WHITE PAPER

ZTNA AND SASE BETTER TOGETHER, CLOSER THAN EVER

SASE is a global service that provides remote users with secure, direct, and high-speed access to their cloud-based applications. ZTNA adds new security layers that extend SASE benefits to more users, located anywhere, using any device.

open-systems.com

In the days of old, IT professionals relied on technologies like firewalls to keep out bad actors. With perimeter security in place, and users and applications protected inside, tech experts and upper management were confident that their organizations had appropriate cyber safeguards.

But with the rise of mobility, more corporate users began to connect to enterprise resources from various remote locations – outside the perimeter. Then the cloud took hold, and more and more business applications moved from on premises to cloud service providers. As more users worked remotely and more applications moved to the cloud, the perimeter became murkier. The once clearly delineated network edge around which IT experts set up perimeter security needed to evolve.

Today, the enterprise edge can be anywhere and everywhere. This is prompting enterprises to seek new cybersecurity solutions to address this new reality.

> “SASE unifies cybersecurity and networking into an easy-to-manage cloud-based service that is flexible and fast. Organizations can connect users to applications quickly and react to new opportunities with greater insight, confidence, and agility.”

"With SASE and ZTNA, any user on any device working in the park, corporate headquarters, or from home will have the same work experience."

SASE ADDRESSES THE EXPANDING ENTERPRISE EDGE

Secure access service edge (SASE) emerged to help organizations safeguard applications and users in this new enterprise environment. SASE provides fast, secure communications by delivering optimal network connectivity and cloud-based security as close as possible to the user.

More organizations are beginning to realize that perimeter security is not enough. Enter SASE. In the "Top Actions From Gartner Hype Cycle for Cloud Security, 2020" report, "Gartner predicts that by 2024, at least 40% of enterprises will have explicit strategies to adopt SASE, up from less than 1% at the end of 2018." [1]

ZTNA ENABLES ACCESS WITHOUT SHARING THE KEYS TO THE CASTLE

In addition to SASE, cybersecurity architecture called zero trust network access (ZTNA) – which authenticates and authorizes users and any-to-any communications – is taking off. Gartner's "Zero Trust Architecture and Solutions" report says that "by 2023, 60% of enterprises will phase out most of their remote access virtual provider networks in favor of ZTNA." And that "by 2023, 40% of enterprises will have adopted ZTNA for other use cases." It adds that "by 2022, 80% of new digital business applications opened up to ecosystem partners will be accessed through ZTNA." [2]

Organizations use ZTNA to allow users (such as employees, contractors, or partners) and devices (that could be managed or unmanaged endpoints in any location) to access applications and data (that could be anywhere) in a secure and dynamic fashion.

Mergers and acquisitions were a key initial driver of ZTNA. When two companies merge, they have two sets of users and environments. ZTNA provided easy and secure access to each of the infrastructures. The pandemic drove even broader adoption of ZTNA because users are on the move and, with accelerated cloud adoption, applications are everywhere. [3]

Traditionally, granting access to enterprise IT resources meant handing over the keys to the castle. Once access was given, users were inside and had broad access to resources, some of which they didn't need or shouldn't try to use. Traditional methods for zoning users and controlling access were already complex and difficult. When you add securing cloud applications and controlling remote users, managing access became worse. In fact, properly authenticating a remote user on an unmanaged device to a cloud-based application became nearly impossible.

ZTNA does away with traditional wall-and-moat-style perimeter security. It shifts security from static network perimeters and places it wherever users, assets, and resources intersect – on premises or in the cloud. ZTNA leverages a set of technologies that authenticates users on unmanaged devices located anywhere, and gives them secure and direct access to applications and resources located anywhere.

ZTNA employs preset policies to granularly – and dynamically – control who and what gets access to which IT resources no matter where they are located. Users are never given access to the network. They are only given access to the applications they are authenticated and authorized to use, and nothing more. This protects the network and other assets.

> “Using a single fully integrated SASE-ZTNA service simplifies connecting users to applications, eliminates multi-vendor complexity and cost, and provides a higher security posture.”

Authentication and access are enforced in the cloud or on premises using ZTNA access control points. Authentication and authorization are based on many factors, including user identity, time of day, location, device identity, device posture, and more. As a result, employees and partners only get direct, isolated access to the resources they need.

SASE AND ZTNA AMPLIFY ONE ANOTHER

ZTNA and SASE can exist separately. But they are better together.

SASE is a service that includes complete network and cybersecurity functions such as application visibility, encryption, routing, SD-WAN services, application optimization, secure web gateway, cloud access security broker (CASB), secure email gateway, and next-generation firewall services. SASE authenticates a user and grants access using traditional means. When ZTNA is integrated, it takes over access control for the resources and applications ZTNA is configured to secure – in the cloud or on premises. ZTNA starts with zero trust “no access” and then grants access to resources based on policies and the level of available authentication information. ZTNA authenticates users with a broad range of information and enriches it with data from SASE security technologies.

The benefit of adding SASE information to other ZTNA-collected information is that the flexibility and precision of ZTNA are greatly improved. Moreover, when ZTNA is integrated with SASE, access enforcement using SASE technologies is more thorough.

ZTNA makes SASE more powerful as well. With ZTNA, SASE can securely extend its reach to include more users and partners, connect to managed and unmanaged devices, and reduce or eliminate the limitations and security risks associated with VPNs. In addition to greater reach, IT professionals gain more precise, secure, and easier to manage access control. Adding ZTNA to SASE provides more extensive and deeper cybersecurity visibility across the entire infrastructure.

That is why Open Systems considers ZTNA an essential component of a SASE solution.

TIGHT INTEGRATION BETWEEN ZTNA AND SASE IS KEY

Enterprises that choose a single solution where ZTNA and SASE are unified into one service derive maximum value – quickly.

Integrating separate ZTNA and SASE solutions means a business has to contend with multiple contracts and vendors. In this scenario, SASE and ZTNA are stitched together, and a change on one may require manual configuration of the other. This also means that enterprises will need to monitor separate control consoles and coordinate two independent customer service departments. It will take months to integrate everything as promised and, in some cases, that promised integration is never realized at all.

Tight integration is even more important once the cybersecurity solution is up and running. When an enterprise has to integrate multiple systems, there are multiple interfaces. Each one represents a potential point of failure and cybersecurity vulnerability. This is problematic because ZTNA and SASE are both business-critical. If ZTNA or SASE has an issue, cybersecurity may be compromised, or users can’t access the IT resources they need to be productive, both of which will have a negative business impact. By selecting a single platform that tightly integrates ZTNA with SASE, enterprises can avoid such problems.

Enterprises integrating ZTNA with SASE also need to consider the maintenance implications of their solution and supplier choices. Lack of tight integration means that if an enterprise is updating one solution, it must ensure the new patches don't cause issues with the other solution. An upgrade on one may even cause a security configuration error and vulnerabilities in the other.

GAIN GREATER CONTROL, PRODUCTIVITY, AND RELIABILITY

Organizations today need to guard against sophisticated cybersecurity threats to their increasingly distributed, far-flung IT environments – at a time of great change and competition. That represents a significant challenge to business leaders, cybersecurity experts, and organizations.

Securing an enterprise against cyberthreats is never easy. Businesses can reduce cost and complexity while heightening their cybersecurity posture by using a fully integrated and seamless SASE-ZTNA cloud-based platform that addresses today's requirements and is built for the future.

Open Systems incorporates ZTNA and SASE into a single and seamless platform, relieving enterprises of the burden and pitfalls of integrating ZTNA with a separate SASE platform. Open Systems SASE with ZTNA is offered as a single unified cloud-based service supported by Mission Control, our 24x7 globally connected NOC, staffed by level-3 certified experts. You can begin with SASE or ZTNA and add the other service when you are ready.

To learn more,
visit Open Systems.

[1] Gartner, Top Actions From Gartner Hype Cycle for Cloud Security, 2020

[2] Gartner and Qi An Xin Group, Zero Trust Architecture and Solutions, n.d.

[3] PwC, Can You Meet Customer Demand for Cloud-Based Computing?, 2020

Open Systems connects and protects users, apps, and data everywhere they reside with a comprehensive, unified easy-to-use technology platform combined with an excellent 24x7 Managed SASE service.

Learn more at open-systems.com | Approved for public use.