SONICWALL

Braxton-Grant TECHNOLOGIES

SonicWall Cloud Edge Secure Access

Deploy Zero Trust Security in minutes

SonicWall Cloud Edge Secure Access enables a simple Network-as-a-Service (NaaS) for site-to-site and hybrid cloud connectivity to AWS, Azure, Google Cloud and more. By combining Zero-Trust and Least-Privilege security, the solution enables organizations to offer remote-work flexibility while still protecting high-value business assets.

With Least-Privilege Access, users and devices are permitted access to what's necessary and nothing more, similar to the concept of a "need to know basis." By limiting exposure to sensitive areas of the network, organizations can prevent threats from moving laterally, thereby securing their resources without sacrificing operational flexibility.

The SonicWall Cloud Edge Secure Access solution applies Zero-Trust Security based on four core security actions:

- **Verify** all user and device credentials, even for internal traffic
- **Contextualize** the request to ensure authenticity and compliance with corporate guidelines
- **Micro-segment** network access to stop threats from moving laterally
- **Grant** access to the requested applications and nothing more

SonicWall Cloud Edge Secure Access is built around the modern and secure-by-design Software-Defined Perimeter (SDP) architecture. SDP decouples the controller, which authenticates users and devices, from the gateways that act as trust brokers. By distributing the gateways close to the end-user locations, Cloud Edge Secure Access can scale rapidly as needed and maintain high performance and deliver the best cloud experience possible.

This separation of functions also enables Cloud Edge Secure Access to stop common cyberthreats, such as DDoS, public Wi-Fi hijacking, SYN flood and Slowloris.

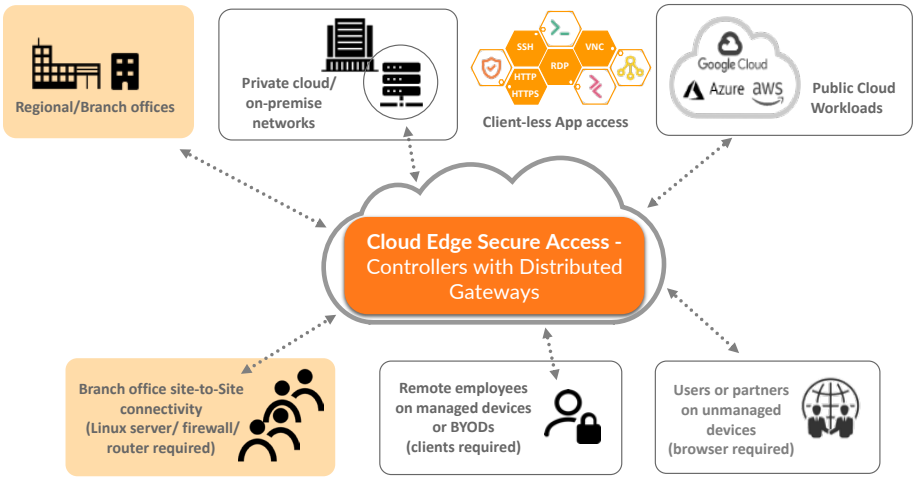

Figure 1 – SonicWall Cloud Edge Secure Access

Benefits:

- Security solution for distributed enterprises and remote workforce
- Instant, secure access to sites and resources on hybrid clouds
- Zero-Trust/Least-Privilege policies segmentable by network, application, user and device profiles
- Built-in micro-segmentation to prevent unauthorized lateral movements
- Scales from 50 users to thousands of users
- Configurable in 15 minutes by IT manager
- Can be deployed by end user in five minutes
- No usage or bandwidth limit
- Security for public Wi-Fi use
- High-performance WireGuard encryption
- Cloud Identity Provider integration
- Modern SSO and MFA Integration
- Stops DDoS, Slowloris, SYN flood
- Multi-tenancy for MSSPs
- Complete monitoring and reporting for compliance audits
- Dedicated per-customer cloud gateways and IP addresses
- Available in USA, Europe, Middle East and Asia

The Evolution of Traditional VPN to Zero-Trust Security

Today's employees want the flexibility to work from anywhere — and today's organizations want to take advantage of the cost savings and operational efficiencies offered by the cloud.

But traditional VPN solutions weren't built for this reality. Deploying one can take days or even weeks. Supply availability issues mean they may or may not be available, and once you have one in place, it can be difficult to schedule downtime.

Worse, they can offer a back door into your network, as any successful login grants broad network access and allows for lateral movement within the network subnet.

And because the user traffic loops through the on-premise VPN concentrator instead of going directly to the cloud, VPN creates latency that decreases efficiency and degrades users' cloud experience.

Gartner predicts that by 2023, 60% of enterprises will phase out most of their remote access virtual private networks (VPNs) in favor of ZTNA.

With Cloud Edge Secure Access, SonicWall offers a ZTNA solution that overcomes these problems while offering a host of other benefits. At the core of SonicWall Cloud Edge Secure Access are three essential capabilities:

- Least-Privilege access to protect corporate assets
- Fast self-service deployment
- Cloud-direct, reliable access from anywhere

Primary Use Cases

Rapid Deployment and Self-Service Onboarding

- **Faster deployment –** An IT manager can sign up, create a gateway, and configure granular policies based on network and user context — all in less than 15 minutes.
- **Faster user onboarding –** An end user can choose whether to connect via their mobile device or desktop client app, or bypass client installation altogether when using a public computer, provided a browser is available. With the self-service deployment model, onboarding can be completed in 5 minutes.
- **Reliable access to hybrid cloud –** Once they're up and running, users will enjoy fast, easy and secure access to on-prem and public cloud resources.

Work-from-Anywhere Protection — From Trusted Areas to Public Hotspots

- **Automatic Wi-Fi security –** Cloud Edge Secure Access for Windows and mac OS proactively monitors the environment, automatically activating a secure access connection in public hotspots. This extra layer of protection stops Wi-Fi intercepts, which are increasingly common and can result in data thefts and compliance violation.
- **Kill switch –** When a secure access connection is interrupted, the device's internet connection is instantly halted — disrupting potential cyber breaches and preventing any data from leaving the device.
- **Trusted Wi-Fi networks –** When an SSID is specified as "trusted," the automatic Wi-Fi security feature will not activate.
- **Always-on VPN/applications –** This convenient feature automatically reconnects to an application or set of applications without requiring users to login or authenticate again.

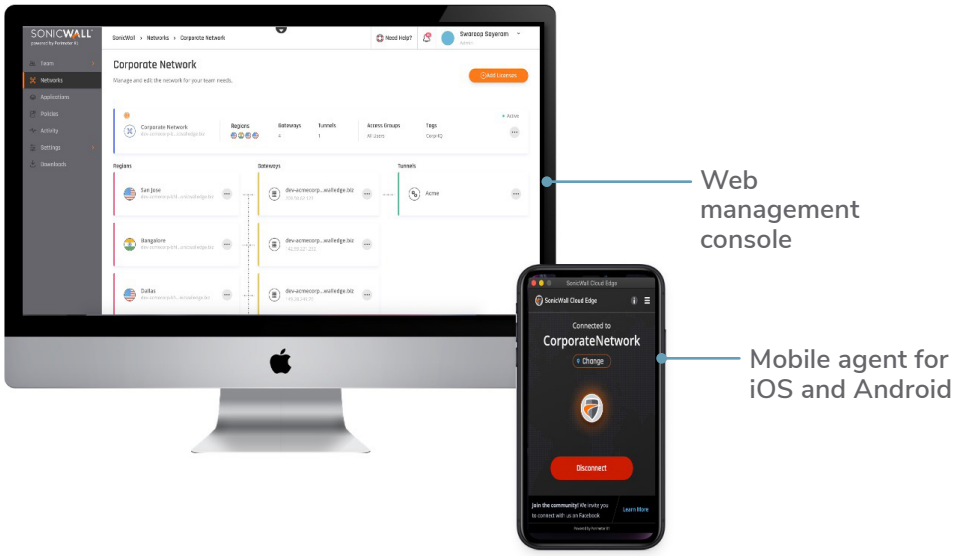

Figure 2 – SonicWall Cloud Edge Secure Access Management Console and Mobile Agent Application for Apple iOS

Zero-Trust Application Access

Cloud Edge Secure Access offers organizations the ability to enable and empower a remote workforce while simultaneously protecting corporate resources.

With Zero-Trust policies, external users with a proper set of context can securely access a host of remote desktop and web applications without exposing the corporate network to cyberthreats.

- **Least-Privilege Access Control –** Organizations can control interactions with resources based on relevant attributes, including user and group identity and the sensitivity of the data being accessed.
- **Context-driven access –** The solution ensures user-centric and policy-based access to on-premise and cloud-hosted resources.
- **Integration with leading cloud-based identity management providers –** Organizations can extend the service life of legacy on-premise assets or migrate to the modern, cloud-based identity management services from providers, such as Azure AD, Google Cloud Identity and Okta.
- **Micro-segmentation –** By precisely segmenting all incoming traffic, Cloud Edge Secure Access prevents malware or unauthorized users from moving laterally, shrinking the attack surface and reducing overall exposure to cyberthreats.
- **Federated Single Sign-On and Multi-Factor Authentication –** This combination provides users a single portal for authenticating into a hybrid IT environment, creating a consistent and seamless experience.
- **Optimized for compliance and reporting –** Every Zero-Trust Access activity is fully monitored and recorded for future audits.

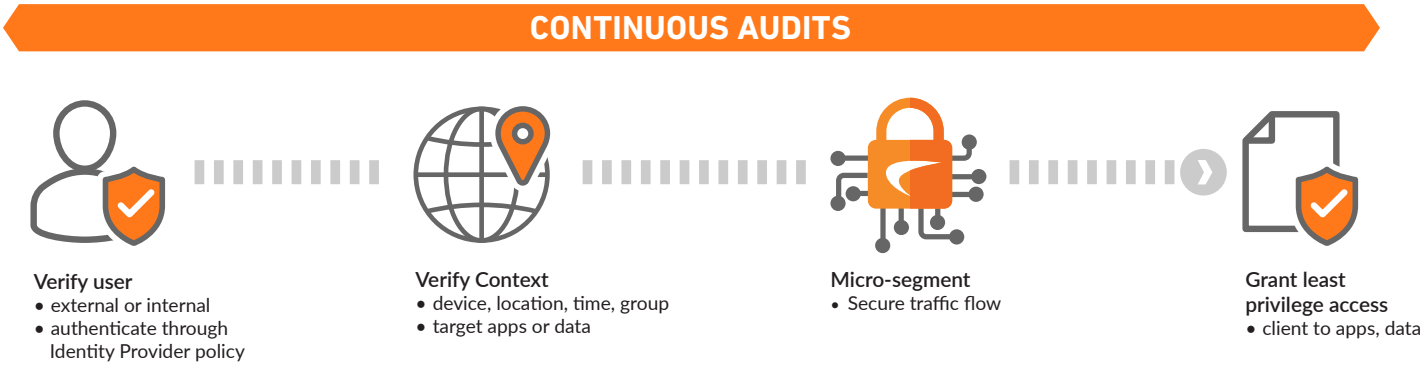

Figure 3 – SonicWall Cloud Edge Secure Access ZTNA process

Site-to-Site Interconnectivity or Network-as-a-Service (NaaS)

Cloud Edge Secure Access offers the choice of site-to-site connectivity service or Network-as-a-Service (NaaS), which IT managers can use to quickly onboard branch offices in geographically dispersed locations. NaaS also allows you to quickly and securely connect mobile kiosks, retail stores and sales points to cloud-hosted resources without needing to rely on costly MPLS.

- **Site-to-site or site-to-cloud interconnect service –** The solution easily connects to popular cloud environments, including AWS, Azure and Google Cloud — or can be used to create a secure communication link between networks located at different sites.
- **Multi-regional deployment –** Administrators can deploy dedicated Cloud Edge gateways in different locations to deliver optimal speed and performance to international branches and employees.
- **High-performance global backbone –** SonicWall Cloud Edge service is available globally. The infrastructure offers minimal latency by distributing gateways close to the customer locations and load-balancing traffic across servers.
- **State-of-the-Art WireGuard tunnel –** An IT manager can leverage any branch router or firewall with IPsec to connect to the nearest Cloud Edge gateway. *SonicWall recommends the WireGuard tunnel, which can deliver much faster performance. This deployment requires a branch Linux server to run the WireGuard tunnel service to the nearest gateway.*
- **Network auditing and monitoring –** SonicWall Cloud Edge offers a comprehensive and easily accessible overview of your network's health, activity and security — including visibility into group and server creation, team member authentication, password changes, and more.

Specifications

Category	Feature	Benefits
Scale & performance	Users	50 to thousands
	Performance	1Gbps per customer gateway; Horizontal cloud scaling with more gateways
Cloud platform	Cloud management platform	Cloud management platform to easily create your organization's network. Included on-premise and on the cloud
	Fast and easy network deployment	Automatically deploy your network in less than 15 minutes
	Availability and Uptime	Automatically managed by the service. Current Cloud Edge service status is provided at https://status.sonicwall.com/
	Load balancing	Provided by shared/dedicated gateways across 30+ global POPs, hosted and managed by SonicWall
	Site-to-Site Interconnectivity	Connectivity between two sites (onsite, offsite or cloud-based). Supports IPsec and WireGuard
	Custom DNS	In order to use your internal DNS servers, once defining a tunnel you can also define a custom DNS server instead of using the default DNS
	Clientless application access	Zero Trust application access to HTTP, HTTPS, RDP, VNC, SSH
	Client-based access	Available for Windows, Mac, iOS and Android platforms
	Apps & environment	Best suited for hybrid environments and cloud workloads
Zero Trust capabilities	Always-on Applications	Always-on applications provides secure access to the internet when connecting to a non-trusted network, which protects you from security threats
	Policy-based segmentation	Policies applied per user and application
	Granular Access Control Policies	Based on user, application, Geo IP, geo-location (country), browser type, OS, date and time
	Split tunneling	Enables you to decide which subnet your traffic will go through
	Kill Switch	To disrupt a potential cyber breach, when a secure access connection is interrupted, the device internet connection will be instantly halted to prevent any data from leaving the device.
	Automatic Wi-Fi security	Our patented feature automatically protects employee's devices when they connect to unsecured public Wi-Fi
	DNS Filtering	Block users in your network from accessing certain websites, site categories, and IP addresses with an internet browser
Authentication	Single sign-on capabilities	Implement a unified login via Single Sign-On providers such as Okta, G Suite, Azure AD and Active Directory LDAP
	Two-factor authentication	Prevent remote attacks with built-in SMS, DUO Security and Google Authenticator 2FA integration
Monitoring, Logging and Support	24X7 support	Fully managed cloud solution with support included
	Activity audits & reports	Monitor logins, gateway deployments and app connections
	SIEM integration	Capture, retain, deliver of security information and events in real-time to all SIEM applications, including easy click-through integration with Splunk
	Cloud service status	Check https://www.sonicwall.com/support
Interoperability	Enterprise Firewall	SonicWall, Check Point, Fortinet, Palo Alto Networks, WatchGuard, Sophos, Xyxel, UniFi, pfSense, Cisco and Untangle
Custom Integrations	API available	Our comprehensive REST-based API enables quick-and-easy integration with third-party management, automation and orchestration tools, ensuring protection for newly provisioned or relocated virtualized applications
Compliance	ISO 27001 & 27002, SOC-2 type 2	SOC 2 type 2 compliant cloud infrastructure
Ordering	Subscription	Contact your MSSP, reseller and distributors to subscribe to Cloud Edge Secure Access subscription

About SonicWall

SonicWall delivers Boundless Cybersecurity for the hyper-distributed era and a work reality where everyone is remote, mobile and unsecure. By knowing the unknown, providing real-time visibility and enabling breakthrough economics, SonicWall closes the cybersecurity business gap for enterprises, governments and SMBs worldwide. For more information, visit www.sonicwall.com.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Refer to our website for additional information.
www.sonicwall.com

Datasheet-CloudEdge-US-VG-3813

SONICWALL®