INSIGHTS | **TECH BRIEF**

Written By Terry Dever
WEI Solution Architect & Professional Services Engineer

Simplify Network & Security: Introducing SASE & Why It Is Needed

Today, enterprise networking and security face a growing challenge stemming from an ever-expanding attack surface and company perimeter (every user and every application is a company perimeter). The front line is everywhere! With the majority of employees working off site, and the majority your enterprise data is off site in the cloud/in SaaS applications etc., each of these factors produce data leaks, resulting in a "perfect storm" for data security.

Our collective goal is to keep data and customers secure. That said, attackers know there is an "attack surface explosion" today. Consequently, zero-day malware (unknown malware) has also exploded in volume. In 2019, cyber companies like Palo Alto Networks mitigated two billion pieces of zero-day malware daily. Two years later in calendar Q2 2022, that figure jumped to 224 billion daily (also fully mitigated).

Companies have more borders and perimeters than what meets the eye:

- Cloud-based SaaS applications containing your internal data and intellectual property.
- Increasingly more mobile users globally.
- Headquarters, data centers and branches with legacy Internet and WAN edge appliances.
- Networking and security point products all managed seperately (firewall stack, routing layer, decryption appliance, IPS appliance, proxy service, URL filtering appliance, etc.) do not correlate threat intel with each other in real time. Thus, many have become obsolete.

The future of enterprise networking and security depends on how well the features are delivered. Features must excel in a way that is real time, automated/cloud-delivered, reliable, scalable, and flexible versus solving networking and security issues with point products (each one with its own specific use case). When deploying point products, they can be complicated by themselves and complex to manage many at one time.

51%

of IT decision makers indicated **'security and compliance concerns'** as a top driver for digital transformation.[1]

CYBERSECURITY

Gartner identifies the key components of SASE, which are:

- **SD-WAN:** Flexibly optimize WAN performance across several branches and data centers.
- **Security as a Service:** Includes Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), and SaaS Security.
- **Firewall as a Service** (FWaaS).
- **IAM (Identity and Access Management):** Authentication and authorization so that only legitimate users and devices can access internal data resources.
- **Data Loss/Leak Prevention:** Prevent sensitive data from being leaked or improperly accessed.
- **ZTNA 2.0:** All security services are built on the pillars of ZTNA 2.0.

SASE is a single "as a service" subscription-based product, combining the WAN (Wide Area Network) edge device functionality (on prem SD-WAN edge devices, bandwidth aggregation, visibility into traffic, guaranteed SLA for traffic, WAN optimization, remote branch segmentation, etc.) with next-gen L3-L7 "security as a service" (FWaaS, SWG, URL Filtering, Client VPN, remote branch networking, Advanced Threat Prevention powered by AI, CASB and sometimes Explicit Proxy functionality).

SASE is cloud delivered and globally deployed, meaning your service, with all the same capabilities, is available globally, self-healing, scalable, and elastic. SASE is designed to handle more users and more capacity automatically, eliminating the backhauling of traffic and users to one HQ, data center, or branch hub, as opposed to point product appliances in one or two specific places (which the admin also must manage and maintain). These point products can be prone to oversubscription. SASE is built on the architecture/pillars of ZTNA 2.0, which is also simple to deploy, manage, and is globally available. This means the flexible service is always close to the user and branch, is simple to configure, and decreases latency (users to applications, users to data centers, users to branches, etc.).

Keep In Mind What SASE Is NOT:

- **It is not** an SD-WAN deployed, then an SSE (secure service edge or security as a service) deployed, and the two solutions either do not interoperate with each other or are not configured to interoperate with each other (like two ships passing in the night or two point solutions).
- **It is not** traditional hardware, a "castle and moat" network perimeter protection strategy, and does not perform daisy-chaining for on-prem point security solutions to form an "offensive line" of security.
- **It is not** a series of on-prem "boxes" forming a full mesh over a public or private WAN.
- **It is not** a creatively packaged telco bundle.
- **It is not** rigid, stagnant, complicated, or limited (visibility, changes)
- **It is not** simply cloud delivered SSE deployed without SD-WAN at the customer WAN edge. There are leaders in the SSE space, but a company cannot be a leader in the SASE space without delivering a "secure service edge" and SD-WAN, according to Gartner.
- **It is not** a one-size-fits-all total replacement for all security solutions for every single enterprise. Most companies could really use a SASE solution, while other companies do not have a fit or a need for it today. All of that is okay!

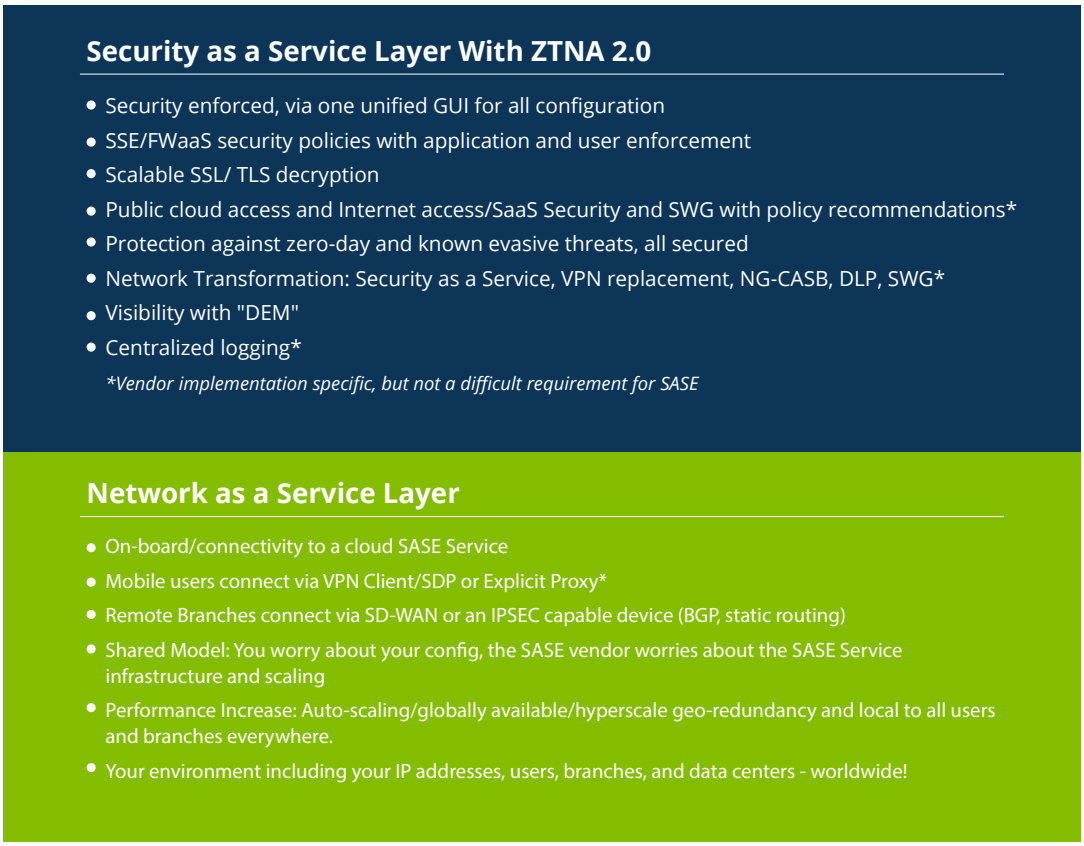
Thinking Of SASE In Two Layers

It helps to think of SASE as broken up into two layers, similar to how we've used the OSI model to make sense of networking in the past:

- **The "Service Edge" Layer:** Once the users and remote sites are connected to the SASE service, how do they route to each other and how is data secured, especially against known and unknown malware as well as data loss prevention, as data moves from site to site or to the Internet?

Below is a user-friendly representation of this:

Once the user and branch are connected to the SASE service, they have pervasive, location independent, globally



deployed and distributed/security as a Service with real-time intelligence to detect anomalous flow and protection for all traffic against known and unknown threats and vulnerabilities at line speed. This is possible within scalable/centrally managed and simple/low latency/scalable and elastic features. This is the "Security as a Service" layer.

SASE is a cloud delivered networking and security as a service, simplifying networking and security, all in one "as a service" globally available product, based on the pillars of ZTNA 2.0. It is taking your network from technologies that worked well in the 1990's, the 2000's, the 2010's and earlier in the 2020's, then systematically transforming your WAN edge and security, to arrive at the goal of arriving at and keeping your network security built within the ZTNA 2.0 framework.

What is ZTNA 2.0?

Let's now deep dive into ZTNA, which is a framework for security, not a product. If we boil ZTNA down to one phrase, *it is Zero Trust with NO Exceptions.*

If we look at client VPN and site-to-site branch connectivity prior to SASE, we typically could not enforce any secure granularity as to which people or networks could access which applications and then what they could do with applications. There was virtually no data inspection. Users and attackers had free access, data could leak out, there could be exploit attempts that we were unaware of, etc. Attackers had free access if they were on your network!

Traditional networks and VPNs were designed to grant full network access, without security for the most part, while most resources were on-prem. This caused many security issues such as:

- **Uninhibited Access:** You need strict access controls while classifying applications. You don't want too much access, especially for applications that use dynamic ports or IP addresses.
- **Allowed And Ignored Access:** Once access to an application is granted, that communication is then trusted forever. You don't want to assume that the user and the application will always behave in a trustworthy manner. This is a complete handoff of a connection with no more traffic inspection happening. Now, there's no way to fend off known or unknown attacks
- **Too Little Security:** Security for all applications, including applications using dynamic ports like voice and video applications, SaaS applications have been completely overlooked. What about server-initiated applications like HelpDesk and patching systems?

Legacy network architectures completely ignored strict access control and, as a result, most people and corporations still have little to no visibility or control over data. Legacy network architectures fall prey to security issues when it comes time for legacy VPN/ SWG replacement, SaaS Security and even with branch transformation, only to discover it doesn't live up to their needs/expectations.

Work is no longer a place we go, but an activity we perform despite our location. During and after the Covid-19 pandemic, many businesses scrambled to scale their client and site-to-site VPN infrastructure. So, the ideal situation would be to perform strict authentication, but also restrict which users can access which applications, continuously inspect traffic inline.

Modern networks require next-gen security. SASE is a solution which delivers network access and security based on the five pillars of ZTNA 2.0:

1. **Least Privilege Access:** Enabling precise access control at the application and sub-application levels, independent of things like IP and port numbers. Continuously evaluated "Trust"/MFA Integration/ Users connect to resources through the SASE Service/ session is authenticated/Identify applications users require access to/Secure Application access granted per user or by group (example being security by user(s) accessing which application(s) via posture-assessed trusted device.)
2. **Continuous Trust Verification:** Once access to an application is granted, trust is continually assessed based on changes in device posture during the life of the connection, user behavior and application behavior. An example is continual device posture checks to continually assess any changes in endpoint posture, enforce authorization, ensuring proper user and application behavior, blocking inappropriate user, application, or traffic behavior.
3. **Continuous Security Inspection:** Providing deep and ongoing inspection of all traffic, even for allowed connections, to prevent all threats including zero-day threats and block inappropriate application behavior. What if, during an application connection data starts flowing to some unknown destination? An example is if the adversary takes over a connection or was there all the time, the SASE Service will inspect the connections for misbehavior, see exploits, vulnerabilities and stop code executions. This is performed all in real time, whether the malware was previously known or is a true "zero day" unknown piece of malware code or campaign, because anomaly and threat prevention (depending on SASE vendor implementations) should use AI, deep learning and machine learning to stop threats in real time to out-pace the attackers.

4. **Protection of All Data:** Prevent data loss and loss of your intellectual property! It is your data. Take control of it! The SASE Service takes control of data across all applications in the enterprise, including private applications and SaaS applications, all with a single DLP policy.
5. **Security for All Applications:** Safeguarding all applications (not just web-based or DNS based applications) used across the enterprise, including modern cloud-native applications, legacy private applications and SaaS applications. This includes applications using dynamic ports and applications that leverage server-initiated connections.

Why Do You Need SASE?

To mitigate the aforementioned attack surface explosion, you need flexible, consistent security as a service everywhere, wherever your company is, wherever your employees are, to do one thing: transform your network and security while keeping your data secure.

The SASE service needs to mitigate zero-day malware natively using mechanisms such as AI/machine learning/deep learning. It needs to replace legacy site to site and client VPN solutions that were implemented years ago. It needs to include and support SD-WAN. It needs to be a FWaaS, SWG, CASB, provide security for public and private SaaS applications, potentially be an explicit proxy (vendor dependent), provide deep visibility into all data traversing this SASE service, needs to perform SSL Decryption at scale, all without oversubscription of resources.

- **Assess Current Security Posture:** Evaluate if your organization has a consistent security policy across the enterprise or if gaps exist due to disparate tools or systems.
  - Identify the weakest links in your security infrastructure.
  - Consider resource requirements for managing on-premises security, including downtime, patches, appliances, and manpower.

- **Unified Security and Networking:** Replace fragmented "point products" with a cloud-delivered solution offering:
  - A single unified console for streamlined management.
  - Coordinated threat intelligence sharing across security features.
  - Reduced dependency on hardware patching, power, and cooling.

- **Cloud-Native, Cloud-Delivered Benefits:** Leverage a scalable, elastic, globally available solution to:
  - Provide consistent policies and Zero Trust Network Access (ZTNA 2.0) to users and branches worldwide.
  - Cut costs by retiring outdated WAN technologies (e.g., MPLS).
  - Optimize WAN and internet traffic without geographic constraints.

- **Key Features:** Ensure the SASE solution includes:
  - Security services: SWG, CASB, Firewall as a Service, Threat Prevention (e.g., antivirus, DNS security, URL filtering).
  - SD-WAN capabilities.
  - Support for SaaS security with DLP, encryption, and decryption.
  - Visibility and monitoring for all traffic.

- **Comprehensive Connectivity:** Secure all access points:
  - Mobile users (VPN replacement).
  - Remote branches and data centers.
  - Safe web browsing through Remote Browser Isolation.

Talk to WEI today

Contact the WEI cybersecurity team to learn more about SASE and why it could make sense for your business operations.

Sources:

1. IDG Research commissioned by WEI, January 2021.

About WEI

WEI is an innovative, full service, customer centric IT solutions provider.

Why WEI? Because we care. We go further.

WEI is an expert in business technology improvement, helping clients optimize their technology environments and work efficiently. WEI works with clients to understand goals, integrate strategy with technology solutions, and leverage their current IT environment into one company-wide model to increase utilization and efficiencies around their unique business processes.