SASE-READY WAN EDGE FOR THE WORK FROM ANYWHERE ERA

WHITE PAPER

Document Date: March 2021
Author: Mauricio Sanchez, Research Director
& Shin Umeda, Vice President

Abstract

Enterprise networks are on the verge of a major tipping point, driven by the shift from employees working at a corporate office to working from anywhere. Enterprises are quickly realizing that legacy network and security architectures are inadequate. They must evolve toward a unified networking and security service that increases scalability, agility, and security in a user and application environment that is now highly distributed, and mobile across the Internet. The need to provision and deliver new networking and security services in a matter of hours, not weeks or months, holds as much priority as the ability to reduce total cost of ownership (TCO). There is no question that the combination of cloud-based networking and security services that are global, context-driven, and flexible is fueling a wave of next-generation secure and optimized networking upgrades.

DELL'ORO GROUP

INTRODUCTION

In our paper, we discuss the key drivers behind the work from anywhere trend and why traditional wide area network (WAN) and virtual private network (VPN) approaches no longer work. Based on engaging a leading communications service provider, we describe the requirements that enterprises need to consider as they shift towards cloud-based networking and security. We propose that two technologies, SD-WAN and cloud-based secure web gateway (SWG), are merging to satisfy the new requirements and are the basis of a new solution called secure access service edge (SASE).

Contents

THE NEW "WORK FROM ANYWHERE" ERA

IT architects have a need to re-architect their network and security strategies in light of two key trends that accelerated with the arrival of the COVID-19 pandemic and that are at the core of the new work-from-anywhere era:

- Transition to an Internet-based application infrastructure
- Growth of a highly distributed remote workforce

We discuss each trend in greater detail below.

Transition to an Internet-based Application Infrastructure

A clear trend for more than a decade has been enterprises' migration to public cloud-based applications and computing models for their businesses. The growth in the number of cloud-based applications and services available is leading enterprises to choose multiple cloud services that generally fall into one of three categories: infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS). With the vast array of available cloud services, enterprises will find themselves in a multi-cloud environment in which they use any or all of these types of services with separate cloud providers.

While this migration is expected to continue for the foreseeable future, enterprises may not be able to move all applications to public cloud services, and will have to operate in a hybrid cloud mode. Enterprises face an increasing challenge in managing access to these applications by the expanding remote workforce, irrespective of where the applications are hosted, on-prem or in-cloud.

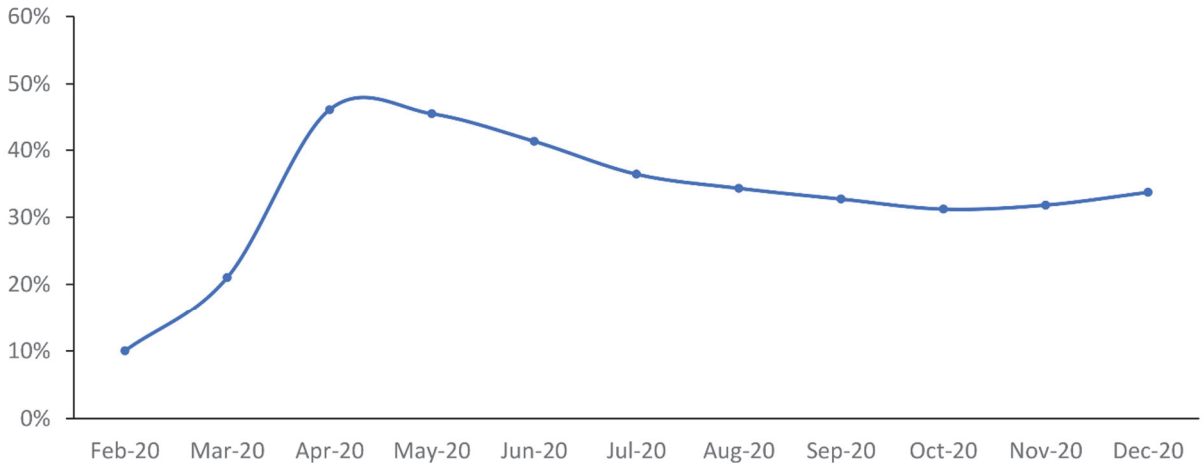
The COVID-19 pandemic has caused a significant redistribution of the enterprise workforce. This dramatic rise in the number of people working from home has caused a rethinking of the role of IT infrastructures, which has led to the accelerated adoption of many technologies that enable enterprises to digitalize their operations and processes.

The combination of the migration to cloud-based services and the redistribution of the workforce has led to a new era in how enterprises view, build, and manage infrastructures that leverage the Internet.

A Highly Distributed Remote Workforce

According to our analysis of US government and public research data, only 10% of the total US workforce was working remotely prior to the pandemic, either full-time or occasionally (Figure 1). As states and localities enacted shelter-in-place health orders to slow the spread of COVID-19, the percentage of the US workforce that was working remotely shot up to 45% in spring 2020, a 4.5x increase over the pre-pandemic baseline. In market verticals with a high percentage of knowledge workers, such as education services, finance, and scientific and technical services, telework percentages were much higher.

Figure 1: Percentage of U.S. Workforce Working Remotely in 2020
(full-time or occasionally)

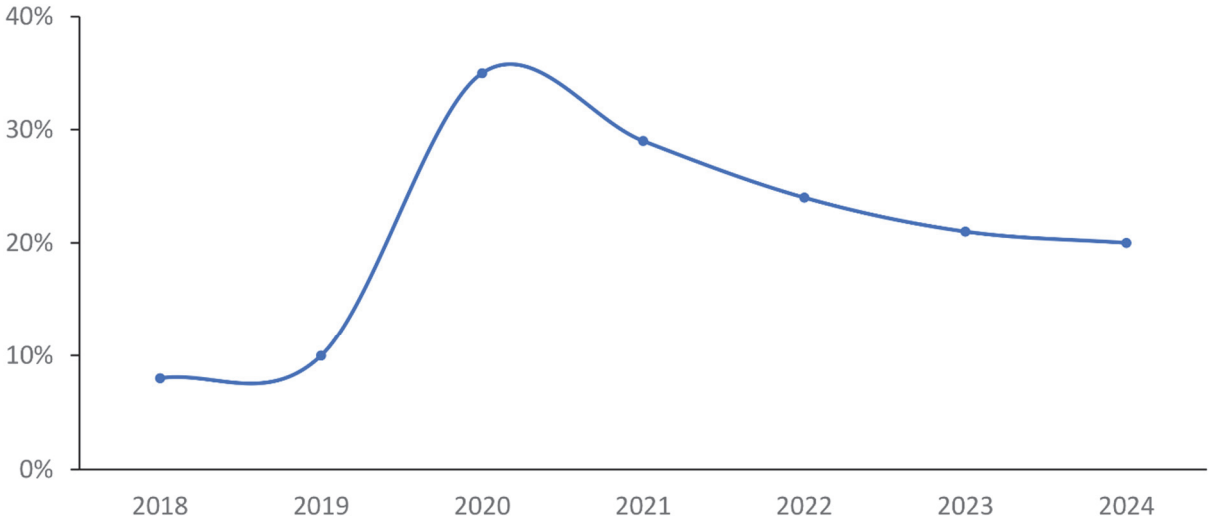


Source: Dell'Oro Group

While the same US government data show overall telework rates starting to drop as health orders are rescinded and some workers begin to return into corporate settings, based on Dell'Oro analysis we expect an elevated rate of teleworking post-pandemic compared to pre-pandemic. Business leaders forced into adopting a remote workforce have become more comfortable with the concept. Likewise, workers thrust into working remotely have an increasing desire to work partially, if not fully, remotely.

Based on greater acceptance of a remote workforce by business leaders and an increased interest by employees in working remotely, we anticipate that up to 20% of the total US workforce will continue to telework post-pandemic. In industries with a high percentage of knowledge workers, we foresee up to 50% of the workforce having remote work accommodations (Figure 2). This equates to a doubling of the US teleworker population post-pandemic in comparison to pre-pandemic times. On a global scale, we see similar teleworker dynamics.

Figure 2: Percentage of U.S. Workforce Working Remotely 2018-2024
(full-time or occasionally)



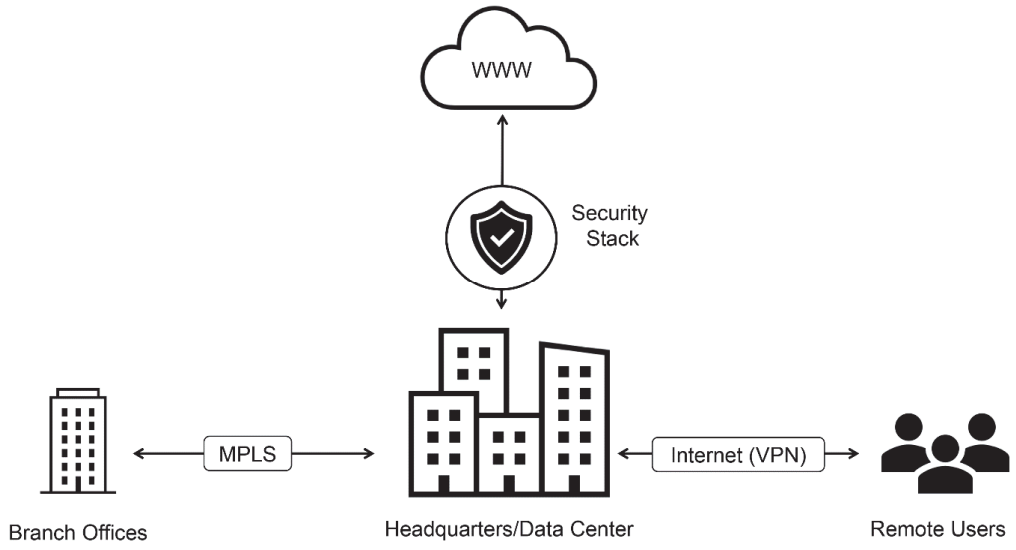
Source: Dell'Oro Group

In the new era of working from anywhere, the long-term scalability, agility and security implications for the enterprise network are significant. In the following section we describe traditional approaches and ensuing challenges.

TRADITIONAL APPROACHES AND CHALLENGES

For decades, enterprises favored the hub-and-spoke network topology (Figure 3). The hub—the corporate headquarters and data center—was at the center of the network. The spokes emanating from the central hub were the network's connections to individual branch offices and remote users.

Figure 3: Legacy Network Topology (Pre-2010)



Source: Dell'Oro Group

Legacy WAN Architectures and MPLS vs. Internet at the Branch

Historically, enterprises have used WANs to connect geographically dispersed locations to each other, to data centers and, more recently, to cloud-based services. The locations are referred to generically as branch offices, though they may vary in physical size, number of people, or bandwidth requirements. In size, they could be as small as a stand-alone kiosk with no staff, or as large as a large factory or office complex with thousands of employees. Bandwidth requirements may range from kilobits per second from a set of sensors, up to gigabits per second from a data center. Enterprises typically deploy one or more customer premises equipment (CPE) devices at each of the locations to perform various networking functions to ensure that traffic is routed securely across the WAN. The devices have typically been deployed and maintained by network engineers sent to the branch offices—an expensive proposition as the number of visits increases.

For WAN connectivity, enterprises have multiple options depending on requirements for network performance, security, location, and cost. Common services used for private, secure network connections with service level agreements (SLAs) are those based on multi-protocol label switching (MPLS) technologies. MPLS connections command premium prices because of their security features and scalability, but they are generally complex and time-consuming to provision, upgrade with more bandwidth, and expand to new sites. Other services—such as broadband Internet, metro Ethernet, and cellular—are also used for WAN

connections. These services provide a wide range of bandwidth, price, and location options, but may not offer the same level of security or performance guarantees as MPLS.

Traditional MPLS WANs were designed with a hub-and-spoke architecture to support static and centralized applications with low bandwidth requirements. However, the enterprise migration to cloud-based services and the growing use of video and mobile technologies have increased bandwidth requirements and changed WAN traffic patterns, making traditional WANs more costly and difficult to operate.

Traditional VPN Architectures for Remote Users

In the legacy network topology, remote users relied on virtual private network (VPN) agents based on Internet Protocol security (IPsec) or Secure Sockets Layer (SSL) on each endpoint (that is, mobile phone or laptop) to connect over the Internet back to VPN concentrator devices located at corporate headquarters.

VPN concentrators were but one of multiple network security appliances composing the enterprise security stack. Also common were firewalls, intrusion prevention services (IPS), email gateways, and SWG appliances. All network security enforcement took place within the centralized security stack as traffic traversed the boundary between the enterprise network and the Internet.

The hub-and-spoke network model worked well for many decades due to four key reasons:

- ***The overall amount of traffic generated by the enterprise was significantly less than today.*** Legacy applications required much less network bandwidth than contemporary networked applications. The corporate spending on MPLS circuits to serve the enterprise bandwidth needs remained reasonable.
- ***The amount of traffic bound for the Internet was significantly less than today.*** Most traffic was between users and applications living within the corporate enterprise. A single connection to the Internet at headquarters, the hub of the network, sufficed.
- ***As a percentage of workforce, the number of remote users remained low.*** Remote users were the exception rather than the rule.
- ***Cybersecurity philosophy was to largely trust all traffic within the enterprise network.*** Internet traffic was untrusted. This philosophy gave rise to the traditional perimeter security stack. With the amount of traffic heading to or coming from the Internet being a minority share of overall traffic, the single central security stack was practical.

Legacy WAN and Traditional VPN Outmoded in the Work-from-Anywhere Era

As the popularity of Software as a Service (SaaS) applications and highly distributed workforces grew, so did the limitations of the hub-and-spoke topology. There is a new confluence of cost, application experience, and security problems:

- ***High cost of MPLS:*** MPLS spending for branch offices became untenable as network bandwidth requirements increased appreciably in order to service SaaS and web applications that required significantly more bandwidth.
- ***Poor application experience:*** Application experience suffered because traffic from branch offices or remote users to an Internet-based SaaS application had to be first backhauled to the Internet gateway in the corporate headquarters.
- ***Perimeter security circumvented:*** As Internet-based SaaS apps became popular, some remote users began to skip the enterprise network altogether and go directly to those apps via the Internet, which created enormous security blind spots. Ensuring that the enterprise network maintained a role in enforcing corporate security became impossible.
- ***Gateway capacity challenges:*** With the increasing number of remote users and traffic from those users, the network teams were in a constant struggle trying to provision the correct amount of VPN capacity to maintain user experience while not overspending.
- ***BYOD uptick:*** The increase in the usage of personal BYOD (Bring Your Own Device) in the corporate setting created new network and security challenges in terms of device onboarding and configuration, and data risks.

WORK FROM ANYWHERE: WHAT ENTERPRISES NEED

According to Mike Frane, Vice President of Product Management at Windstream Enterprise—a provider of award-winning managed communications solutions—enterprises are realizing that legacy network and security architectures are inadequate and overly restrictive for the work-from-anywhere era. In an age where uncertainty is a constant, Mike is assisting his customers to transform their legacy architectures towards one that satisfies the following principles and goals.

Agility

- Ability to easily provision and deliver new networking and security services in a matter of hours, as opposed to weeks or months
- A flexible network edge that can support and secure a wide variety of users, devices, applications, and networks

Scalability

- Capability to scale up and down dynamically based on business requirements
- Ability to serve the business on a global scale and maintain a satisfactory application experience irrespective of location

Security

- Use of user identity, device, network, and application context to make and implement network and security decisions
- Extension of the same network and security controls possible on corporate-owned networks and apps to corporate traffic on the Internet and destined for third-party SaaS apps

Manageability

- A wide array of security and networking services in a unified offering providing central visibility and control that is easy to manage

Optimized

- Reduction in the total cost of ownership either by replacing more costly technologies or lowering IT labor costs

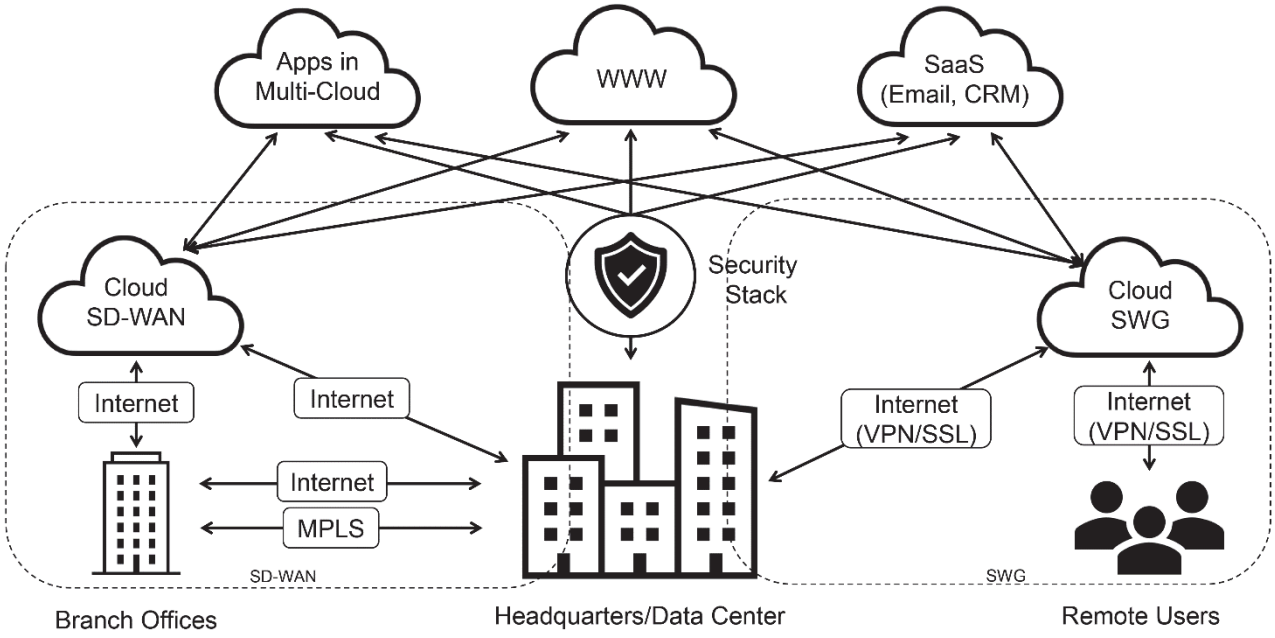
We note that the principles and goals described above are not new. Some of these goals are fulfilled by technologies that have arrived over the last ten years. What is new is that the era of working from anywhere demands a technology approach that is able to satisfy all goals equally well.

In the following section, we describe two technologies that have arrived in the last ten years and service a subset of the goals noted above: software-defined WAN (SD-WAN) and cloud-based secure web gateways. We go on to describe how they are the stepping-stones to the emerging secure access service edge (SASE), which aims to satisfy all goals.

ASCENSION OF SECURE ACCESS SERVICE EDGE (SASE) AND SASE-READY WAN EDGE

The cost, application experience, and security pain points of the hub-and-spoke topology model were the impetus for the emergence of the software-defined wide area network (SD-WAN) and cloud-based secure web gateway, starting in the late 2000s (Figure 4). SD-WAN emerged to address the pain points associated with branch offices, while cloud-based SWGs emerged to address the pain points on the remote user side. In the following sections, we summarize each, since both are fundamental to SASE.

Figure 4: Current Network Topology (2010 to Present)



Source: Dell'Oro Group

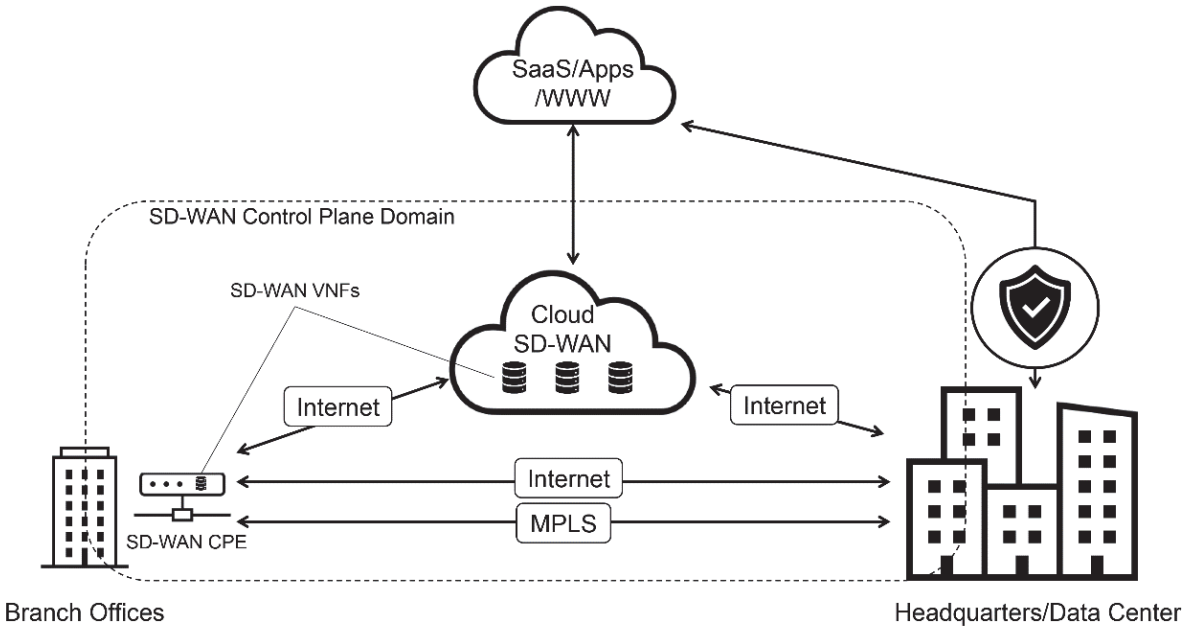
SD-WAN for the WAN/Branch Office

SD-WAN joins the concepts of software-defined networking (SDN) and network function virtualization (NFV) to form an alternative networking solution that leverages cheaper and faster broadband Internet connections, and addresses many of the shortcomings of traditional MPLS-based WAN.

Based on SDN's principle of separating the software control plane from the hardware data plane, SD-WAN uses control plane abstraction to manage multiple aspects of the WAN, including devices, connections, routing, policies, and security. SD-WAN also leverages NFV to run virtualized network functions (VNFs), such as routing and security, on commoditized hardware rather than on proprietary equipment, which had historically been used in WANs.

SD-WAN's core components include the SD-WAN control plane software, the CPE and associated network functions, and WAN connectivity (Figure 5).

Figure 5: SD-WAN Topology



Source: Dell'Oro Group

SD-WAN control plane software is a key element of SD-WAN solutions. It is the central authority that sets policies at the application level to prioritize network traffic and direct that traffic by enforcing policies. The software also treats multiple WAN connections as a pool of bandwidth resources, whether they are private MPLS networks or public Internet connections. The control plane software is run from a centralized location or the cloud.

SD-WAN CPE devices route traffic onto the WAN network. Depending on vendor implementation, they may perform additional network and security functions. The SD-WAN control plane software directs SD-WAN CPE devices' forwarding behavior. The three common forms of SD-WAN CPE devices are access routers, firewalls, and dedicated SD-WAN appliances.

Decoupling network functions from hardware via VNFs is key to SD-WAN's scalability, flexibility, and—ultimately—to better TCO. SD-WAN vendors differentiate in terms of where VNFs reside in the SD-WAN architecture. VNFs can be fully distributed and executed within each CPE, fully centralized as a cloud-based service, or can combine the two approaches.

As noted earlier, many enterprises have run into cost and bandwidth challenges with MPLS-based WANs. In contrast, the Internet is ubiquitous, is much lower in cost, and offers higher speeds compared to MPLS. However, Internet connections do not offer the same level of SLA and security compared to MPLS. This is where SD-WAN functionality for prioritizing, directing, and securing network traffic across the optimal path makes it such an attractive solution. For most applications, SD-WAN solutions can make Internet connections function much like private MPLS circuits at a substantially lower cost and, typically, with better performance than the MPLS circuits they replace.

Cloud-based Secure Web Gateways (SWGs) for Remote Users

A new breed of SWG solutions delivered from the cloud began to appear in the late 2000s to address emerging challenges with the increase in remote users and cloud application usage.

Cloud-based SWGs arose from the traditional on-premises SWG appliance landscape, which for many years was considered to be a vital part of the centralized enterprise security stack. Cloud-based SWGs reinvented the traditional SWG appliance into a cloud-native, multi-tenant central service.

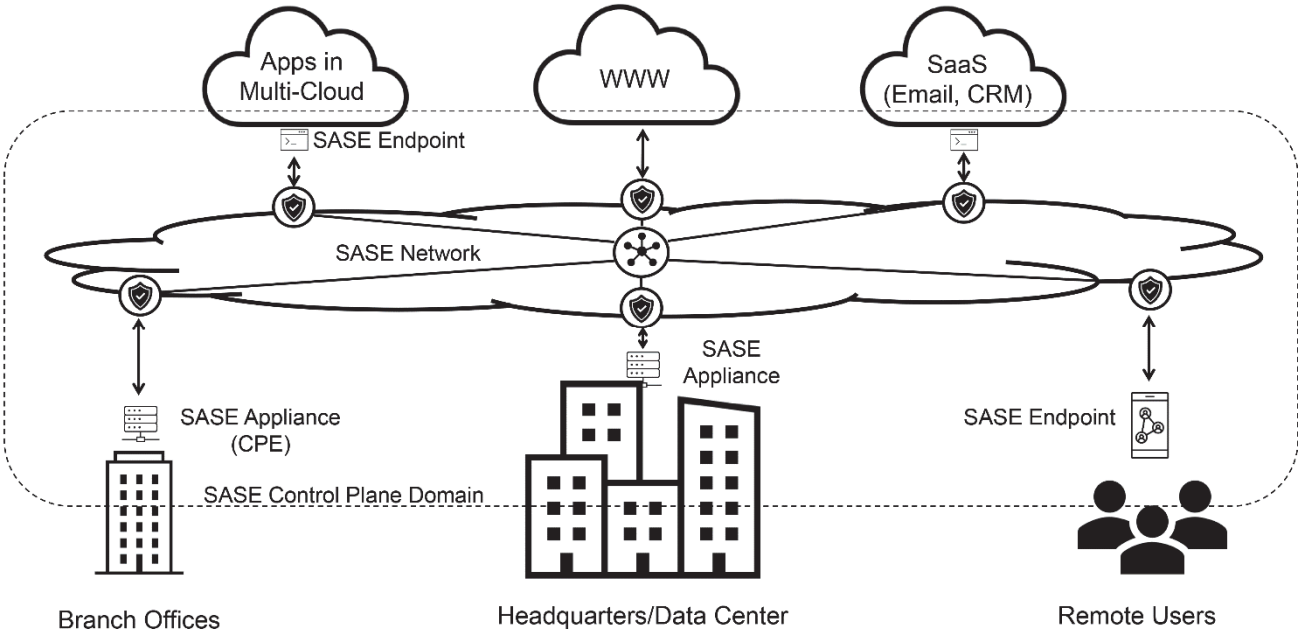
The architecture of cloud-based SWGs shares significant commonalities with SD-WAN, including:

- Merging the concepts of SDN and NFV to create a network security solution that changes the way enterprises secure remote users and applications.
- Using control plane abstraction to centrally manage how IT controls and secures connectivity between users and applications.
- Leveraging VNF to perform security processing in a scalable and flexible manner. Requiring the logical equivalent of an SD-WAN CPE device at each endpoint to help onboard and direct traffic. In cloud-based SWGs, the logical equivalent of the CPE is the endpoint agent: the client software or configuration. Endpoints are the users and applications connecting to the network.

SASE: The Union of SD-WAN and Cloud-based SWGs

SASE (pronounced "sassy") is a service-centric, cloud-based solution for providing network connectivity and enforcing security between users, devices, and applications. SASE utilizes centrally-controlled, Internet-based networks with built-in advanced networking and security-processing capabilities (Figure 6).

Figure 6: SASE Architecture



Source: Dell'Oro Group

Considering the numerous commonalities between SD-WAN and cloud-based SWGs, it was inevitable that these two technologies would intersect. With SASE rooted in SD-WAN and cloud-based SWG precursors, it shares the same architectural underpinnings and is composed of similar components. SASE consists of five components: the control plane software, endpoints, appliances, functions, and the network.

1 *SASE Control Plane Software*

The SASE control plane software is the brain of a SASE solution. It is able to set network and security policy at a granular level, and secure and direct network traffic by enforcing policies. It makes network and security decisions based on multiple criteria, including user identity, device state, time of data, user/device location, bandwidth, latency, destination, and application. This provides fine-grained security control and increases the efficiency, performance, and security of individual users and applications that traverse the SASE network.

2 *SASE Appliances*

SASE appliances aggregate traffic from users, devices, and applications that are unable to connect directly to a SASE network. For example, a SASE appliance may be deployed to provide secure network connectivity to all users, devices, and applications at the branch office. SASE appliances are under the control of the SASE control plane software.

3 *SASE Endpoints*

SASE endpoints include all the users, devices, and applications utilizing the secure network connectivity services provided by the SASE solution.

SASE endpoints include logic by which to connect a SASE network. It may be as simple as using web proxy configuration. More typically, the SASE endpoint logic consists of a software agent provided by the SASE vendor. Software agents allow richer interactions with users, devices, and applications. For example, on a device, the software agent can participate in the authentication to the SASE network by providing the user identity and device state, requesting specific services of the SASE network, and encrypting user traffic via SSL/IPsec between the user and SASE network.

4 *SASE Functions*

Similar to SD-WAN and cloud-based SWGs, SASE leverages NFV to run VNFs in a distributed fashion, nominally in the cloud. VNFs perform either a network function or security function.

Common networking functions include bandwidth optimization, caching, content delivery network (CDN) services, cost optimization, deduplication, load balancing, path selection and resiliency, quality of service (QoS), routing, and traffic shaping.

Common security functions include secure proxying (traditional SWG), cloud application security broker (CASB), zero trust network architecture (ZTNA), firewall as a service , and remote browser isolation (RBI).

5 *SASE Network*

The SASE network is at the heart of the SASE architecture designed to connect all SASE endpoints and appliances together, and bridge their connectivity to the Internet. It is controlled and managed by the central SASE control plane software. The SASE network lives on the Internet and leverages the ubiquity of the Internet to provide the last mile connectivity to all connected assets. Within the SASE network live the SASE functions to route and secure traffic.

By merging and improving upon standalone SD-WAN and cloud-based SWGs, SASE brings together networking and security into a unified service offering that provides the necessary agility, scalability, security, and optimization for the work from anywhere era.

CONCLUSION

While remote work is not new, we are entering a new era where many enterprises are realizing that their legacy WAN and VPN architectures are inadequate. SASE solutions that build and improve upon standalone SD-WAN and cloud-based SWG solutions should be at the top of the list for any enterprise seeking to address the needs of the new work from anywhere era.

About Authors:

Mauricio Sanchez joined Dell'Oro Group in 2020, and is responsible for Network Security & Data Center Appliance market research program, as well as Security Access and Service Edge (SASE) Advanced Research Report. He brings over 20 years of experience as an executive manager in networking and security technologies, products, and solutions spanning data center, campus, and mobile architectures. Mr. Sanchez helps shape the coverage of next-generation networking architectures and services models. Mr. Sanchez's research and analysis has been widely cited in leading trade and business publications. Mr. Sanchez is a frequent speaker at industry conferences and events.

Email: mauricio@delloro.com

Shin Umeda covers a broad view of Telecommunications Infrastructure at Dell'Oro Group as he has built our coverage and researched many of the technologies. He is currently responsible for our SP Routers and SD-WAN market research. Mr. Umeda's research and analysis has been widely cited in leading trade and business. He has appeared as an invited speaker and judge at industry conferences. He has also presented at investor conferences, customer seminars, and sales meetings around the world.

Email: shin@delloro.com

About Dell'Oro Group

Founded in 1995 with headquarters in the heart of Silicon Valley, Dell'Oro Group is an independent market research firm that specializes in strategic competitive analysis in the telecommunications, networks, and data center IT markets. Our firm provides world-class market information with in-depth quantitative data and qualitative analysis to facilitate critical, fact-based business decisions. Visit us at www.delloro.com.

About Dell'Oro Group Research

To effectively make strategic decisions about the future of your firm, you need more than a qualitative discussion – you also need data that accurately shows the direction of market movement. As such, Dell'Oro Group provides detailed quantitative information on revenues, port and/or unit shipments, and average selling prices – in-depth market information to enable you to keep abreast of current market conditions and take advantage of future market trends. Visit us at www.delloro.com/market-research.

Dell'Oro Group
230 Redwood Shore Parkway
Redwood City, CA 94605 USA
Tel: +1 650.622.9400
Email: dgsales@delloro.com
www.delloro.com