CIO ACADEMYASIA

The Journey to the SD-WAN Enabled Edge

A research primer published by CIO Academy Asia

2021

In partnership with

aruba
a Hewlett Packard Enterprise company

Introduction

Authors

P. Ramakrishna
CEO
CIO Academy Asia

Andrew Milroy
Principal Advisor
CIO Academy Asia

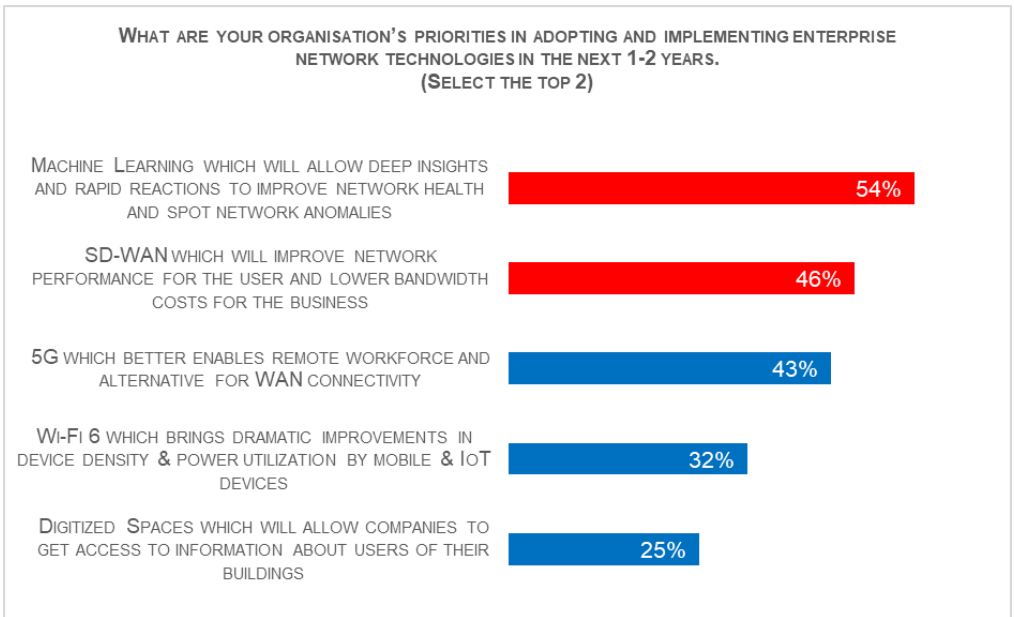
The massive shift to remote working combined with accelerated cloud adoption, have created demand for agile and secure network capabilities that can support the edge, including remote working, distributed clouds, and the Internet of Things.

Many of today's networks are rigid and static. Security is heavily fragmented across multiple domains of physical locations, cloud resources, edge devices, and mobile users. This inflexibility has been highlighted by the shift to remote working and dependence on traditional VPN-based access. Digital transformation initiatives enabled by rapid cloud migration are also exposing the lack of agility in traditional network architectures. Together, networking and security are slowing down businesses as silos erected decades ago are stretched and patched to accommodate emerging requirements. To address the needs of the new generation of digital businesses, a cloud-native networking and security architecture, along with a connectivity solution that can be deployed and scaled instantly, is necessary. SD-WAN is a fundamental enabler for such an architecture and the only way to protect users regardless of location and device is to provide cloud-delivered security.

SD-WAN enables the combination of edge computing and cloud computing. Using cloud resources for data intensive activities such as analytics, AI and ML, while enforcing policy at the edge makes IT and networks more manageable as well as more adaptable.

Indeed, the integration of SD-WAN with cloud and edge services can ensure reliability and efficient operations across the enterprise. It can also be a platform for innovation.

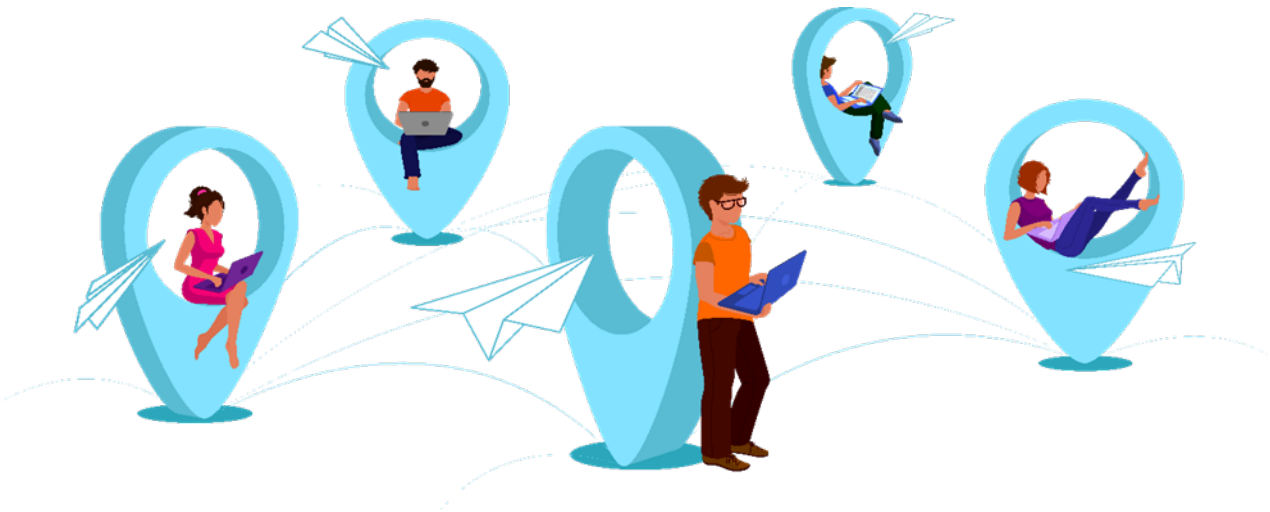
Figure 1 shows enterprise priorities in adopting and implementing network technologies in the next 1-2 years. ML and SD-WAN lead, followed by 5G which can be expected to further enable innovation at the edge.



Source; CIO Academy Asia Survey, May 2021

This paper uses insights from technology decision makers in South East Asia, to highlight the need for network modernisation, allowing companies to benefit from edge computing. It will focus on:

- Optimising connectivity for the dynamic remote workforce
- The rush to the cloud and the need for agile and scalable connectivity solutions
- SASE: The convergence of networking and security in the cloud
- Driving SD-WAN at the Edge with Advances in AI and automation



Optimising Connectivity for the Dynamic Remote Workforce

Remote user access has become critical for business operations, as unprecedented numbers of people work from home. The remote working model has moved from an occasional use model that typically involves the use of VPNs to a model that urgently needs the adaptability and flexibility of SD-WANs.

Traditional VPN based access, has required the backhauling of traffic to corporate data centres, adding unnecessary delays, and reduced application performance for users accessing cloud resources. With the migration of applications and workloads to the cloud, this outdated traffic pattern results in a sub-optimal user experience. Security issues have also been widespread as it has been difficult to enforce policies on remote workers and ensure that VPN software is updated and secure.

Although WANs are developing a software-centric approach to support distributed users and applications, security has not kept up. Traditional infrastructure-based security is not fit for purpose when applications are deployed across multiple clouds, with end users distributed across multiple locations. Defining a perimeter to secure becomes impossible and companies must completely re-think their cybersecurity postures. Effectively, identity becomes the new perimeter, whether it is the identity of human being or the identity of a device.

To mitigate business risk and protect digital assets, companies must address security holistically so that it can be automatically applied, based on the user, or device identity and context, while accessing enterprise resources.

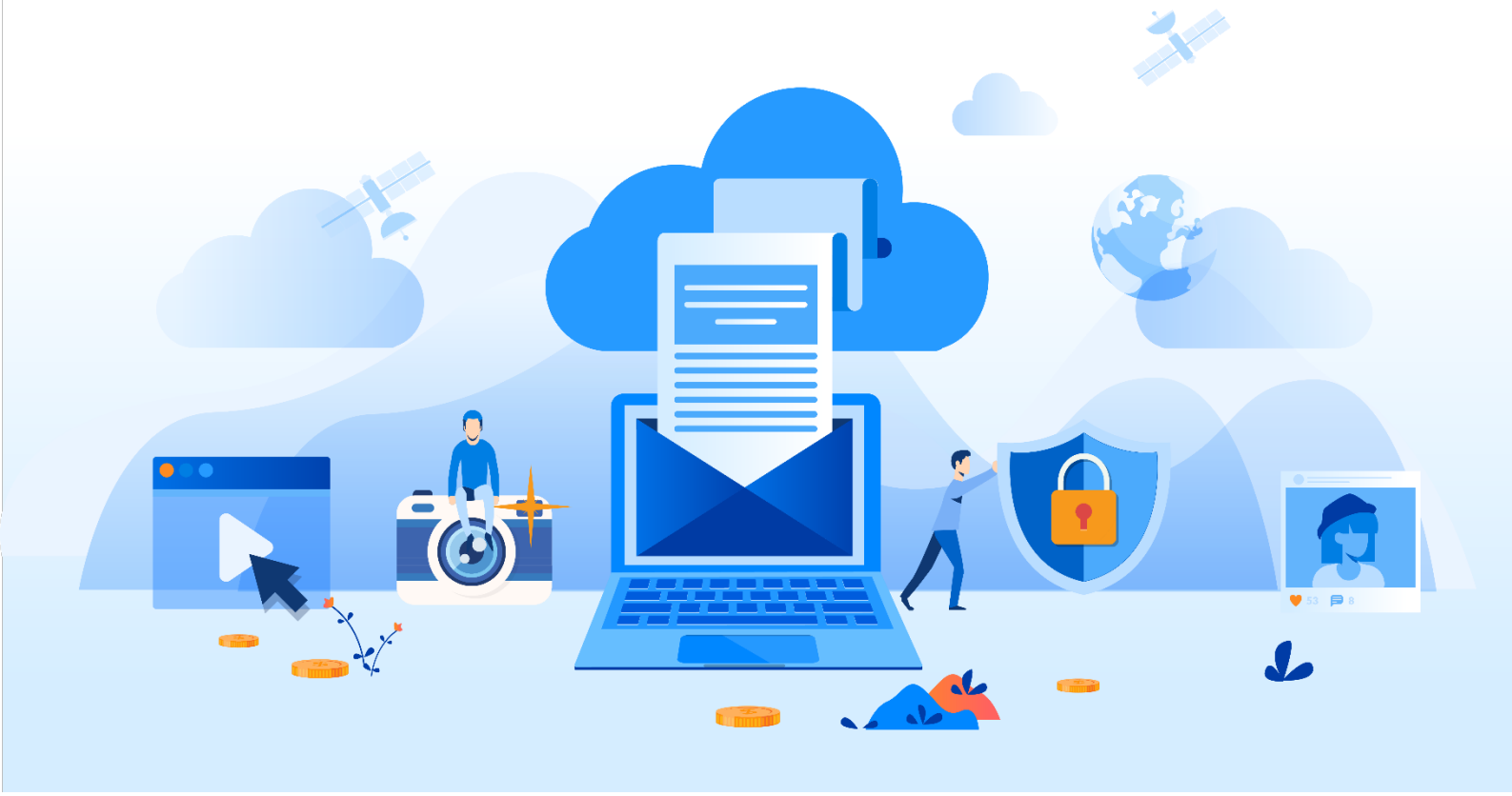
SD-WAN technology automates the network selection process to enable businesses to use public and private network links effectively. This allows remote workers to securely connect to cloud applications over the internet directly.

The Rush to the Cloud and the Need for Agile and Scalable Connectivity Solutions

The pandemic has accelerated the shift of workloads to cloud environments. Increasingly, companies are working with multiple cloud providers and often sharing data between clouds. As well as benefiting from the agility of cloud computing, companies have a much wider choice of services when they work with multiple cloud providers. Working with multiple providers can also help to reduce dependence and mitigate risk associated with working with a smaller number of partners. Companies do need to ensure that performance is not negatively impacted when moving data between clouds. They also need to ensure that integration between the SD-WAN and the cloud is seamless and that there is visibility across all cloud assets. SD-WAN architectures can address potential performance and resilience issues with multiple dedicated high-speed links, allowing employees to access their cloud resources.

To support their digital transformation initiatives, companies need networks that offer the adaptability and flexibility which is necessary to enable cloud-based digital transformation and widespread remote working.

SD-WAN technology builds on automation and virtualisation technologies to provide more agility and control, support cloud use and remote working and, drive the adoption of new technologies such as edge computing and machine learning. This allows decision makers to better understand their infrastructure and to scale up and down on demand.



Key benefits include of SD-WANs include:

- The provision of high performance access to cloud services for users located anywhere, enabling a more agile network.
- Better application performance. SD-WAN can be configured to prioritise traffic and real time services, transporting data across the most efficient route, thus enhancing performance.
- Increased business agility. Companies don't need to plan weeks or months ahead to deploy bandwidth. Instead, they can scale up and down on demand in line with requirements.
- Cost savings. SD-WAN allows traffic to be routed more efficiently across multiple channels. Traffic can be routed not only via existing MPLS circuits but also over the public Internet, LTE or wireless broadband.
- Simplified network administration. SD-WAN centralises network management making it easier to monitor user activity and optimise application performance. Deployment is typically automated making it much easier to scale on demand. This also increases IT efficiency — it frees IT resources for more strategic projects.
- Improved security. SD-WAN enables companies to consolidate infrastructure and manage resources from a single location. Centralising configuration of security policies removes human error associated with manual configuration of edge connections.
- Enabling remote work. Remote workers are often dependent on a single residential broadband link at their home. SD-WAN offers value to users by optimising the link through continuous monitoring and the ability to prioritise traffic. SD-WAN solutions typically provide private network reliability and security over residential broadband links while offering direct, optimised connectivity to the cloud. Additionally, users with approved mobile devices can add their wireless 4G/LTE links to their home network and use SD-WAN to aggregate available bandwidth and provide resiliency over multiple links.
- Consistent Standards and Governance. SD-WAN provides better transparency into governance processes and enables companies to enforce governance more effectively. IT no longer needs to manage to tension between service delivery, service management and innovation. Instead it can focus more on services which help the business to grow.

SD-WAN offers better application performance as it can be configured to prioritise business critical traffic and real times services like collaboration services — driving it over the most efficient route. Multiple options for moving traffic reduces packet loss from overloaded circuits, and latency due to heavy traffic.

SASE: The Convergence of Networking and Security in the Cloud

With increased remote working, users need to be able to connect to resources from anywhere forcing companies to provide network access and a secure, route to the internet without impacting performance.

Secure access service edge (SASE) is designed to enable the delivery of an integrated set of network and security services in a consistent way. This enables digital transformation, cloud migration, edge computing and remote working.

SASE can address the need for centralised, software-defined security architecture when applications, users and devices are highly distributed. It combines the flexibility of SD-WAN with a full suite of virtual security services, all delivered from the cloud. In essence, it integrates security and networking into one cloud solution, instead of having multiple discrete services.

Figure 2 illustrates the SASE model.

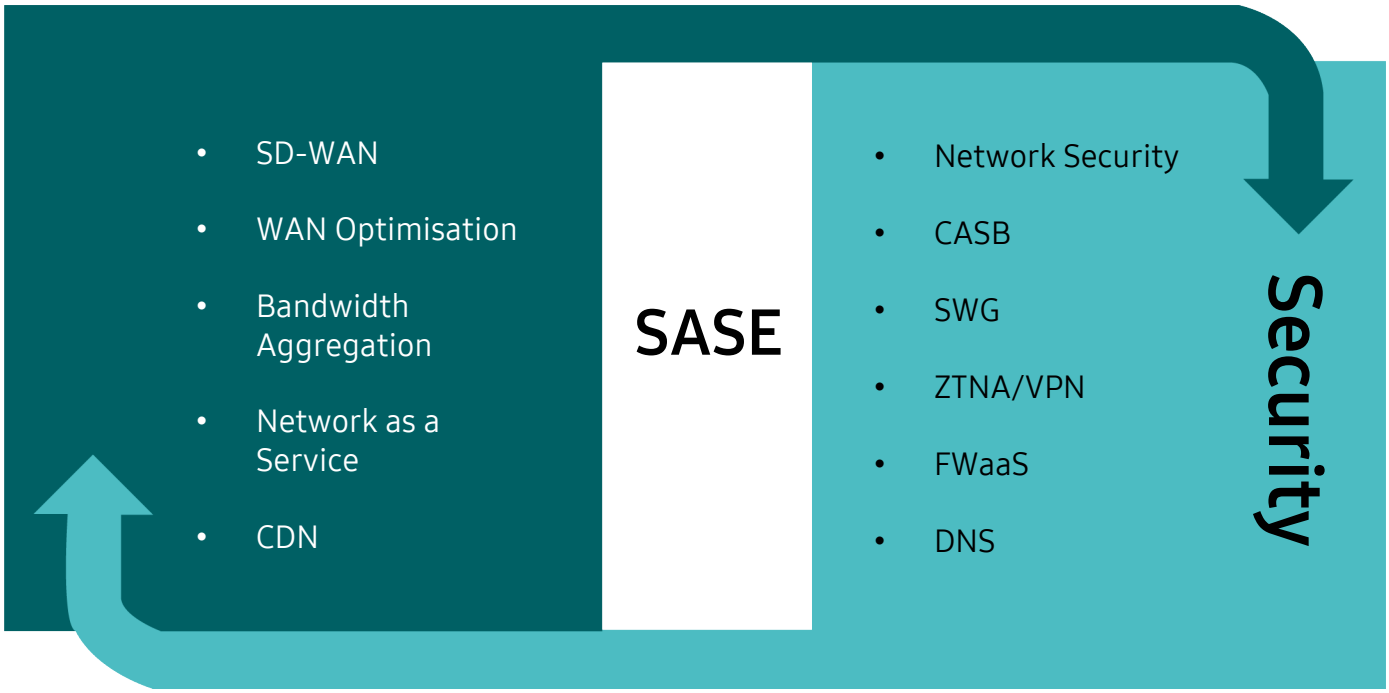


Figure 2 - SASE Model

SASE allows companies to eliminate a complex and fragmented set of physical and virtual solutions by providing one integrated cloud-native solution. This removes the cost of the appliances, and reduces network complexity. It offers much lower latency, greater visibility across assets and centralised control.

SASE is also essential for the development of a zero-trust approach to security. In addition to addressing many of the challenges associated with hybrid clouds and remote working, a zero-trust approach plays a significant role in mitigating third-party risks.

Current digital transformation and cloud migration projects are placing unnecessary risks on companies. SASE and a zero-trust approach to security are the best ways in which companies can mitigate the increasing risk they face.

While cloud adoption has been accelerating so has edge computing. Edge computing refers to pushing intelligence, data processing, analytics, and communication capabilities to where the data originates — at network gateways or directly at the endpoints. By bringing computing closer to the data source, edge computing enables low latency, greater business agility through better control and faster insights, lowers operating expenses, and more efficient network bandwidth support.

The edge can refer to a device including an Internet of Things device or a smartphone, or a location such as a home office, branch office or POP, that combines compute and network resources.

In most edge deployments, data processing usually happens locally. Edge locations are typically connected to the cloud, where data is aggregated from multiple sources and integrated with analytics and machine learning software to relay data back to edge devices. For example, data from wearable sensors for remote health monitoring is collected and processed locally at edge locations before aggregated data is sent to the cloud for storage and securely accessed by healthcare professionals.

Consequently, the edge expands the attack surface for threat actors as data is stored and processed across a much larger number of devices, systems, and networks. There is a need to ensure that connections between the edge, the cloud and data centres are secure. To achieve this SASE needs to be complemented by a zero-trust security framework which ensures that users and devices can only access resources that are consistent with their roles in the business.

The same software defined principles associated with SD-WANs, are increasingly applied across other technologies including data centers, clouds and devices.

In other words, software-defined silos are gradually converging into a wider software-defined enterprise architecture. With end-to-end automation, AI and policies driven consistently across home offices, remote sites, data centers and cloud workloads, companies will benefit from much greater adaptability, flexibility and scalability across all of their activities.

Advances in AI and Automation will Drive SD-WAN at the Edge

The benefits of edge computing are realised when combined with the cloud — multiple edges with multiple clouds. This combination brings the advantages of cloud and edge to where they make the most business sense.

SD-WAN enables the combination of edge computing and cloud computing. SD-WAN architecture relies on centralised application-based policy controllers for both intelligent path selection and routing, so cloud management is critical to orchestration at the network edge. Using cloud resources for data intensive activities such as analytics, AI and ML, while enforcing policy at the edge makes IT and networks more manageable as well as more adaptable.

Indeed, the integration of SD-WAN with cloud and edge services can ensure reliability and efficient operations across the enterprise.

An AI-powered SD-WAN can adapt to changes on demand. This technology is at the core of the convergence of networking, security, and AI to help businesses address growing data challenges as they migrate to the cloud.

The only way to achieve a self-healing network—one that can monitor, correct, defend, and analyse with minimal human intervention—is through automation and AI. When AI is embedded in an SD-WAN solution, the network gains extensive data processing capabilities and a richer understanding of network and application performance for quicker incident response. It continuously learns and automatically adapts to changing network conditions — aiming to deliver optimal end-user experience.

For example, if a network administrator wants to increase the bandwidth of an application, but the action is banned in a certain country. The SD-WAN network can intelligently make changes automatically when necessary. Such a WAN can predict problems before they occur through fault prediction and alert administrators. It can address the issue independently before end users are impacted.

Conclusion

The remote working operating model can be expected to involve the increasing use SD-WANs. This offers levels of adaptability, flexibility, performance, and security that are necessary to optimise the productivity of remote workers and to offer the best connectivity to cloud resources.

SD-WAN technology will increasingly act as a platform for innovation and drive the adoption of edge computing combined with greater use of AI and ML. This will also give much better control and visibility of infrastructure and make it easier to scale up and down resources, on demand.

From a security perspective, it is becoming impossible to define and defend the enterprise perimeter. Companies need a new approach which provides visibility and security across remote edge assets as well as multi-cloud deployments. SASE can address this need by incorporating SD-WAN. It can offer a centralised, software-defined security architecture across highly distributed users, devices, and applications. SASE integrates security and networking into one cloud solution with comprehensive security functionality all delivered from the cloud.

AI-powered SD-WAN technology is at the core of next-generation cloud applications that demand smarter and more reliable networks, which can manage themselves. This technology can provide enterprises with the freedom to deploy best-of-breed cloud delivered SASE security components of their choice.

It is important to strike a balance between delivering on-premises security functionality at the WAN edge and providing customers with the freedom of choice to integrate leading cloud-delivered security services.

When AI is embedded in an SD-WAN solution, the network gains extensive data processing capabilities and a richer understanding of network and application performance. Most importantly it can build more intelligence into the edge, facilitating innovation and accelerating digital transformation in a distributed connected world.

CIO ACADEMYASIA

This research primer is prepared by CIO Academy Asia in partnership with

aruba
a Hewlett Packard Enterprise company