last couple of decades, the standard model for wide area networking has been based on MPLS routers connecting enterprise branches and data centres via private circuits. The assumption was most network traffic was internal, following workloads that were processed in the organisation's own data centres.

This model offers a robust, reliable platform – assuming the network designers have made all the right decisions at the outset.

Once in place, the network largely defined what you could do with it. Change means reconfiguring individual devices. If lines become congested, your options are limited. Failover means ensuring you have more private links – an expensive proposition. And as business demands change and evolve, it can be difficult for the network to evolve with them. This is particularly true with the shift to cloud computing.

SD-WAN offers more detailed visibility into what is happening on the network, in real time, lending itself to more detailed analytics.



Hybrid WAN approaches have been used to supplement traditional WAN approaches. This has involved using two or more WAN circuits to connect branches and datacentres, giving some resilience if a circuit fails or becomes congested. These could be two traditional MPLS circuits, or a mix of internet, 4G or MPLS circuits. While more flexible, the approach is again limited by what has been designed in at the start. Upgrading configurations or changing policies becomes another exercise in micromanagement.

SD-WAN extends the hybrid WAN approach. The aim is to separate the network from the underlying circuits, creating a software defined "overlay" over the transport layer, or "underlay". In practice, organisations will usually define multiple overlay networks.

The underlay is transparent to the user, and may embrace a range of technologies, including traditional leased lines, as well as standard internet circuits and 4G.

A "central controller" manages and orchestrates the software defined overlay networks. Policies are set and changes are affected centrally, in software, not by managing individual devices, and are applied at network scale. This opens the possibility of much easier management for, and addition of, branch locations, and even individual remote workers.

Edge devices at each location handle routing and local firewalling. Traffic across the SD-WAN is encrypted, and security policy is also handled centrally.

SD-WAN offers detailed visibility into what is happening on the network, in real time, lending itself to more detailed analytics. These can be used to inform decision making and optimisation, to set automated policies to deal with changes in workloads and traffic, and to ensure quality of service and experience.

SD-WAN is typically offered as a service, though some organisations with relatively simple needs may choose to implement a DIY approach.

Market Trends

IDC in 2019 identified SD-WAN infrastructure as one of the fastest growing segments in the network infrastructure market, with 30.8 per cent Compound Annual Growth Rate (CAGR) expected between 2018 and 2023 to reach $5.23bn. This figure did not include managed services.

This growth is driven by the inability of traditional WANs to match the needs of increasingly digital businesses, particularly around access to Software-as-a-Service (SaaS) and hybrid and multi-cloud, said IDC. SD-WAN also satisfies the increasing desire of companies to use multiple connection types in order to improve application performance and the experience for the end user.

Challenges around enterprise WANs

33.8%
challenged security requirements

28.3%
found complexity with interconnecting multiple transport types

26.7%
raised US for on-prem enterprise apps and off-prem cloud apps

2023:
$5.23bn

In IDC's Software-Defined WAN Survey in November 2019, which covered 1,200 global enterprises, 95 per cent of respondents were using SaaS, while 94 per cent were using Infrastructure-as-a-Service (IaaS) in some form.

The survey found that 30.1% of respondents identified integrated security as the most "defining feature" of a next generation SD-WAN 2.0 platform. The second most mentioned feature, at 28.3%, was the ability to provide robust network and application performance management and assurance features, while 24.1% flagged up the ability to manage the deployment from a centralised or cloud-based platform.

When it came to the challenges around enterprise WANs, security requirements relating to web, IaaS and SaaS cloud services and other internet-based applications were raised by 33.8% of respondents. In second place was complexity associated with interconnecting multiple transport types, at 28.3% of respondents, while managing consistent user experience for on-prem enterprise apps, and off-prem cloud apps, was raised by 26.7%.

Separate research conducted by IDC on behalf of Cisco highlights the reasons companies have adopted SD-WAN. Companies reported that their traffic to the internet, and the cloud in particular, vastly outweighed their internal traffic and they were looking for ways to optimise this traffic and set and enforce policies for it.

Companies that adopted Cisco's SD-WAN solutions had, on average, increased their available bandwidth by more than 2.25 times, while WAN management was judged to be 33% more efficient.

Adopting SD-WAN meant onboarding new services was now 59% faster, the researchers found, while implementing policy and configuration changes was 58% faster. Overall, companies cut their unplanned down time by half.

In August 2020, IDC declared the managed SD-WAN market was at an inflection point, moving from early adopter to early majority phase.

The technology was "a top of mind consideration" for enterprises pursuing digital transformation, the research firm said, while the architecture is well suited to distributed enterprises, and supporting remote workers.

The conversation around SD-WAN is moving beyond purely technical considerations, according to IDC, with an increased focus on developments around orchestration, automation of operational processes, and gaining insight from data with artificial intelligence and machine learning.

Defining features of SD-WAN

30.1%
identified integrated security as the most "defining feature"

28.3%
said it provided robust network and application performance management and assurance

24.1%
said it managed the deployment from a cloud-based platform

33%
judged it to be more efficient than traditional WAN

Onboarding new services
59% faster

Policy and configeration changes
58% faster

Increased bandwidth by more than
2.25 times

The technology was a top of mind consideration for enterprises pursuing digital transformation.

Benefits of SD-WAN

The key promise of SD-WAN is increased flexibility and simplicity. This has implications right across your wide area network but has particular relevance to the following three key areas.

Security

Traffic on an SD-WAN is encrypted, adding increased security even when traffic is sent over the public internet. There is an overhead associated with this, and this should be planned for when designing the system. If you are using SD-WAN as a service, it should be the operator's responsibility to ensure the network has been appropriately scaled from the outset.

Depending on your provider, traffic can be sent to an external provider for unified threat analysis, for example through integration with Cisco's Umbrella service. This means traffic does not have to be backhauled for treatment, for example to an internal data centre, optimising the flow of data.

The edge device installed at each location will typically provide local firewall protection, something that would not necessarily be available as part of a standard broadband service.

Broader benefits come with the visibility and centralised policy control that SD-WAN offers.

Security policies, such as those around anti-virus, URL filtering, and access, can be set and applied centrally, using the most up to date threat intelligence, with the assurance they will be enforced throughout the network.

SD-WAN enables much easier network segmentation across the enterprise, allowing different areas of the network to be fenced off, with security controls applied appropriately, for example by line of business or by restricting access to key IP. Similarly, overlays can be designed with regulation or compliance needs in mind. Suspicious activity will be more visible, in real time.

Depending on your provider, SD-WAN offers significant security benefits for remote or home workers. By using an SD-WAN appliance designed for home workers, they will be able to log on to the corporate WAN using their normal network authentication process. Their business traffic will be encrypted and segregated from domestic traffic, and subject to all the controls and security policies enforced across the network.

The increased automation SD-WAN allows for, along with the potential for zero touch installations, and the general reduction in manual configuration and patching, dramatically reduces the potential for human error and the inadvertent introduction of vulnerabilities.

Network resiliency and optimisation

Traditional wide networks are highly prescriptive. The engineers designing a traditional network will have chosen what they believe are the best paths for particular traffic or workloads, based on the best information available at the time.

Older networks will have typically been designed with a focus on internal traffic. Once in place, they are difficult to adapt for new workloads or workflows. Traffic is routed the way the "network" says it should be routed. It may control for resilience, but not necessarily for the quality of the link.

SD-WAN offers far more flexibility, particularly if you are using a provider with access to a wide range of circuits. Centralised policy control means the network can prioritise traffic both by type and desired quality, and make the optimal use of all the available circuits.

If you are using a managed service, your provider should be taking measurements across all the networks available - including 4G, public internet and third-party networks - meaning path quality can be assessed in real time.

So, for example, a Service Level Agreement (SLA) can be set for voice traffic, or video traffic, to only use paths which meet certain criteria on latency and jitter. Traffic will then be routed only on those paths that meet the SLA requirements.

The nature of the underlay means that SD-WAN can offer seamless failover. If a primary circuit does fail, the network will automatically start using a secondary circuit. For example, in the case of the home or remote worker, if their domestic broadband connection fails, their appliance can seamlessly switch over to a 4G connection,
if this is part of the package provided.

Policies can be set to enable cloud traffic to break out directly from branches to the internet to chosen cloud providers, avoiding the latency hit of internal routing. Depending on the provider, customers may be able to take advantage of optimised connectivity directly into key cloud platforms or SaaS providers.

If your organisation's priorities and workloads change, policies can be updated to reflect this. The aim, again, is to deliver a network that fits the workloads and applications the business needs - for example, to support better use of Microsoft Teams or Zoom, or to migrate large amounts of data to the cloud to fuel analytics applications.

Ultimately, rather than simply quality of service, it is perhaps better to talk about SD-WAN delivering improved quality of experience.

Operational agility

SD-WAN decouples network management from the underlying infrastructure, resulting in simplification and increased agility, again ensuring the network evolves to meet the business' needs.

Because the network is monitored centrally and in real time, an SD-WAN package will typically include access to real time analytics which will give administrators much deeper insight into what is going on within the network. Problems and weakness should be identified much more quickly.

This in turn will inform evolving policy decisions, enabling continuous optimisation of the network for the organisation's key workloads and applications, rather than forcing it to work within the increasingly onerous constraints an inflexible legacy network can impose.

Configuration and policy changes can be made centrally based on solid metrics. There will be reduced need for engineering staff to visit individual sites to manually install and configure kit or perform updates.

Problems and weakness should be identified much more quickly.

Adding and managing branches, or even single remote workers, becomes much easier, to the point of becoming a zero touch operation. It becomes a question of shipping an appliance to the remote location, connecting it, and ensuring authentication.

This also means organisations no longer face the dilemma of having critical employees - whether senior execs or key engineering or support staff - having to use an inferior connection if they have to work from home, as in the current conditions.

On a broader scale, mergers and acquisitions no longer result in a one company two networks situation. Your SD-WAN provider can provide an overlay network for the acquired sites which is identical to the parent firm, producing one logical network.

How SD-WAN supports digital transformation

Digital transformation is the process of exploiting digital technologies and capabilities to create a robust new business model. In practice, it involves a shift from a hardware and infrastructure defined, manual, closed, and reactive world, into a world which is software driven, and where automation replaces manual processes as far as possible.

As a result, processes become programmable, and up to the minute data allows processes to be predictive rather than reactive. Ultimately, this means decisions can be based on business intent, not on rigid rules that may have made sense when they were set, but which cannot evolve. And inevitably, workloads, and their associated traffic, tend to move to the cloud.

It's not hard to see how this maps to SD-WAN. Your network options are no longer constrained by the underlying hardware, meaning your network can change and evolve as your workloads and business priorities evolve.

Network options are no longer constrained

Digital transformation is often associated with the migration of data and workloads to the cloud.

Change can be intelligence led, predictive and automated, whether that is spotting and remediating a potential security flaw or choosing the best path for data or workloads. When larger adaptations are required, change can be defined and implemented centrally and at network scale. The need for micromanagement of multiple devices at multiple sites is massively reduced.

As previously noted, internal network traffic has shrunk in proportion to the amount of network traffic that wants to go the cloud.

Depending on the providers used traffic can be securely directed from local branches direct to the major cloud platforms and SaaS providers. Quality of service can be prioritised for the traffic that is most important for you and your organisation, whether that is voice calls or video conferencing.

So, for example, companies embracing SD-WAN are better able to ensure key workers, or even their entire remote workforce, can access the full range of corporate network services, without compromising on connectivity or security.

Similarly, retail customers using SD-WAN have the visibility, and flexibility, to reconfigure their networks to account for the rapid rise in the volume of contactless and other card-based transactions as shoppers scale back their use of cash as a result of the Covid pandemic.

Ultimately, SD-WAN gives organisations the freedom to set the network policies they need to enable them to prioritise and optimise access to the applications they need with the experience they need, without having to worry about the underlying network infrastructure or topology.

Managed SD-WAN vs DIY SD-WAN

Companies are increasingly looking to managed service providers to supply SD-WAN technology. However, it is possible to take a DIY approach.

Lower-level DIY options will typically be based on cloud infrastructure, with companies paying a monthly subscription for the infrastructure management software. There may be limits to the number of overlays such a DIY solution can support. There may also be issues around the number and types of circuits a DIY solution can access, or that customers are able to manage.

Operational problems also become much more complex. If a fault does develop it is less likely to be a straightforward connectivity issue, but more likely to be a performance issue that is difficult to trace, for example if it involves an individual location having a problem with a particular application running in the cloud. So, a DIY approach might require a more proactive stance when it comes to dealing with problems, as well as in managing the underlay network and provider relationships.

More complex DIY efforts will eventually transition to a managed service, not least because this releases inhouse staff from the day-to-day toil of network management, freeing them up to focus on challenges such as business transformation.

A managed solution will typically involve detailed design at the outset, with the provider taking an extensive inventory of the customer's current workloads and building in projections for how an organisation's needs are likely to develop.

A managed service provider should be able to offer a range of different circuits and network paths, such as ADSL, 4G/LTE, Gigabit FTTP and Ethernet. They should also be able to offer bullet proof security options, including tight integration with a UTM provider.

As mentioned previously, a major reason for moving to SD-WAN is because the organisation's workloads are moving to the cloud. A managed SD-WAN provider should have detailed knowledge of the main cloud providers and SaaS providers to offer application optimisation - and be able to ensure any performance problems can be diagnosed and resolved quickly.

A final factor to consider is whether a company would prefer to keep its SD-WAN as a cap-ex-based spend, or switch to a managed service, which could come under op-ex spending, and which offers more flexibility for upgrading hardware and services.

However, the ultimate reason for moving to SD-WAN is not about security or networking,or even a balance of the two. It should be about what you need for your business, now and in the future.

About Zen Internet

Zen Internet is the largest independently owned and B Corp accredited telecommunications and technology service provider in the UK. Providing business broadband, Ethernet and data services for a wide range of large and corporate businesses, Zen's close partnerships with Cisco, AWS and Microsoft enable first class delivery of tailored cloud, networking and communications solutions.

A multi-time Which? recommended provider, Zen is renowned for delivering excellent customer service and technical support. This is reflected in the many awards it has achieved, including PC Pro's Best Internet Service Provider for 17 consecutive years, the UK IT Industry Award for Services Company of the Year and a UK Customer Experience Silver Award for Technology & Telecoms.

Zen has offices in Rochdale and Leeds and employs over 550 people. The organisation puts great emphasis on maintaining a people-centric business and was once again named a Sunday Times 100 Best Companies to Work For in February 2020.

Carbon Footprint Standard Carbon Neutral Organisation +

Certified B Corporation

CERTIFIED ISO/IEC 27001

The Zen SD-WAN Managed Service

To find out more about what Zen can do for your organisation

Visit: zen.co.uk/business
Email: solutionsales@zen.co.uk
Call our team: 01706 902579

CISCO Powered

zen