WHITE PAPER

Enterprise Network Security and the Future of Work

Mobile Security Is Key to Post-COVID-19 Playbook

Published by

Clavem Research

Executive Summary

COVID-19 will have a lasting impact on how employees work and how businesses operate. Security needs will evolve in an era when the office needs to go wherever employees happen to be. The challenge facing CIOs is how to take the same consistent and policy-compliant business tools available to staff in the fixed office WAN and securely extend them to remote working situations.

Remote work is not going away. Even as employees gradually return to workplaces and travel, the virus will continue to have a lasting impact. Some web-scale companies may choose to alter their way of working permanently.

Technology resilience and agility in enterprise network and IT is tremendously important, now more than ever. Keeping communications and collaborative tools up and running is vital in keeping businesses on track during times of crisis. But organizational agility cannot come at the price of security.

In this white paper, we explore the future of networking security concepts in more depth to show the future of the corporate network. We share insights into the main capabilities for SD-WAN, CASB, and ZTNA, in relation to the emerging and anticipated requirements of remote work after COVID-19.

We also assess the pros and cons of technologies available in the market and discuss a new way to integrate mobile and IoT endpoints into existing enterprise private networking solutions by creating a private on-demand mobile network slice.

Overall, IT and network decision-makers need to focus more on integrating mobile and IoT endpoints into enterprise private networks in an elegant way – for example, by adding these endpoints in a seamless way through a zero-footprint clientless option. Ideally, solutions like these also need to be managed within the same service wrap or WAN management dashboard as you use with your current SD-WAN, CASB, ZTNA, or SASE implementations.

Table of Contents

Introduction: Securely Managing the New Normal

Before March 2020 and the global spread of COVID-19, enterprises were continuing to invest in securely connecting branch, headquarters, and data center locations. The increased adoption of cloud-based services accelerated innovation in WAN connectivity, giving rise to strong growth for SD-WAN technologies. Any investment and effort must drive productivity gains, while businesses also need to manage costs effectively in the face of global disruption.

But CIOs are increasingly under pressure to empower a secure mobile workforce, and both traditional WAN and more modern SD-WAN developments tend to overlook smooth and secure integration of mobile devices and IoT sensors.

During the pandemic, enterprises everywhere were forced to adopt a remote working model, meaning their fixed network infrastructure investments were not being used anywhere close to full capacity. Instead, remote employees connected to their work applications through domestic ISP connections. In other words, they used unprotected consumer-grade internet access and conducted work activities, such as video conferencing, over potentially unsafe and congestion-prone links.

In addition, many businesses did not have adequate remote VPN access solutions, leading to some challenging business disruptions overnight as entire workforces moved to remote working without nearly enough remote VPN access to handle the traffic increases.

Businesses still need to recuperate investment on their deployed fixed infrastructure technologies, including spend on newer SD-WAN deployments, for example. They need to look for ways to innovate while protecting their existing investments.

In Akamai's previous white paper (see: The Future Is Mobile: And Why SD-WAN Is Flawed for Secure and Manageable Mobile and IoT Endpoints) we showed how a private mobile network slice can solve the challenges thrown up by mobile workloads and securing IoT devices outside the secure fixed WAN environment.

In this part 2 white paper, Clavem Research (on behalf of Akamai) explores how COVID-19 will affect the evolution of secure enterprise networking and offers an in-depth analysis of CASB, ZTNA, and SD-WAN. We also examine a new and innovative solution to secure mobile and SIM-based IoT endpoints based on SPS Secure Edge, a private mobile network slice developed by Akamai.

Covid-19 Drives a Peak in Remote Collaboration

Cloud- and web-hosted unified communications and collaborations have evolved consistently over the past 10 years or more. Current events have placed great pressure on these platforms, however. Internet and service provider IP backbones have mostly been up to the task of coping with the new barrage of voice and video conferencing traffic. But what about user security for unsecured endpoints?

CIOs must review secure access policies for open collaboration and video conferencing tools. With human error often exposing the network, user action to access secure conferences needs to be simple and kept to a minimum. Cloud-based collaboration tools should be automated, on-demand, and self-serve to make it easy to set up and run conferences.

A balance needs to be struck too. Enterprises have seen in the past that too much remote working can negatively affect innovation, so in this new world they need to make space for innovation to flourish. And humans are gregarious by nature – we will want to continue to meet and gather. Therefore, office locations will need to flex and contract on an as-needed basis. Businesses need to extend secure remote access to their employees as the future office can effectively be anywhere.

Enterprise CIOs must take these considerations into account when developing a corporate IT strategy that will not only cope, but also enhance productivity during times of crisis:

- Collaboration tools are crucial for ongoing communications and coordination, but they must be protected securely
- Cybercriminals have upped their game to take advantage of COVID-19, meaning enterprises must invest in and deploy best-in-class security; workers will want to gather and collaborate face-to-face once lockdown rules are relaxed – they may need more flexible and "portable" workspaces
- Mature enterprises will likely need a private network (WAN) and private data center for quite some time due to security and issues replacing private applications with public SaaS alternatives
- Seamless access from anywhere will be critical

Business Continuity

In the wake of COVID-19, technology resilience has become a must for every company. With employees now working from anywhere, CIOs need to consider the protection of the corporate assets wherever they may be; i.e., outside the protection of the corporate firewall.

Domestic Network Security Posture

COVID-19 has caused an unwelcome spike in cybercriminal activity, and home-worker networks are typically more exposed and vulnerable to penetration by malicious actors compared with office networks. Also, mobile devices are being targeted, with rises in malware and phishing being reported. So how can enterprise IT managers extend more collaborative tools to a remote and mobile workforce, while not compromising security?

Some of the answers lie in cloud and network security tools, including the encryption mechanisms that are inherent in SD-WAN, as well as CASB, ZTNA, and the overarching SASE for automated management of all these components. In the next section, we explore secure enterprise network trends in more detail.

The United Nations disarmament chief Izumi Nakamitsu told an informal meeting of the UN Security Council on May 22, 2020, that there had been a "600% increase in malicious emails during the COVID-19 virus pandemic, and an increase in volume and intensity of cyberattacks on healthcare and medical research institutions. A cyberattack takes place every 39 seconds."

Secure Enterprise Networking Trends

In a post-pandemic world, the way we conduct business will be altered forever. Staff will continue to need to conduct their jobs from anywhere, taking their secure access to corporate resources with them. Meetings will involve smaller groups, with few if any large in-person gatherings, industry events, and conferences. Enterprises need ZTNA for workers that is well-suited to the new working paradigm.

ZERO TRUST CONCEPTS

Traditionally, everything inside the enterprise network security perimeter was deemed as trustworthy. This included users, devices, and applications. To enable employees to access internal applications from outside the office, enterprises typically use legacy VPN technology. The basis for trust is that user credentials are validated before access to the enterprise private network is granted to a device.

The problem with granting access to anybody that is trying to gain entry to the network from access points within the office VPN is that true identification of the person trying to access the network is not verified. To close the security gap, enterprises are adopting the Zero Trust concept. Zero Trust implies the network trusts nothing, not the user, the device, any application, any data or even any data sessions.

The core concepts of Zero Trust, and how it is implemented for data storage, application traffic, devices, locations, and users, ensuring a holistic security approach, are listed here.

- Trusted Devices: Enterprises are using unified endpoint management solutions such as Microsoft Intune to manage, monitor, and control devices. Device attestation assures each device complies with the latest enterprise security policy before it connects to the enterprise private network.
- Trusted Users: With tools such as active directory, multi-factor authentication, and conditional access, enterprises no longer rely solely on password-based authentication.
- Trusted Applications: Enterprises with workloads across private data centers, multiple clouds, and SaaS are using SSO solutions if applications support it. For applications with no SSO integration, isolation remains the best option.
- Trusted Data Sessions: In its simplest form, enterprises are applying the principle of least privilege, meaning users or devices are given enough access to do the task at hand. Policies are implemented on the IP 5-tuple (the IP source and destination address, the port source and destination value, and the protocol in use). At a server level, the IP source address must be known and the IP range must be allowed.
- Trusted Data: Two key aspects of protecting data are doing so when the data is at rest and when data is in motion.
    - Data at Rest: Encryption, access management, and monitoring activity logs are needed, and are supplemented by mobile device management and data loss prevention tools to ensure data integrity at rest.
    - Data in Motion: Strong encryption of data on the wire between validated trusted application hosts and devices is crucial.

An Analysis of Client-Based Security in ZTNA

By zooming in on one of the core concepts of Zero Trust – trusted data sessions – we see a clear need to be able to bookend the IP tuple. This works well when the device is inside the enterprise private network, where the enterprise can assign the IP address.

But the enterprise has no way to control the IP address assignment to mobile devices, which essentially limits its capability to bookend the enterprise configuration. Some ZTNA solution providers are fudging this by offering a mobile application – essentially a legacy VPN client in which the enterprise gets a VPN headend or concentrator in the cloud.

Conceptually, the application works, but the mobile is still on a public internet, in which case the CIO has no control or visibility. Why is this important? The mobile is on a metered bearer, so every byte of data must be paid for (see the next section: Goodput vs. Throughput).

Additionally, VPN clients demand considerable power on mobile devices, meaning that batteries will run down far more quickly than clientless solutions. Another issue is that SIMs can be swapped from one device to another, thereby bypassing security measures. Furthermore, MNOs offer secure networks by design based on a globally recognized standard of 3GPP. When combined with a ZTNA application, this correlates to a VPN over a VPN.

Goodput vs. Throughput

The costs of an always-on mobile VPN client add up quickly on a metered bearer. Imagine an IoT endpoint needs to securely send 1 Byte of data, for example, "Y" or "N" each day.

All encrypted sessions have additional data overheads, which are application dependent. But taking a base example – that the encrypted session takes 6,500 Bytes to establish and the encrypted payload is roughly 40 Bytes – we can quickly see that to send 1 Byte of data daily, the data rates quickly add up over a month. The impact of a mobile VPN client on the metered bearer, over a 30-day billable period, is:

- Goodput = 30 Bytes
  (useful data collected by the enterprise)
- Throughput = ~196,200 Bytes
  (estimate of the actual billable data)

In short, supporting basic security costs much more than it should. Furthermore, an always-on mobile VPN client is only truly secure while the device is under UEM supervision, in which the mobile is locked down to supervisory mode. In nonsupervisory mode, security can be bypassed. Indeed, if malware takes hold, it will consume the metered bearer at will.

For dongles, Mi-Fis, cellular routers, and cellular IoT, ZTNA apps are OS-centric, meaning they are specific to Android, iOS, or Windows. Furthermore, no UEM can be used to seed trust of devices. In short, many devices used outside the enterprise private network remain untrusted under a ZTNA framework.

CASB – Protecting the Cloud-Based Application

With widespread remote working and enterprise applications being widely distributed across multi-clouds and SaaS offerings, security needs to be everywhere and anywhere. Security practitioners advocate that security should be as close as possible to user locations. As the name suggests, cloud-based solutions provide 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, requiring no software on the endpoint. Furthermore, it offers enterprises greater visibility over traditional data access and controls, helping to mitigate data loss prevention.

This is great in theory, if the devices are inside the enterprise private network, as the enterprise firewall on the corporate Wi-Fi protects them. Devices connected to public internet services such as mobile and IoT cellular connections remain vulnerable to malware and phishing. When combined, CASB and ZTNA undisputedly provide a strong defense as part of an in-depth security posture for a modern enterprise. But significant security gaps remain when it comes to mobile endpoints.

Is SASE the Winner?

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

SASE capabilities include:

- Supporting mobile users and cloud resources regardless of location
- Converging WAN edge and network security tools into a single integrated and centrally manageable system
- Delivering services over cloud-native environments
- Being a network designed for all edges, including mobile-first WAN strategies
- Supporting user and location identity

SASE should drive dynamic secure access to meet the needs of the enterprise. It encompasses automation and control of network as a service, SD-WAN, and content delivery networks along with a complete portfolio of network security, including:

- NGFWs as a service
- Secure web gateways
- Secure DNS
- CASB
- ZTNA

From an enterprise perspective, its value is enhanced security and greater agility, and it will help to address the networking and security skills shortage faced by enterprises.

The issue remains that no one vendor can offer SASE. There is no standard definition for SASE – it can mean different things to different vendors and managed security service providers. The same can be said of the NGFW. There are no established protocols to which vendors need to adhere or get certified, meaning independent labs cannot validate SASE and NGFW vendor claims.

If we ignore the marketing hype, SASE helps us see (and this whitepaper aims to show) that enterprises are currently forced into using siloed security solutions. As we have seen, CASB and ZTNA have their place when it comes to addressing security in a fixed network.

The ideology driving SASE is that most devices and applications are now outside the enterprise fixed security perimeter. For many enterprises, these will be mobiles and IoT devices. If we ignore the security gaps of CASB and ZTNA, we are still left with interesting questions to answer in relation to SASE: How do enterprises take control of a mobile network? How can an enterprise control the mobile network, as they do SD-WAN, in order to deliver seamless access for mobile? Isn't this what SASE is touted to deliver – secure seamless access for all?

SD-WAN, ZTNA, CASB Network Security Scorecards

Security and privacy center on protection of infrastructure and data. The following table shows how the different solutions address these business issues.

Is the business problem solved?	SD-WAN	ZTNA	CASB
Security for apps running in the cloud	√	√	√
Network segmentation	√	x	x
Customer IP subnet configuration	√	x	x
Protection against sniffing/ snooping	√	x	x
Protection against routing exposure	√	x	x
Prioritizing apps in the cloud	√	x	x
Identifying and inspecting mobile/ IoT traffic endpoints	x	√	x
Identification of mobile/IoT endpoint location	x	√	x
Cloud-native and cloud-enabled architecture	x	x	√
Mobile and IoT endpoint security	x	x	x

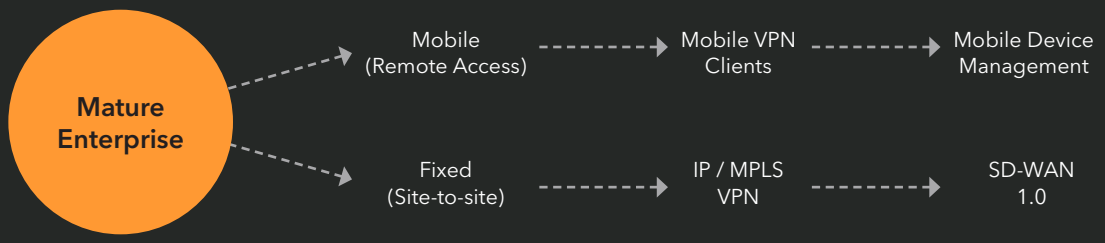
Table – An Assessment of Business Problems Solved by SD-WAN, CASB, and ZTNA

The Customer Journey – Brownfield vs. Greenfield

All existing enterprises already have various formats of VPN connectivity, WAN, and security in place, along with a cloud program. Large established businesses, such as those operating for more than 20 years, with several thousand employees and hundreds of sites around the world, are likely to adopt SD-WAN as a migration path from IP/MPLS VPN.

In such cases, they have invested in fixed-line infrastructure securing site-to-site access. The IT-plus-network adoption trajectory is likely to be from MPLS to SD-WAN. After that, a company may look to transforming its security and cloud platforms toward ZTNA, CASB, and SASE. Securing remote and mobile user access is an afterthought. The lower section of the figure below shows path divergence from the fixed infrastructure program.

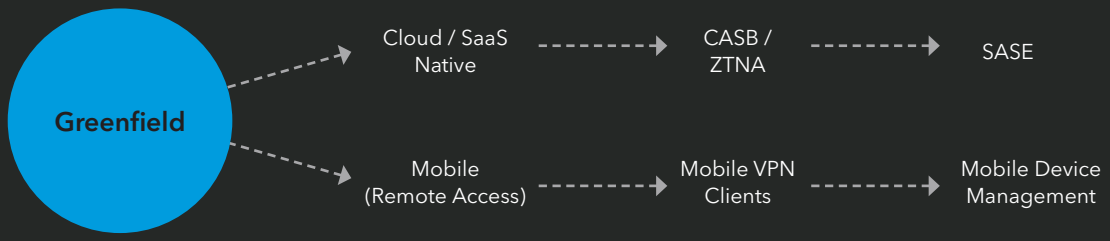
Mature Enterprise Path from MPLS to SD-WAN



Smaller, less mature companies founded in the past five years or so are more likely to directly adopt ZTNA and SASE – simply because these businesses have adopted cloud and SaaS platforms from the outset with fewer legacy issues.

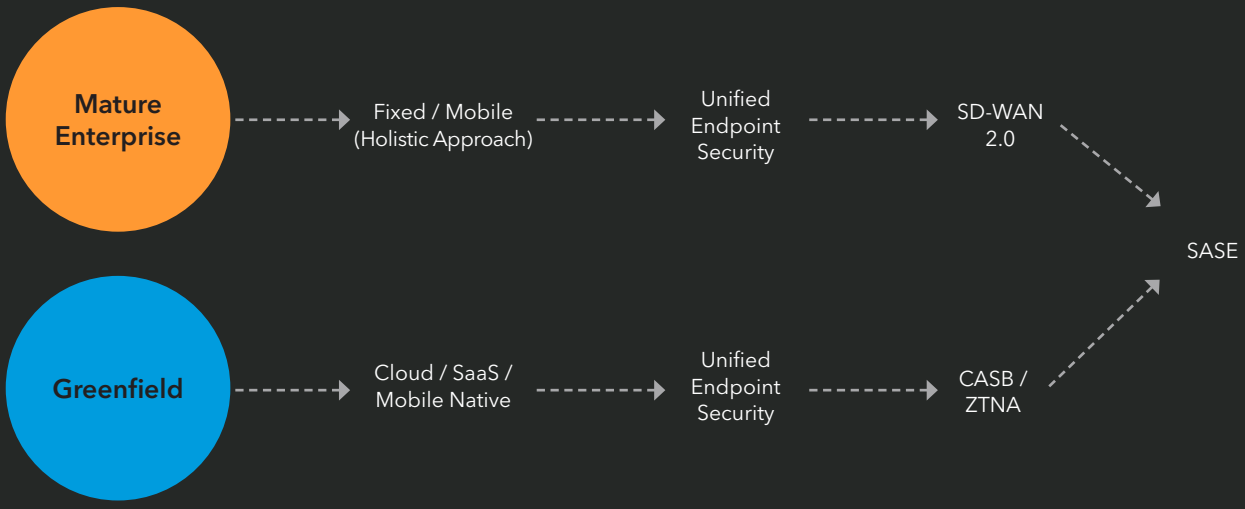
These companies are attracted to a clientless solution for mobile endpoints because they dislike the client-based approach for a mobile workforce, knowing it demands additional tooling, expense and management effort.

Less Mature Business Adoption of CASB, ZTNA, and SASE



The above scenarios reveal different network topologies and different approaches or attitudes toward adopting network security for fixed and mobile assets. Unified endpoint security solutions in both cases are sourced separately, however, giving rise to a siloed approach. The industry needs to consider including mobility and IoT in a single holistic digital transformation program, with nondivergent central network orchestration — see the figure below.

Migration of Enterprise to SD-WAN and SASE



Exploring the Alternative – A Private On-Demand and Clientless Mobile Network Slice

Earlier, we focused on the new working realities businesses must face. The office needs to go where employees are working, whether that is a pop-up office, their homes, or other office sites such as factories. At the same time, security postures need to be consistent across each of these scenarios.

When we evaluate all the available options (see the figure below), we can conclude that combining SD-WAN, CASB, ZTNA, and SASE will result in powerful security that ticks boxes for any CIO looking to give their company technology resilience for the future of work.

Providing security for mobile and SIM-based IoT endpoints based on the existing network-security investment is missing, however. As we have outlined, there are several workarounds, including VPN clients and passing mobile traffic through a secure URL, but they all have their disadvantages.

What CIOs need is a more sophisticated zero-footprint option that makes the endpoints behave as if they are seamlessly integrated within the enterprise private network (be it SD-WAN, ZTNA, CASB, or SASE) service, without relying on a client being deployed on the mobile handset or SIM-based IoT sensor. (The latter is probably not possible in any case, as the IoT sensor is not likely to have an operating system, and even if it did, it might not support the installation of a client).

Pros and cons of SD-WAN, CASB, ZTNA, and SASE

SD-WAN

SDN/NFV for centralized orchestration. Re-architect branch architecture with automation and virtualization.

CASB

Security goes with the app and user.

ZTNA

Good for cloud and fixed endpoints. However mobile and moving IoT devices/endpoints change their IP addresses (nonstatic). The metered bearer can cause bill shock.

SASE

Integrates all the components, converging network and security under software automation.

The Elegance and Power of Going Clientless

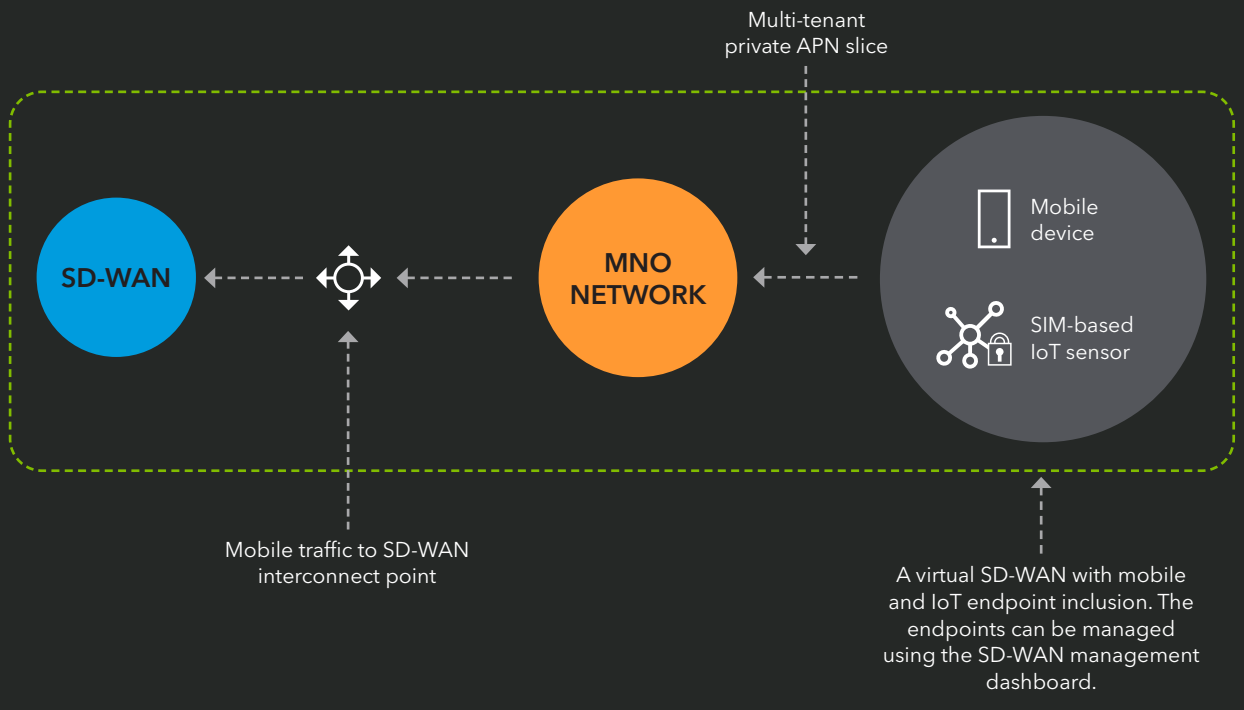
Akamai has developed a solution – Akamai SPS Secure Edge – that offers an on-demand mobile private network slice per enterprise that is clientless for remote users and IoT devices. Akamai SPS Secure Edge makes IoT and mobile endpoints behave as if they are within the enterprise private network, meaning CIOs can make the most of existing investments in next-generation cloud-based firewalls.

In this scenario, mobile devices and SIM-based IoT devices send traffic over the subscriber's mobile network (networks managed and operated by AT&T, Orange, Singtel, Telefonica, Verizon, Vodafone, and so on). The traffic then passes through a "mobile interconnection point" or hub so it can then be passed onto the SD-WAN, as we can see in the figure below.

Using this solution, IT administrators can apply the same security policy to all connected devices. They can see and control them using the central enterprise private network (for example, SD-WAN) management console or dashboard.

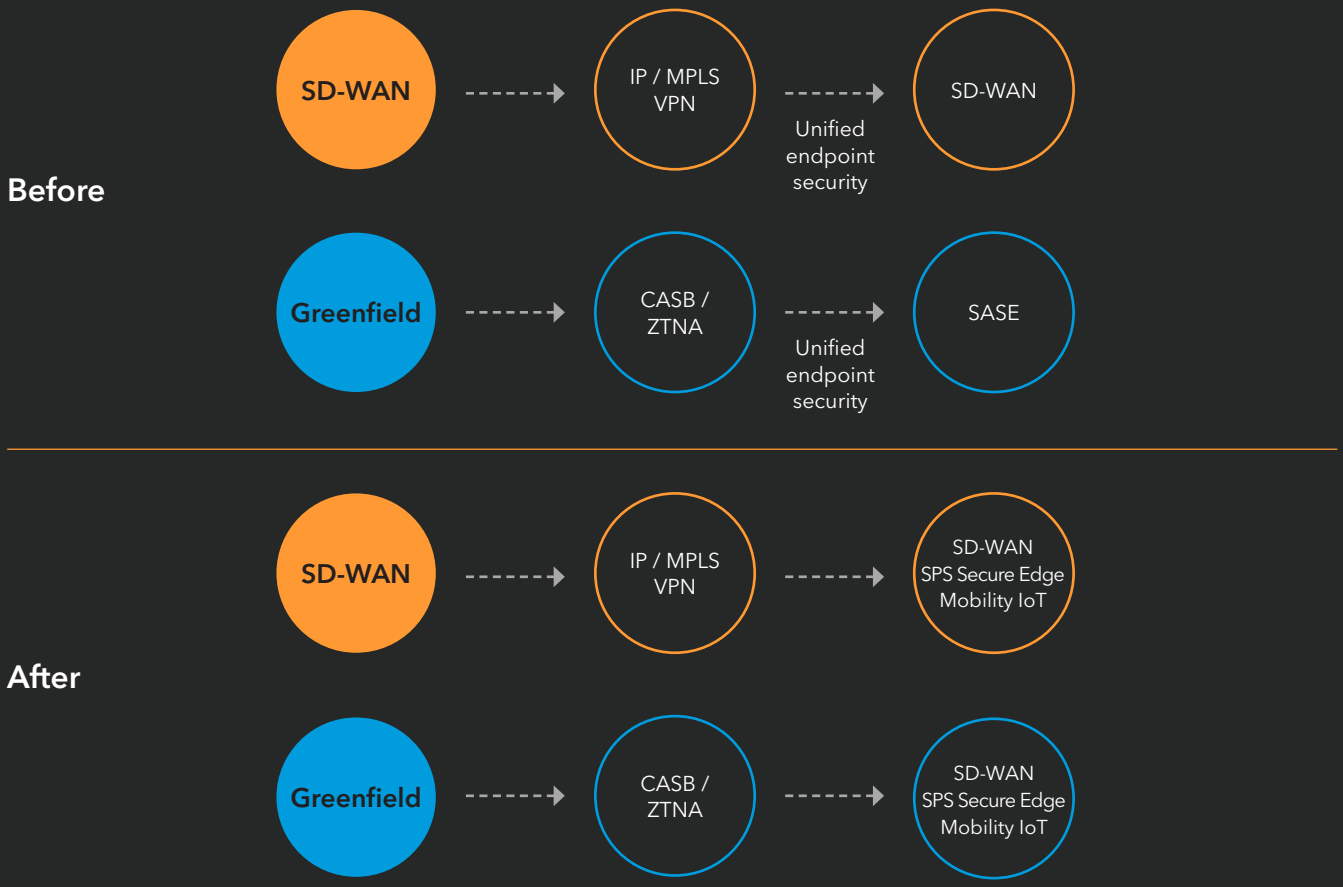
In the below architecture, the endpoints may be quite distributed from the perspective of performance, with the SD-WAN security policy and control applied to traffic at the nearest local traffic breakout point.

Mobile Network Traffic to SD-WAN Interconnect Point



In a previous section, we discussed typical pathways for newer and more mature companies, highlighting the need to break down the traditionally separated mindset for buying managed enterprise mobility. A more efficient, holistic approach to digital transformation is to see the mobility aspect as part and parcel of, and fully integrated with, the SD-WAN (see the figure below).

A Holistic Approach to Enterprise Network Transformation



Multi-Tenancy APN for Mobile Network Operator Cost Efficiencies

The private Access Point Name (APN) provides the point of entry into an IP network that can be secured and configured for individual SIMs on a cellular network. Creating a multi-tenancy private APN allows MNOs to realize cost efficiencies by creating a private on-demand network slice for each enterprise.

Akamai helps MNO partners to increase consumption of connectivity services through automation, self-service, and cloud adoption:

- **Faster time to market**
    - Akamai reduces effort and eliminates the manual processes of private APN builds for MNOs
- **New revenue streams**
    - Market differentiation that allows MNOs to address new market segments
- **Operational efficiencies**
    - Reduced cost of sale with an automated onboarding process with a self-service portal/API for the enterprise

With Akamai, mobile network assets can support several enterprise clients to help MNOs achieve quicker ROI on their infrastructure. This also pushes down costs for enterprises as infrastructure can be shared. This might appeal to companies that want more than one private network slice, and/or to create hierarchies for priority application traffic. Akamai has created an automated private mobile network slice factory that can multi-tenant a private APN within minutes.

Conclusions

- Technology resilience is incredibly relevant in the post–COVID-19 world. Enterprises need to develop solid business continuity so productivity continues during any crisis.
- Enterprises need to pay more attention to building and supporting mobile-first operations and business models, as workers want to be flexible – the office must be anywhere post–COVID-19.
- The future of network security demands Zero Trust concepts. The secure network and uniform policies need to go with the worker, device, and app to support flexible working models. Staff may move freely between offices, their homes, and pop-up locations, and take their secure IT solutions with them.
- When combined, SD-WAN, CASB, ZTNA, and SASE are secure. But these solutions do not give a flexible or easy way to incorporate mobile devices and SIM-based IoT sensors into the SD-WAN. To do this, customers can use Akamai SPS Secure Edge, which gives a clientless private on-demand mobile network slice to bring endpoints outside of the WAN into the same SD-WAN management console/dashboard. To be cost-effective, MNOs can use multi-tenant APNs.
- Akamai SPS Secure Edge is not a replacement for CASB, ZTNA, and SASE. It complements these technologies to further strengthen security in a more elegant way for mobile endpoints. The Akamai SPS Secure Edge becomes a "virtual mobile branch" within the existing SD-WAN. It is a Zero Trust network access mechanism for mobile and SIM-based IoT endpoints that integrates with existing SD-WAN solutions to deliver a better ROI for the enterprise.
- Akamai SPS Secure Edge gives each enterprise a mobile network slice in which it can deliver secure internet experiences, alongside seamless remote access for all mobile assets, under a single umbrella of management. This self-serve mobile network with unified endpoint security of fixed and mobile assets is a step closer to the true vision of SASE.

Glossary of Terms

3GPP	3rd Generation Partnership Project
AI	Artificial Intelligence
CASB	Cloud Access Security Broker
CDN	Content Delivery Network
CIO	Chief Information Officer
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
MNO	Mobile Network Operator
MPLS	Multiprotocol Label Switching
NFV	Network Functions Virtualization
NGFW	Next-Generation Firewall
PC	Personal Computer
ROI	Return on Investment
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 Endpoint Management
VNF	Virtual Network Function
VPN	Virtual Private Network
WAN	Wide Area Network
ZTNA	Zero Trust Network Access

Akamai secures and delivers digital experiences for the world's largest companies. Akamai's intelligent edge platform surrounds everything, from the enterprise to the cloud, so customers and their businesses can be fast, smart, and secure. Top brands globally rely on Akamai to help them realize competitive advantage through agile solutions that extend the power of their multi-cloud architectures. Akamai keeps decisions, apps, and experiences closer to users than anyone – and attacks and threats far away. Akamai's portfolio of edge security, web and mobile performance, enterprise access, and video delivery solutions is supported by unmatched customer service, analytics, and 24/7/365 monitoring. To learn why the world's top brands trust Akamai, visit www.akamai.com, blogs.akamai.com, or @Akamai on Twitter. You can find our global contact information at www.akamai.com/locations. Published 04/21.