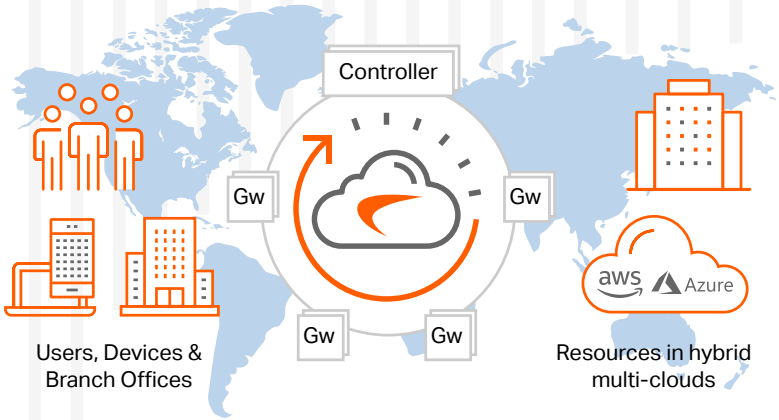
SONICWALL

Cloud Edge Secure Access

Deploy Zero-Trust Network Access at Global Scale 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. It combines Zero-Trust, Least-Privilege security and software-defined micro-segmentation to permit users and devices to access only what's necessary and nothing more, similar to the concept of a "need to know basis."

Now, organizations can offer remote-work flexibility, preserve operational flexibility and at the same time, protect high-value assets from costly security breaches.



HIGHLIGHTS

- Zero-Trust with software-defined micro-segmentation policies effectively prevent breach from spreading.
- Supports Single Sign-On and Multi-Factor Authentication using LDAP, Okta, Google, and Azure Identity Provider services.
- Network Traffic Control (NTC) is a stateful firewall-as-a-service (FwaaS) that provides policy-based protection by defining who can access what resource and from where.
- Device Posture Check (DPC) grants network access only to authenticated and compliant devices.
- Client apps are available for macOS, Win10, Android and iOS operating systems.
- Supports client-less Remote Desktop access using RDP, VNC, SSH and HTTP/ HTTPS for web access with any public devices.
- Provides better user experience with the fast and modern WireGuard secure tunnels.
- Always-on VPN emulates in-office experience and maintains strong security posture in public hotspots.
- Supports an easy drag-drop policy configuration interface to save time, and a dashboard to simplify compliance audits.
- Network monitoring provides a comprehensive overview of traffic pattern, and security postures of users, groups and servers.

Feature Preview. View full Feature Summary »

10–1,000s	5-15 min.	30+ PoPs
Scale of users	Deployment time	In USA, Europe, Middle East and Asia

Zero-Trust Network Access applies explicit trust approach that limits exposure to sensitive areas of the network to safeguard business assets

www.sonicwall.com/cloud-edge

DATASHEET

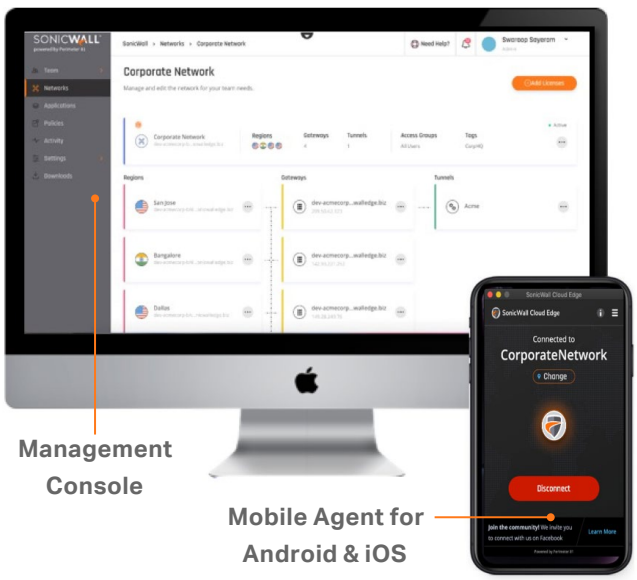
Traditional VPN solutions are not built for the cloud era. Some of the inherent problems include implicit trust allowing threats to move laterally inside the network, often long-lead deployment time, and increased cloud latency due to traffic hair-pinning, which impacts user quality of experience.

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

Infrastructure is Built for Rapid Scale and Global Deployment

SonicWall Cloud Edge Secure Access is built around Software-Defined Perimeter (SDP), an advanced and cloud-native architecture, to deliver 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.



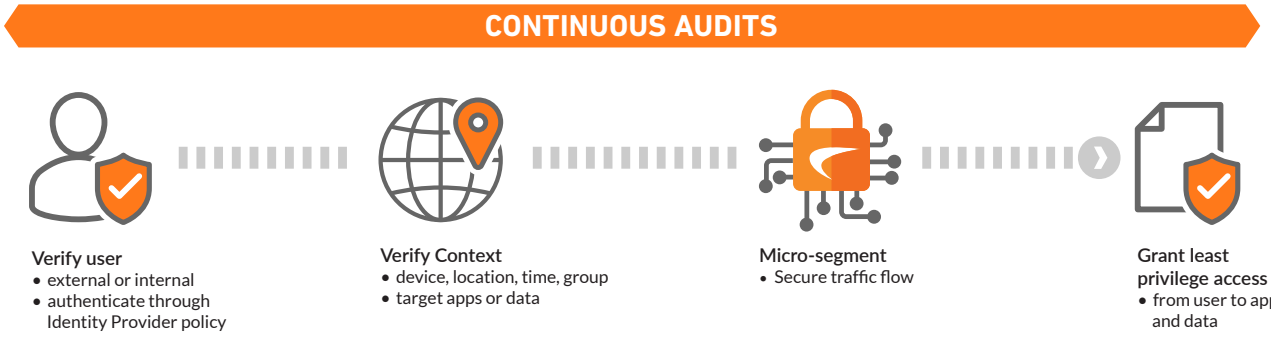
SDP is also secure by design because it decouples the controller, which authenticates users and devices, from the gateways that act as trust brokers. By distributing the gateways close to the end-user locations, Cloud Edge Secure Access can scale rapidly as needed, maintain high-performance and deliver 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.

Software-Defined Micro-Perimeter Security That Follows Users

Today's employees want the flexibility to work from anywhere — and organizations want to take advantage of the cost savings and operational efficiencies offered by the cloud. In this new inverted reality, where everything is outside of centralized locations and beyond physical firewall protection, there is a need to complement the current on-premises service delivery model with an agile follow-the-user security model.

With the SonicWall Cloud Edge Secure Access, the perimeter is software-defined, meaning each micro-perimeter segment encapsulates a particular type of traffic flow, defined by access policies. The segment starts with the user and extends to specific networks or services or assets anywhere in the cloud — a much more versatile approach.



Zero-Trust Network Access

Trust Nothing and Verify Everything

Zero-Trust policies allow external users with a proper set of contexts to securely access a host of network resources using the supports of:

- **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.
- **Integration with leading cloud-based identity management providers** – Organizations can extend the service life of legacy on-premises assets, like LDAP, or migrate to the modern, cloud-based identity management services from providers, such as Azure AD, Google Cloud Identity and Okta.
- **Context-driven access with Device Posture Check (DPC)** – grants network access only to compliant and authorized devices that pass OS integrity and malware-free environment verifications to ensure no malware slips into the infrastructure.
- **Software-defined micro-segmentation** – Network Traffic Control (NTC) precisely segments all incoming traffic to prevent malware or unauthorized users from compromising network resources and sensitive data.
- **Least-Privilege Access Control** – Organizations can control user interactions with resources based on relevant attributes, including user and group identity and the sensitivity of the data being accessed.

Work-from-Anywhere Securely

From Trusted Areas to Public Hotspots

- **Automatic Wi-Fi security** – Cloud Edge Secure Access for Windows and mac OS proactively monitors the environment, and automatically activate 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.

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 secure 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.

Native multi-tenancy support with per-customer portal and tiered subscription services are designed to help MSSPs build profitable business.

Feature summary

Scale and performance

- 10 to thousands of users
- 1Gbps per customer gateway
- Horizontal cloud scaling with more gateways

Cloud platform capabilities

- Cloud service status: https://www.sonicwall.com/support
- Cloud management included
- Infrastructure managed by SonicWall
- Services managed by MSSPs and customers
- Dedicated per-customer cloud gateways and IP addresses
- Load-balancing across redundant gateways included
- Choice of IPsec and WireGuard connectivity between two sites
- Choice of default or your internal DNS server

Zero-Trust Security capabilities

- Clientless access using HTTP, HTTPS, RDP, VNC, SSH
- Client app available for Windows, Mac, iOS and Android platforms
- Devices and context verifications (with DPC, time-based access, continuous user and device monitorings)
- Least-Access Privilege Policy enforcement (with Access Control Policies)
- Software-defined micro-segmentation (with NTC)
- Policy-based segmentation applied per group, network, user, application, services, device
- Control and micro-segment network traffic flow between users, groups and services based on customizable rules
- Granular Access Control Policies based on user, application, Geo IP, geo-location (country), browser type, OS, date and time

Public Hotspot Security

- Split tunneling enables local breakout of subnet traffic
- Kill Switch disrupts a potential cyber breach by halting the device internet connection to prevent any data exfiltration.
- Automatic Wi-Fi security automatically protects employee's devices when connecting to unsecured public Wi-Fi
- DNS Filtering blocks access to certain websites, site categories, and IP addresses

Authentication

- Single sign-on support through providers such as Okta, G Suite, Azure AD and Active Directory LDAP
- Two-factor authentication using SMS, DUO Security and Google Authenticator 2FA
- Verify security and compliance of the connecting devices even before accessing the network using Device Posture Check

Enterprise Firewall and Router Interoperability

- SonicWall, Check Point, Fortinet, Palo Alto Networks, WatchGuard, Sophos, Xyxel, UniFi, pfSense, Cisco and Untangle

Monitoring, Logging and Support

- Fully managed cloud solution with 24*7 support included
- Activity audits & reports on logins, gateway deployments, device and app connections
- SIEM integration including capture, retention, delivery of security information and events in real-time to all SIEM applications
- Automated list of devices that connect to your network and associated logs.
- Click-through integration with Splunk

Compliance

- ISO 27001 & 27002, SOC-2 type 2

SONICWALL

Zero-Trust Network Access solution for remote workforce, distributed enterprises and MSSPs

www.sonicwall.com/products/cloud-edge-secure-access

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 or follow us on Twitter, LinkedIn, Facebook and Instagram.

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

SONICWALL

Datasheet-CloudEdge-US-COG-5178