Barracuda
Your journey, secured.

How SASE empowers your business for the cloud generation.

Traditional networking and security concepts are obsolete when adopting the public cloud for digital transformation.

WHITE PAPER

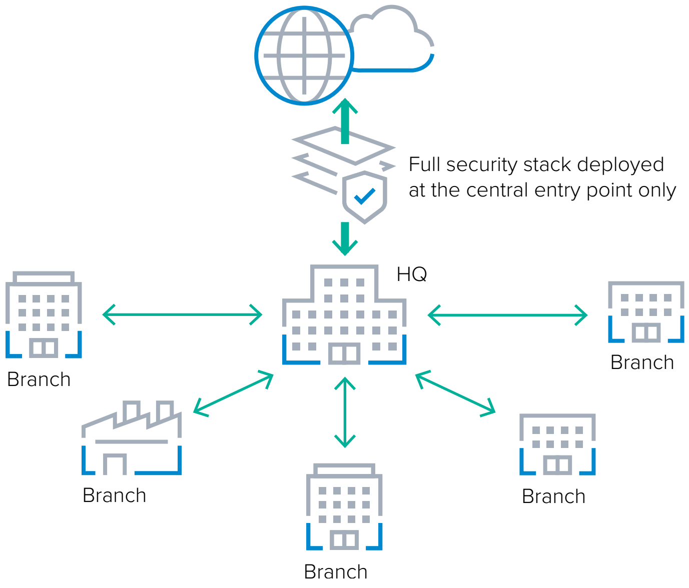
NETWORK SECURITY

Traditional networking and security concepts are obsolete when adopting the public cloud for digital transformation.

SASE solutions by Barracuda Networks accelerate all-in public cloud initiatives by providing ubiquitous cloud access for every branch, access to the fastest global WAN backbone, cloud delivered security enforcement, and Zero Trust Access to any app for all remote employees.

Introduction

Wide area networks (WANs) have played a critical role in business growth for several decades. Early WANs were used to provide mainframe access to remote terminals using networking protocols that were in place long before IPv4 came along. These networks were gradually replaced by WANs that used expensive point-to-point leased lines to connect local area networks across multiple locations. By backhauling traffic from branch offices to the data center, companies could centralize security resources in one location and avoid the overhead of distributed security appliances.

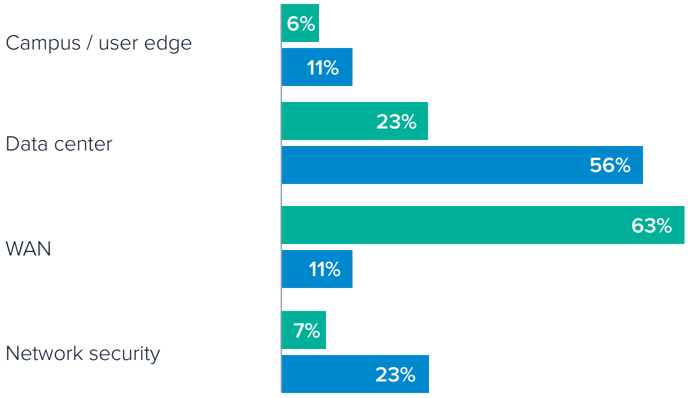


Classic backhauling architecture with a single gateway

As WAN technology matured and software as a service (SaaS) became popular, legacy WANs gave way to new architectures built around branch office firewalls with secure internet breakouts alongside site-to-site virtual private networks (VPNs). This solved the problem of network congestion caused by backhauling, but it created additional overhead at each branch office. By the early 2010s, companies all over the world were struggling with multiple vendors and legacy technologies with no single pane of visibility into networking, security, performance, or compliance.

In early 2016, market analyst firm Gartner conducted a survey of high-profile technology managers and decision makers.

Which portion of your network is the most expensive / most critical?



Gartner Data Center Conference 2016 (n=94 / 84)

Companies were looking for a way to resolve the disparities between priorities and costs, and they found it in cloud services and SD-WAN.

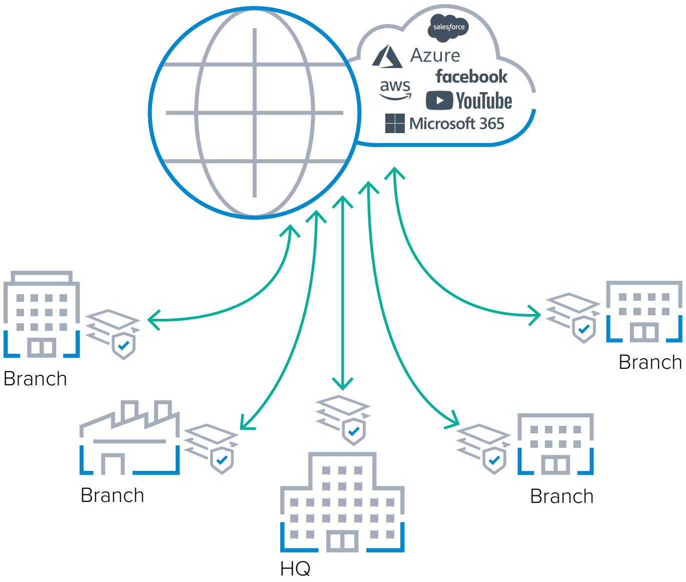
Beyond the software-defined WAN

Gartner defines software-defined WAN (SD-WAN) as solutions that “provide a replacement for traditional WAN routers and are agnostic to WAN transport technologies.” Because SD-WAN is both carrier- and transport-agnostic, it can use any transport mode regardless of who provides it or where the network edges are located. Network traffic is managed intelligently across these transports for the best network performance.

Enterprise bandwidth requirements were increasing, and SD-WAN solutions enabled corporate technology budgets to keep up with these needs. Simplified deployment, rapid bandwidth provisioning, and centralized administration reduced the time and effort needed to manage the WAN. And because SD-WAN is transport-agnostic and supports multiple links, redundancy and failover are baked into the network. ‘Always-on’ internet connectivity had become mission critical, and SD-WAN made this easier and less expensive to deploy.

Industry analysts watched carefully as SD-WAN displaced older technology and became the “backbone of the enterprise.” Branch-to-branch and branch-to-site connections were losing relevance outside of proprietary application requirements, and Gartner analysts predicted that most enterprise data centers would be eliminated by 2025.

This shift in the business technology landscape brought new challenges. How do companies make sure that all locations and all users are always connected to the public cloud? What is the most efficient way to provide access to data and applications to remote workers? How can IT deliver the best possible internet performance while keeping costs aligned with priorities? How can IT provide application performance from anywhere across the globe without having to host the application in various regions or spend a fortune on private lines and co-location providers? How can IT scale the network and the related security enforcement dynamically up and down according to current demand? How can IT apply and scale security and access policy to all offices and remote employees equally?



SD-WAN architecture for accessing internet and SaaS solutions

The solutions to these challenges were found in a completely new technology framework known as Secure Access Service Edge.

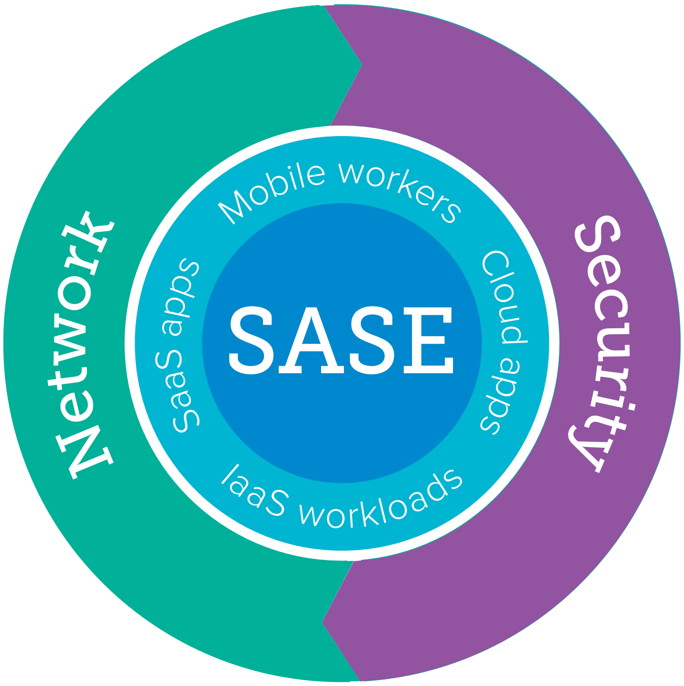
Digital transformation "all-in" with SASE

Secure Access Service Edge, or SASE, is a simple concept put forth by Gartner in a 2019 research note. SASE (pronounced "sassy"), is based on a simple assumption:

If the vast majority of data, applications and servers is hosted in the public cloud or as a SaaS solution, it just simply makes sense to move away from traditional data center and "protected network edge" in favor of **direct cloud access** where everything needs to be considered as an **edge and secured and managed by a cloud service**. Hence the name Secure Access Service Edge. So, when optimizing networking around ubiquitous anytime anywhere access to the cloud, the next logical step is to move all routing, networking, and security functions there to. Once this is done the next step is to provide secure access for remote users.

Traditional VPN solutions turn out to be not agile enough, costly and inflict quite an overhead on the typical remote user. When establishing a VPN connection, the device is essentially "teleported" into the network, and any possible infection that can spread and infect the applications with it. ZTNA, short for Zero Trust Network Access, an upcoming technology at the time, solves these issues. Connectivity is seamless for the end user, only the application currently needed is accessed, network level infections and malware are kept out by definition.

Combining all these services and functions into a cloud delivered service enables enterprises to deploy and scale their resources as needed, enjoying unprecedented agility and network performance across the globe.



Barracuda CloudGen WAN: the SASE you need in the cloud you want.

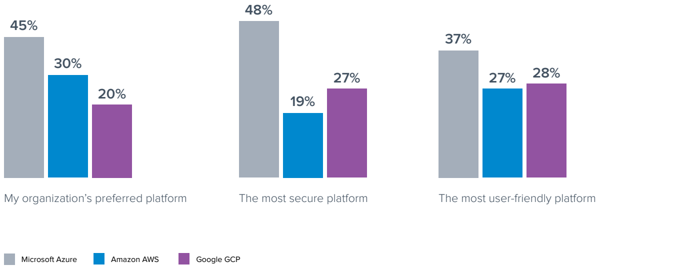
Barracuda CloudGen WAN provides cloud on-ramp with Secure Web Gateway (SWG) and Next-Generation Firewall as a Service (NGWFaaS) for remote endpoints connecting to the SASE entry point hosted in any of the Azure Regions as well as private SASE entry point capabilities.

Office locations are connected to the SASE service by means of the CloudGen WAN site devices. These provide cloud on-ramp capabilities including SD-WAN with simultaneous use of up to 16 physical internet connections that are constantly evaluated by dynamic bandwidth and latency detection. This information is used in application-based routing to dynamically assign available bandwidth, uplink, and routing information based on protocol, user, location, and content as well as application, application category, and even web content categories. This even works for application and traffic flows across multiple logical VPN tunnels spread across multiple physical uplinks and ensures application traffic always uses the best possible uplink for the use case. In the event of adverse network conditions adaptive session balancing and adaptive bandwidth protection selectively shift recreational lower priority traffic to less suitable links or blocks recreational traffic completely until the network conditions have been restored.

At the network level the SASE site devices use built in link optimization technology with advanced Forward Error Correction (FEC) technology to optimize real time traffic like VOIP or video communication. The implementation uses Random Linear Network Coding (RLNC) technology to overcome packet loss by sending repair packets. Using Forward Error Correction on RLNC basis means a more dynamic adjustment of repair packets, less network overhead, faster reaction times and fewer retransmissions required. By eliminating the number of required retransmissions, the available bandwidth is restored quickly, and applications perform as expected, even when the network conditions are suboptimal.

All of this works seamlessly in the background between the CloudGen WAN site devices and the SASE entry points hosted in the Azure region, effectively creating a self-healing cloud on-ramp, even if only a single uplink is deployed.

For organizations that have certain geopolitical requirements or using applications requiring an organization's IP address as the source IP address, every CloudGen WAN site device can serve as a private enforcement node for SWG, NGFWaaS enforcement and entry point to the cloud service for remote endpoints.

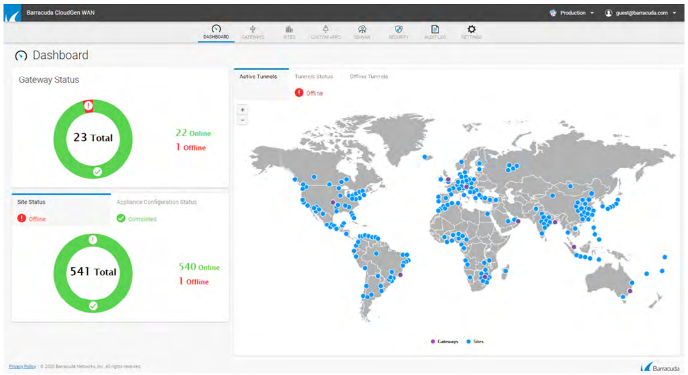


Preferred public-cloud platform of IT business decision makers in the U.S., EMEA, and APAC (Secure SD-WAN: the launch pad into cloud by Vanson Bourne, 2020) (n=750)

The site devices are available in virtual form factor or as easy to deploy hardware unit from small desktop form factor for SOHO or small offices to large 1U office devices up to 10 Gbps SASE throughput per site device. Managed via a cloud console and shipped directly to the branch with zero-touch deployment, setup and onboarding of locations to SASE provided by CloudGen WAN on Azure is a fast and seamless experience.

The SASE Edges in Azure also provide traffic visibility and SWG and NGFWaaS security enforcement for intra-cloud or cloud egress use cases, overcoming the cumbersome deployment of multiple virtual security devices in the cloud or having to deal with Azure Security Groups or Azure Firewall and Azure security partner providers. These solutions are typically more expensive, less integrated and more complicated to use.

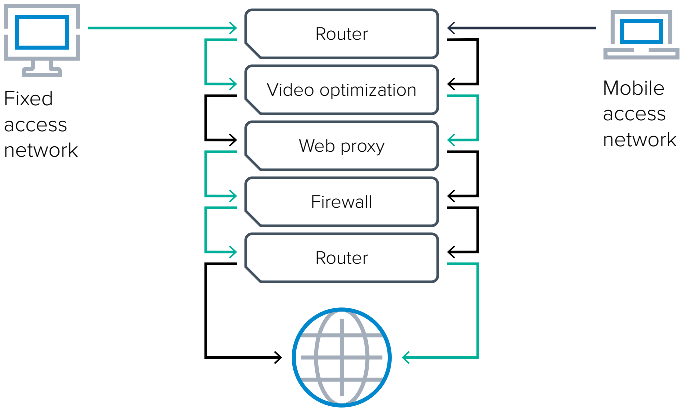
The Service Edge in Azure as well as the private enforcement points on the site devices are controlled by the security policies defined centrally in the CloudGen WAN Management Portal, without the need for the administrator to know where the traffic enters the service.



Dashboard of CloudGen WAN Management Portal

SASE with Barracuda CloudGen WAN is different

Many vendors attempt to provide all SASE core capabilities use a process called "VM service chaining" in the public cloud. This process provides the combined SD-WAN and security functions of SASE by stringing together virtual appliances that are dedicated to a specific subset of functions. The customer receives the SASE service, but Gartner has noted that service chaining will introduce "inconsistent services, poor manageability and high latency" into a SASE solution.



VM service chaining

Barracuda takes a different approach. Barracuda CloudGen WAN for Azure is a cloud-native SASE solution that does not rely on service chaining or multiple service providers. This is a pragmatic implementation of SASE that was jointly developed by Microsoft and Barracuda and is available as a service in the Azure Marketplace. It offers the scalability and automation of Microsoft Azure and the battle-tested security and SD-WAN capabilities of the Barracuda CloudGen Firewall. All of this works along the Microsoft Global Network, which is over 165,000 miles of fiber and subsea cable that connect 61 Azure regions and strategically placed PoPs in edge sites around the world.

> "A cloud-first strategy asks for a different approach on connectivity. We have invested heavily in Microsoft Office 365 adoption across the organization, and traditional connectivity doesn't fit the bill anymore. We need a solution that is focused on delivering application performance, not just 'plain' connectivity. That's why we're moving forward with Barracuda CloudGen WAN."
>
> Leon Sevriens, Program Manager IT at Humankind

Barracuda CloudGen WAN on Microsoft Azure is the only solution that allows the use of the Microsoft Global Network, completely eliminating the need for another third-party cloud or third party network that might lead to potential outages, bottlenecks or regulatory issues.

Direct access to all applications without the complexity of VPN

ZTNA with CloudGen Access

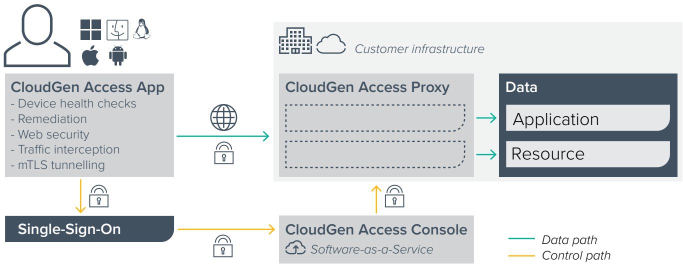
An integral part of SASE is Zero Trust Network Access (ZTNA), which is the new and easy way to connect users to applications directly without the need to use cumbersome VPN technology. In line with the SASE concept, ZTNA with CloudGen Access shifts the perimeter from the network to the device edge as defined by user identity, device health and security posture. The solution continuously verifies that only the right person, with the right device, the right device health status, and the right permissions can access company data or apps.

Zero Trust architecture is a set of guiding principles that rely on the key assumption that the new corporate network is the internet and as such a hostile environment. So, the company network infrastructure is not more secure than any other network and each access must be independently authorized and authenticated.

To ensure security, the enterprise must continuously analyze and assess risks to its internal resources, business apps, and workloads. Zero Trust not only restricts access to resources to only those who must have it, but also goes beyond the concept of role-based access control (RBAC) to implement attribute-based access control (ABAC) and ephemeral trust models. Access is granted only after authenticating the identity and security posture of each access request. To eliminate unauthorized access to data and services and ensure secure access, the focus is on strong authentication, authorization, and granular access controls.

How ZTNA with CloudGen Access works

ZTNA with CloudGen Access relies on three main components: a small lightweight app available for all device types (CloudGen Access App), a proxy on each protected network (CloudGen Access Proxy), and the SASE cloud console (CloudGen Access Console) for management. The CloudGen Access app operates at the network layer at the endpoint devices. When a device starts a connection to a protected resource, the app automatically intercepts it and opens a mTLS (mutually encrypted TLS, meaning the connection is encrypted using both private keys, the one from the endpoint and the one from the Access Proxy) connection with the CloudGen Access Proxy, sending the device and user attributes to CloudGen Access Console which evaluates the policy. The app also queries the device posture and sends the information to the console. The console then checks the attributes and device posture against the predefined policies for the device, user, application combination and allows or denies the connection to the resource. All traffic then flows encrypted from the device -intercepted by the app- to the CloudGen Access Proxy, and then directly to the application.



CloudGen Access environment

When a connection to a resource is denied, the app receives a list of attributes that are not compliant with the policy/policies configured for the resource, together with a list of steps that the user can perform to fix the issue.

For example, an access policy requires users to have the latest software updates installed and prevents access from known hacked Wi-Fi Networks on their devices. CloudGen Access will then deny access to the application. The CloudGen Access app will receive a response from the CloudGen Access Console that includes the reason for the denied access and the steps required to fix it: e.g. “Update iOS version”, together with a URL that links to specific content that shows the user how to do this.

ZTNA with CloudGen Access is different

Application agnostic: Works for any application based on TCP or UDP, not only web apps

No third-party cloud: You own data traffic and decide where it goes, CloudGen Access do not require funneling of any data traffic outside of your infrastructure or your preferred cloud provider.

Designed for the cloud: Deploys in microservices, infrastructure-as-code template (Kubernetes, Docker, CloudFormation). CloudGen Access is the only solution that allows complete automation of ZTNA access to microservices managed by Kubernetes clusters (Automatic tear down and re-init).

Workload-2-workload: CloudGen Access Proxy as well as the endpoint application are available for docker so CloudGen Access can provide ZTNA protection of intra cloud or workload to workload traffic setups. This setup can be automated via API and allows workload-2-workload ZTNA across regions, data centers and even across public cloud types.

Fast: Fast setup and quick self-deployment for the end users from any app store. Rollout of the ZTNA app at the client level does not require an MDM or Admin interaction.

Available everywhere: The complete set of functions is available for all endpoint types: Windows, macOS, Android, iOS, iPAD OS, Chromebook, Linus, Docker.

Intuitive: to use for the end user: The CloudGen Access endpoint app is intuitive to use and provides the common look and feel of today’s apps on mobile devices.

The easy way to start with SASE

Gartner recommends starting the journey to SASE by looking into deploying ZTNA as a high priority:

> Set a three- to five-year goal to replace 90% of legacy network-level VPN access with zero trust network access over the next five years.
>
> Adopt cloud-based ZTNA to augment legacy VPN access for higher-risk use cases such as:
>
> ■ Contractor and third-party access
>
> ■ Unmanaged device access
>
> ■ Cloud administrator and developer access

Source: Gartner 2021 Strategic Roadmap for SASE Convergence - available for download here.

Summary

Barracuda CloudGen WAN is a cloud-native SASE solution in Microsoft Azure. CloudGen WAN enables companies to deploy SASE the way they prefer, running SD-WAN, security, networking and Zero Trust Access using the Microsoft Global Network as the enterprise backbone. All security and connectivity functions are centrally managed by a cloud console. All heavy-lifting security functions like Advanced Threat Protection are done by the Barracuda ATP Cloud service.

Barracuda CloudGen Access enables Zero Trust Access to all of your apps and data from any device and any location. The software-defined perimeter reduces over-privileged access and risks of third-party access corporate applications and cloud workloads. Built for modern cloud infrastructures, Barracuda CloudGen Access enables you to provide secure remote access without creating additional attack surfaces.

If needed, customer premises equipment provides Secure SD-WAN connectivity to the SASE service and even functions as a cloud edge entry point. Deployment of the optional site devices is truly zero-touch and does not require technical personnel on site.

> "By 2022, 80% of new digital business applications opened up to ecosystem partners will be accessed through Zero Trust Network Access (ZTNA)."
>
> Gartner, 2019

Barracuda
CloudGen Access™

Barracuda CloudGen Access is a cloud native Zero Trust Network Access (ZTNA) solution that provides anytime and anywhere secure access to any application and workload from any device and location. Barracuda CloudGen Access is your onramp to SASE to deliver seamless, consistent and secure application access regardless where hosted.

Learn more

> "Traditional data centers are going away. More than ten percent of organizations have already shut theirs down, and Gartner has predicted that will rise to 80 percent by 2025."
>
> Gartner, 2020

Barracuda
CloudGen WAN™

CloudGen WAN is the SASE solution for Azure by Barracuda Networks. Typical SASE solutions just replace on premises appliances by moving security and networking into their cloud. CloudGen WAN is the only SASE service delivered natively by Azure, tightly integrated with its services and using the Microsoft Global Network as its WAN backbone.

Learn more

Barracuda®
Your journey, secured.