WHITE PAPER

The Future is Mobile

and Why SD-WAN is Flawed for Secure and Manageable Mobile and IoT Endpoints

ASAVIE

Published by

Clavem Research

EXECUTIVE SUMMARY

SD-WAN entered the scene to bring new levels of virtualization and automation to the enterprise WAN and branch sites, but has not solved the challenges of securing mobile and IoT endpoints that exist outside the WAN in a seamless and convenient way. New technologies are gaining attention, with SASE, ZTNA, and CASB each promising solutions to needs for deploying and managing security in ways that will follow apps and users, including mobile endpoints.

Truly seamless, hassle-free mobility and IoT inclusion in the WAN is still missing. This paper explores the reasons why and introduces Asavie SD Edge as a way to provide an on-demand mobile network slice, that can run on clientless minimal footprint endpoint to make those IoT and mobile endpoints behave as if they are within the WAN, and preserve existing SD-WAN investments.

TABLE OF CONTENTS

List of Figures

1. INTRODUCTION

From retail to manufacturing, all industries can benefit from the rapid progress of IT, cloud, security, mobile and networking technologies. But adopting new technology is rarely pain-free. IT decision-makers need to focus on attainable business outcomes and ask:

- Is my network performance supporting and enhancing productivity?
- Can we save operational expenditure by virtualizing the functions of hardware, and by running compute and storage apps in containerized workloads on cloud-native platforms?
- Will more automation and virtualization of our hardware functions result in a more agile, intelligent and cost-effective solution?
- Are our business users getting a good experience?
- Is our workforce happy to use the technology provided?
- Are all aspects of our IT and network properly secured, including mobile and IoT endpoints?

A RADICAL CHANGE IN SECURITY REQUIREMENTS

In the beginning of enterprise WAN, networks had basic architectures, since there was little in the way of requirements for managing cloud and Internet traffic. Security was a case of locking down applications, computer servers and PCs within a closed perimeter, and placing these systems behind a firewall to prevent external breaches.

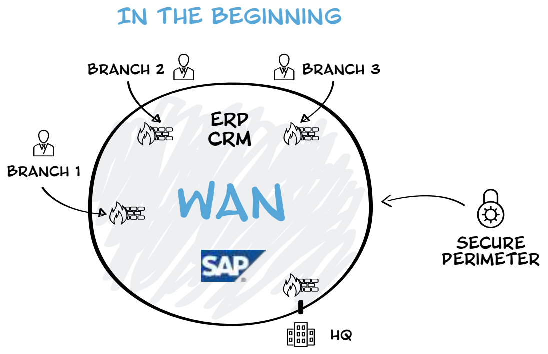


Fig 1 – WANs in the Beginning

WANs increasingly supporting cloud and Internet-based services, however, has meant more connectivity to the outside world. Users and systems demand access to external data centers, more Internet gateways, managed enterprise mobility, and connectivity to locations worldwide. The secure perimeter and site-based firewall scenario has disintegrated.

> 39% of organizations admitted to suffering a security compromise involving a mobile device—up from 33% in the 2019 report and 27% in our first report.
>
> *According to the Verizon Mobile Security Index 2020 Report*

Now we have Next-Generation Firewalls (NGFW) and an ultra-mobile, hyper-connected world. The result? A brand-new set of rules for network and security so secure policy moves with users and applications.

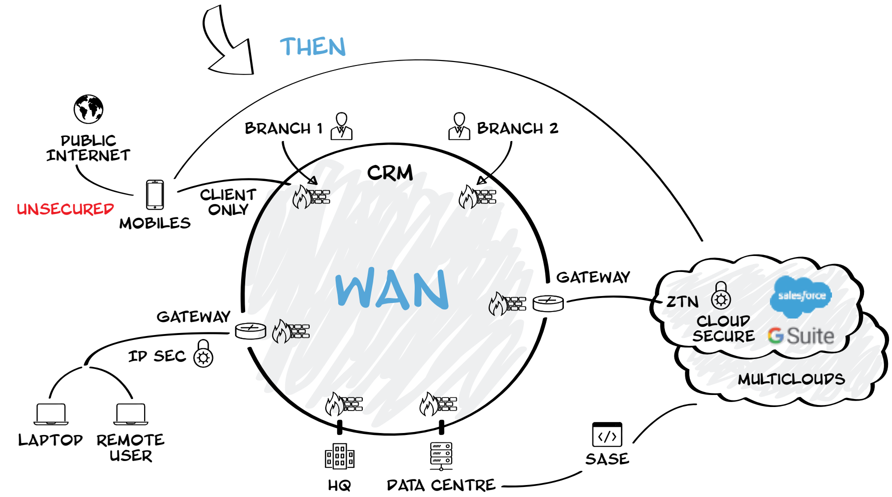


Fig 2 – The Evolution of WANs to Support Multi-Clouds, IoT & and Mobility

WAN TRIES TO KEEP UP WITH CLOUD AND MOBILE

Cloud migration has been rapid and at scale, but parallel developments in traditional WAN technology have been sluggish. It is also-inevitable that over time more and more enterprise workloads will run on mobile endpoints. Current corporate WAN developments only partially address increasing workloads on mobile endpoints.

LEGACY WANS: THE PROBLEMS

Legacy WANs, such as IP MPLS VPNs, were not originally designed with massive cloud adoption in mind, so they're struggling to keep up with new requirements, such as supporting the move of application servers off the customer premise and onto cloud environments. The proliferation of connected devices located outside the fixed perimeter, such as mobile devices and IoT sensors, also makes yesterday's WAN technology unfit for today's needs.

Emerging technologies are already disrupting the way many businesses operate. Manufacturers, for example, are embracing Industry 4.0, also known as the fourth industrial revolution, in which tech advances are facilitating the development of smart and automated systems.

In fact, enterprises in every sector are looking to emerging and disruptive technologies such as:

- Machine-learned data analytics
- 5G
- Artificial intelligence (AI)
- Multi-access Edge Compute (MEC)
- The edge cloud

Being able to deliver scalable on-demand bandwidth and the computational resources to interconnect these new technologies securely is defining the new network and IT era. Enterprises now need the agility to cope with increasing surges in demand from computing resources that no longer sit inside the traditional WAN.

SD-WAN IS PRETTY GOOD - BUT DOESN'T SOLVE ALL CHALLENGES

SD-WAN is now the main driver behind enterprise WAN transformation. It gives enterprises far more agility than before, and a cost-effective way to manage bandwidth growth and use. SD-WAN overlays mean changes can be made to the network quickly and with centralized control and policy consistency, all backed by automation. SD-WAN banishes the bad old days of manual command line script re-writing for even the most basic of network changes. However, for a number of reasons, SD-WAN does not effectively address the new challenges that arise with the ever increasing volumes of workloads running on mobile endpoints. For example, IoT devices may not run the same, or indeed a fully-fledged Operating System, to allow communications and management compatibility with the rest of the enterprise assets. Another challenge is the fact that mobile devices do not have static IP addresses. For solutions that require a book-ended configuration for zero trust, this is a problem as there is no way to map the asset in the zero trust network. Whilst there are workarounds for these challenges, they tend to add overhead, cost, negative impact on performance, and more complexity.

2. MAJOR TRENDS IN ENTERPRISE

EVERYTHING 'AS-A-SERVICE' AND CLOUDIFICATION

On-demand services are the X-factor for today's enterprise. Businesses don't want to make heavy upfront investments in infrastructure that could be obsolete in two years. The answer is 'everything-as-a-Service' or XaaS. This 'SaaS-ification' of software means placing services in multi-cloud environments, including private and public clouds.

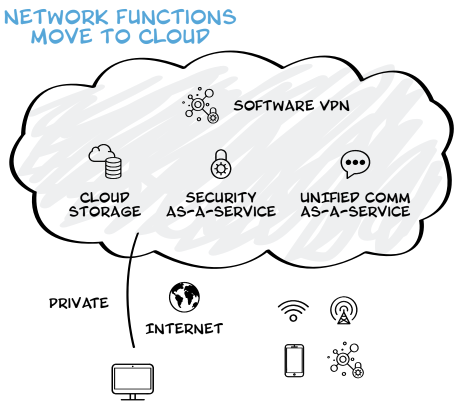


Fig 3 – The Digital Enterprise

THE FUTURE IS MOBILE AND IOT

Alongside 'cloudification', we're seeing growing consumption of corporate apps repurposed for mobile devices, but also seeing the use of non-sanctioned mobile apps for business reasons – which is known as 'shadow IT'. People are carrying out more and more business functions on mobile devices, meaning many IT platforms need to be re-designed to support a mobile-first approach.

This raises new vulnerabilities, however, as mobile devices, IoT devices and sensors often access corporate apps while outside the safety and protection of the WAN.

3. KEY DEVELOPMENTS IN ENTERPRISE NETWORKING

SD-WAN – BRINGING AUTOMATION AND VIRTUALIZATION TO THE CORPORATE BRANCH

SD-WAN has attracted considerable attention as an alternative and powerful network overlay solution to deliver software-defined connectivity.

Whilst SD-WAN solves many issues and helps businesses optimize connections so they can enable distributed workloads, it can also throw up barriers and limitations. SD-WAN implementations are not necessarily simple.

In fact, deploying an SD-WAN network overlay can add complexity. Inevitably, several security vendors are already in the mix with the legacy WAN and existing security tools may need to be reconfigured to work in the new SD-WAN environment. Not only does this create additional work, but security chaining increases latency. This can affect latency-sensitive enterprise apps such as Microsoft Teams.

Moreover, many enterprises don’t have IT teams with the skills to design, implement and maintain SD-WAN services. A typical IT department has legacy WAN management skillsets, but gone are the days of manually implementing command line scripts to make any changes to the network circuit by circuit.

ZERO TRUST RESETS THE BASELINE FOR USER CREDENTIALS

In the old world of secure perimeter VPNs, users had privileged access to everything once they successfully logged into the network. Zero trust implies nothing is trusted, including the user, the device, the application, the data and even the data sessions. The basis for trust is that user credentials are validated before a device is given access to the enterprise private network. Zero Trust Network Access (ZTNA) is a way to treat all users the same and give them access only to certain applications based on credential authentication and policy.

ARE CLOUD ACCESS SECURITY BROKERS (CASB) THE ANSWER?

In a world where enterprise applications are distributed across multi-clouds and SaaS offerings, security needs to be everywhere. Security practitioners advocate that security should be as close as possible to the user locations. As the name suggests, the cloud-based solution provides for protection as close as possible to the enterprise application in the cloud.

With the centralized proxy connection service, enterprises can secure data access and data in motion to the client-side device. An advantage of the CASB approach is that it tends to be clientless so no software is needed on the endpoint. Furthermore, it gives enterprises greater visibility than traditional data access and controls, which helps to mitigate data loss.

This is all great in theory as long as devices are inside the enterprise private network, as they are protected by the enterprise firewall. Devices on public Internet services such as mobiles and IoT sensors, however, remain vulnerable to malware and phishing. While CASB and ZTNA combined are undisputedly a strong defence as part of an in-depth security approach for any modern enterprise, significant security gaps remain when it comes to mobile endpoints.

SECURE ACCESS SERVICE EDGE (SASE): IS IT THE WINNER?

Bluntly, SASE (pronounced “sassy”) is a marketing concept developed by analysts. In short, SASE is the conceptual convergence of networking and security under an umbrella of software automation.

SASE aims to drive dynamic secure access to meet the needs of the enterprise. It encompasses automation and control of Networks-as-a-Service, SD-WAN and content delivery networks (CDNs), along with a complete portfolio of network security of next-generation Firewalls-as-a-Service, secure Web gateways, secure DNS, CASB, ZTNA and more. From an enterprise perspective, the value should be enhanced security and greater agility, and the hope of addressing the networking and security skills shortage many face.

The ideology for SASE is that most mobile and IoT devices and applications are now outside the enterprise fixed perimeter. If we ignore the security gaps of CASB and ZTNA, we are still left with certain questions that SASE does not fully address:

- How do enterprises take control of a mobile network?
- How can an enterprise control the mobile network in the same way they do SD-WAN, so they can deliver seamless access for mobile?

See Chapter 5 ‘Asavie SD Edge’ to learn how the Asavie approach gives answers to mobile network control and seamless access for mobile endpoints.

4. STATE OF MOBILE ENTERPRISE NETWORKING

MOBILE VPN CLIENTS

Mobile VPN clients are used to give secure access to corporate VPNs. This is not optimal from a technology and convenience perspective because it costs more to manage, it adds costs in terms of monthly payments and ultimately does not protect the endpoint from malware or phishing attacks. Furthermore, users can bypass the mobile VPN application by simply turning it off.

> The consequences of mobile compromises were shown to be severe and far-reaching. Of those that had suffered a compromise, 66% said the impact was major and 36% said it had lasting repercussions.
>
> *According to the Verizon Mobile Security Index 2020 Report*

Existing enterprise IT services focus on mobile VPN client-based solutions and mobile device management (MDM) to help mobilize workforces. At the same time, IT succeeds in basic security compliance by enabling a corporate container on the device to protect data from malicious actors. In the world of IoT solutions, there are no MDM solutions for endpoint management.

Mobile Network Operators (MNOs) complement IoT security by delivering eSIM management platforms. By doing so, however, they effectively offload the responsibility of managing the connectivity on/off button to the enterprise. Unfortunately, this means enterprises are still left with a significant hole when it comes to the security of IoT live in the wild.

IOT SENSORS ARE THE WEAK LINK

Dumb IoT endpoints are the easiest part of the network for cybercriminals to crack. That won't change until IoT endpoints have security hard-baked into their hardware components, a scenario that raises per-unit costs. While Android devices and iPhones have basic security features, hackers and cybercriminals are increasingly targeting them and other mobile devices, along with laptops, cloud servers, computers, and business mainframes.

PRIVATE LTE NETWORKS

MNOs offer private LTE networks to enterprises with a high enough number of mobiles. Logistically, MNOs shy away from offering private Access Point Names (APNs) as they're expensive to set up and maintain. Furthermore, the skillset needed to work with MNOs may not exist in-house, meaning the enterprise would need to spend more to bring systems integrators in-house.

Ultimately, private mobile networks from MNOs are not programmable and lack various features and functionalities that are present in zero-touch security and SDN/NFV.

THE ALTERNATIVE?

In a mobile-first world, enterprises can find they have little control over users and the applications they consume. How can mobile and IoT endpoints access the SD-WAN? The ideal solution for CIO and IT managers would make these endpoints behave as if they were within the more traditional fixed WAN environment, or SD-WAN, with the same security postures and without compromising their performance.

That solution should combine the powerful features and benefits of SD-WAN, SASE, CASB and ZTNA into a seamless network, one in which mobile and IoT endpoints can be clientless, and it should offer an easy way to add subscribers.

5. ASAVIE SD EDGE

Asavie enables the delivery of private mobile network slices to enterprises using software. Asavie partners with global MNOs to deliver an alternative approach to securing mobile endpoints and users from the modern threats associated with connecting a mobile device to the public Internet.

Asavie SD Edge is unique as it addresses both the human and machine use cases for mobile endpoints, giving an alternative means to securing mobile connections to the public internet, to the cloud or to internal enterprise systems and resources. Significantly, Asavie's approach stands out as it is clientless, requiring zero footprint on the mobile.

AN END-TO-END MOBILE BRANCH FOR SD-WAN

The solution not only addresses the security of mobile endpoints connecting to the internet, but also gives devices secure and seamless access to the enterprise private network. Through software automation, the private mobile network slice can be terminated as a branch of the SD-WAN. This integration makes it a world's first – a true end-to-end mobile branch for SD-WAN.

Network programmability, which complements the software-defined world of SD-WAN, is a compelling feature of Asavie SD Edge. The solution enhances SD-WAN capabilities by allowing enterprises to self-serve and manage not just the enterprise fixed WAN, but also a slice of the mobile network. Ultimately, this means enterprises gain visibility and control over their entire device estate of both fixed and mobile endpoints.

For enterprises, SD-WAN is about agility and being able to optimize networks in order to deliver productivity and cost savings. By including Asavie SD Edge as part of the SD-WAN, enterprises can squeeze more of a return of investment from their next-generation firewall by extending protection from fixed to mobile assets.

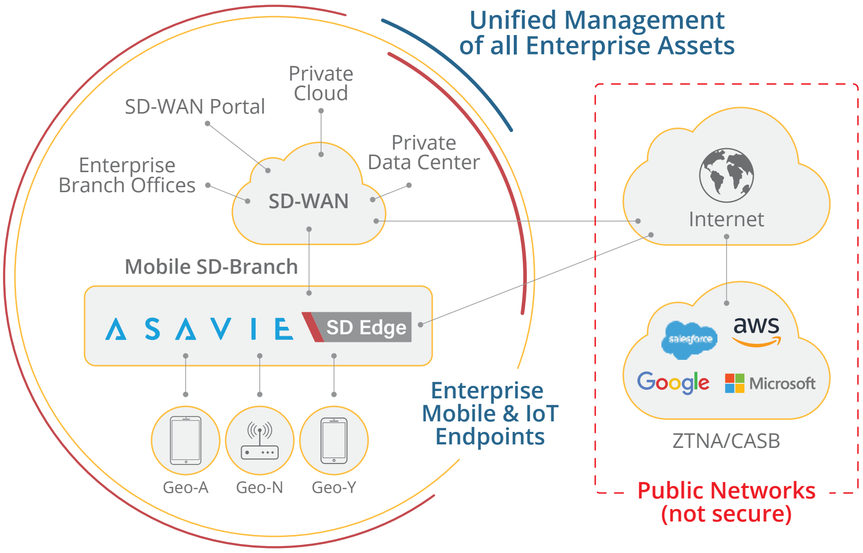


Fig 4 – Asavie SD Edge Brings Mobile and IoT end points into the SD-WAN

ASAVIE SD EDGE BENEFITS FOR SELF-SERVE AND SEAMLESS DEPLOYMENTS

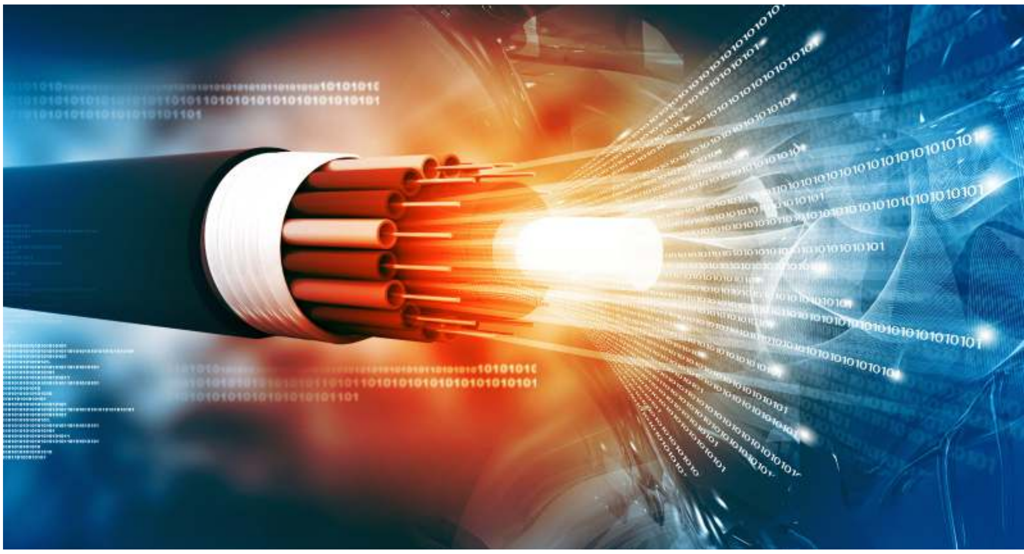
- Requires no CPE
- Is clientless
- Provides on-demand network slice
- Uses existing NGFW
- Gives the IT department a cloud-native SD-WAN-equivalent, with zero-touch automation, and control and visibility for adding mobile users
- Translates fixed policy to mobile policy
- Makes SIM-based identity bullet-proof
- Orchestrated as a tunnel to the existing WAN

6. CONCLUSIONS

While SD-WAN and SASE offer considerable advantages over traditional legacy WAN technologies, neither solution fully caters for a mobile-first WAN.

CASB and ZTNA can introduce powerful layers of security into an integrated cloud and VPN platform, but this approach is missing the real convenience of a self-service mobile SD branch and clientless implementation

Asavie SD Edge combines mobile-first WAN topology with cloud delivery and integrated network security tools. Customers that deploy Asavie SD Edge can begin making the radical move to converged fixed-mobile WAN.



GLOSSARY OF TERMS

3GPP	3rd Generation Partnership Project
AI	Artificial Intelligence
CASB	Cloud Access Security Broker
CISO	Chief Information Security Officer
DNS	Domain Name System
DSL	Digital Subscriber Line
IOT	Internet of Things
IP	Internet Protocol
IT	Information Technology
LTE	Long Term Evolution
MDM	Mobile Device Management
MEC	Multi Access Edge Compute
MPLS	Multiprotocol Label Switching
NFV	Network Functions Virtualization
NGFW	Next Generation Network Firewall
PC	Personal Computer
SAAS	Software as a Service
SASE	Secure Access Service Edge
SDN	Software Defined Network
SD-WAN	Software-Defined Wide Area Network
SSO	Single sign-on
TLS	Transport Layer Security
UDM	Unified Data Management
UEM	Unified End Point Management
VNF	Virtual Network Function
VPN	Virtual Private Network
WAN	Wide Area Network
ZTNA	Zero Trust Network Access