DATASHEET

Cloud Secure Edge

Remote access, better security.

SonicWall Cloud Secure Edge™ is a modern, cloud-native Security Service Edge (SSE) solution that addresses the limitations of legacy network appliances with a unified, scalable approach to secure access. It empowers organizations that consist of a variety of users (employees, contractors, third parties, etc.) to seamlessly and securely connect to both private and internet resources from any device or location.

By consolidating key networking and security functions like remote access VPN, web proxy, and firewalls into a single, cloud-delivered platform, Cloud Secure Edge strengthens your organization's security posture and enables you to adopt a proactive security strategy, all while delivering a disruption-free end-user experience.

Note: Customers already using SonicWall Gen 7 and newer Firewalls can connect to Cloud Secure Edge out of the box and manage access policies easily from a unified dashboard.

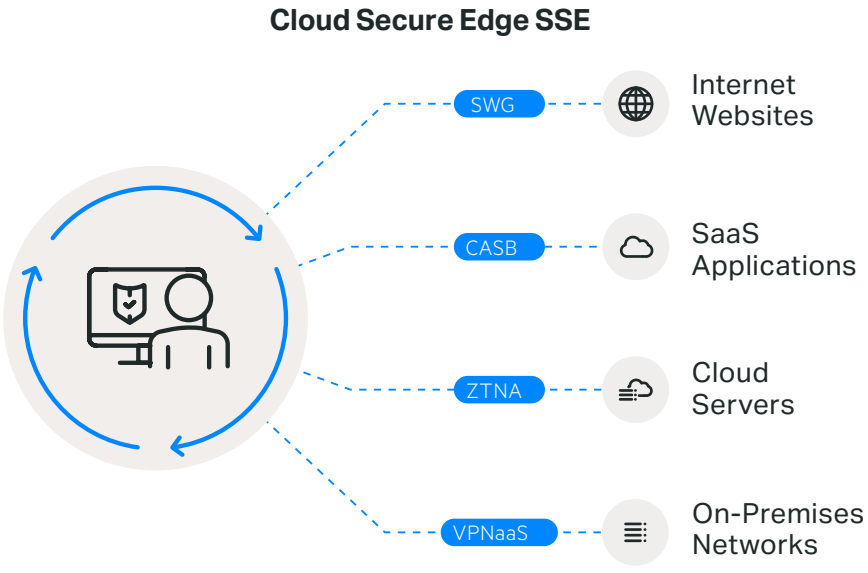

Figure 1: SonicWall Cloud Secure Edge protecting access to any resource from any device

SONICWALL®

Why SonicWall Cloud Secure Edge?

Easy to Manage and Deploy
Cloud Secure Edge can be standalone or added to your existing SonicWall Gen 7 or newer Firewalls as a monthly subscription. It is ideal for MSPs and DIY organizations with overstretched resources looking for low TCO and fast ROI. Upon logging into Cloud Secure Edge for the first time, admins can follow a guided 3-step wizard to establish their first secure VPNaaS tunnel, speeding up time-to-value.

Protect Against Threats
Cloud Secure Edge includes zero trust security controls that are needed for hybrid and remote workforces that need access to the sensitive private and internet assets required to do their jobs from anywhere. It employs a unique technology based on device and identity-centric trust scoring and short-lived cryptography to deliver industry-leading security with excellent user experience.

Performance With Privacy
Cloud Secure Edge was built from the ground-up to deliver high performance while ensuring privacy. The admin is in full control of their data while ensuring users get the most natural and efficient connection possible for maximum productivity, data protection and privacy.

Common Use Cases

Modernize VPN/FW with ZTNA
Rather than rely on coarse tools like firewalls and legacy VPNs to protect company resources, Cloud Secure Edge enables least-privilege access to specific applications and servers based on the combined real-time contextual factors of user and device trust and resource sensitivity.

Cloud Secure Edge is cloud based and can be applied independently or in combination with pre-existing security infrastructures.

Protect Against Internet Threats and Credential Compromise
SonicWall has deployed high-performance global edge POPs to ensure the most efficient and direct routing while applying consistent enforcement controls to protect against every type of attack or risky exposure. This provides simple and effective protection against phishing attacks and malicious websites, while also applying content filtering as desired, and device security is verified up front before access is granted – the way it should be.

Secure High-Risk Users (3rd Parties / BYOD / Contractors)
Provide third-parties easy, secure access to only the specific resources they need without over-provisioning. Cloud Secure Edge ensures access based not only on the security posture of the user and device, but also on their role and what they are authorized to view. Management is simple with groups and roles that can be pre-identified and applied as necessary from one central console. No need to patch or configure hardware—ever.

Licensing

Cloud Secure Edge is available for purchase as Secure Private Access (to resources on internal networks) and Secure Internet Access (to resources on the public Internet).

1. Se cure Private Access provides two core capabilities:
   - Tunnel-based ZTNA (also called Cloud VPN or VPNaaS): Secure network access to specific network segments
   - Proxy-based ZTNA: Secure access to private resources such as internal HTTP applications and TCP services.

2. Se cure Internet Access provides these core capabilities:
   - Cloud Access Security Broker (CASB): Enforcement device trust policies to access SaaS applications.
   - Secure Web Gateway (SWG): Web content filtering to block malware and other threats hidden in encrypted web traffic.

Secure Private Access (SPA) and Secure Internet Access (SIA) SKUs are both available in two tiers: Basic and Advanced. Licenses are sold per-user.

SONICWALL®

Common Capabilities

High Performance Data Plane
Dynamic edge architecture for fast and reliable connections to users around the world

Native Support for All Client Operating Systems
Desktop (Windows, macOS, Linux) and mobile (iOS, Android, ChromeOS)

Cloud Management Interface
For IT and security admins to configure zero trust connectivity

Trust Scoring
Quantify the level of trust and risk associated with your users and devices

Actionable Visibility
A complete view into user/device and application/resource risk

Continuous Policy Enforcement
Based on resource sensitivity, regardless of user's location

Integrations
Integrates with existing tools (IDP, EDR, MDM, SIEM)

SonicWall Firewall Connector
Out of box integration with Gen 7 and newer Firewalls in Global Mode on 7.1.2+

Multi-tenant Management
Cloud-based policies for multi-tenant management

User and Devices

Single Sign-On
Use corporate SSO with just-in-time (JIT) user creation

Posture Management
Analyze the posture of a device, such as firewall, disk encryption, screen lock, OS version, etc.

Trust Profiles
Customize factors and policy effects based on groups of users and devices

Custom Remediation
Configure device posture remediation instructions, such as messaging and links, shown to your end users

Visibility and Compliance

Real-time Event Stream
Monitor a real-time stream of user and device activity

Device Posture Reporting
Track all devices—managed and unmanaged—accessing corporate resources, as well as their security posture

Admin Activity Reporting
Log all admin activity in the Cloud Command Center

Operations and Automation

RESTful API
RESTful endpoint to configure Cloud Secure Edge objects in the Control Plane

API Clients—Pybanyan, Terraform
Python library and terraform for automation and management

Zero Touch Device Registration
Roll out the Cloud Secure Edge app to your device fleet without requiring any end-user interaction

SONICWALL

	Secure Private Access		Secure Internet Access	
FEATURE	BASIC	ADVANCED	BASIC	ADVANCED
Secure Network Access				
ZTNA Tunnel (VPNaaS) to enable access to specific networks	●	●		
ZTNA Proxy to securely connect to internal HTTP applications and TCP services		●		
Private Networks (RFC-1918 ranges) and domains (internal DNS servers)	●	●		
Split Tunneling to specific subnets and domains (private or public)	●	●		
Full Tunneling for all traffic using Private Edge		●		
Network / Layer 4 polices based on CIDRs and FQDNs	●	●		
Secure Access to Private Resources				
Internal Websites access using browser-only OpenID Connect flows		●		
SSH to Linux servers		●		
RDP to Windows machines		●		
Native clients to access database servers such as PostgreSQL and MySQL		●		
Kubernetes client to access cluster		●		
SSH Certificate Authentication, Authorize Principals, and audit logging		●		
Layer 7 policies to access APIs, webpages		●		
Internet Threat Protection				
DNS Layer Security blocking domains with malware, phishing, botnet, and other risks			●	●
Content categorization			●	●
Custom blocking			●	●
SaaS Application Security				
Cloud Access Security Broker (CASB) to enforce device trust policies for SaaS applications				●
Visibility into Cloud Applications / Shadow IT				●
IP Allowlisting for Cloud Applications through SonicWall Edge	●	●		
Device Trust for Okta				●
Device Trust for Azure AD				●
Device Trust for other IDPs such as OneLogin, Jumpcloud				●
Web Content Filtering Service				
Secure Web Gateway (SWG) | Content Filtering via DNS			●	●
Secure Web Gateway (SWG) | Threat Filtering via DNS			●	●
Secure Web Gateway (SWG) | Risk-Based URL Filtering				●
Secure Web Gateway (SWG) | Geo-IP Filtering				●
Users and Devices				
Passwordless Authentication via IDP Federation		●		●
Policy-enforced access from Unregistered Devices with a trusted device certificate		●		●
Clientless access		●		●
Service Accounts (API tokens for programmatic access such as scripting and automation through the Data Plane)		●		
SCIM integration to manage user assignments		●		●
EDR integrations (e.g. CrowdStrike, SentinelOne, Microsoft Defender)		●		●
MDM/UEM Integrations (e.g. JAMF, Kandji, Jumpcloud, Intune, Workspace One)		●		●
Microsoft API Integration	●	●	●	●

SONICWALL®

Visibility and Compliance				
SIEM Integration (eg. Splunk, Elastic, Sumo Logic)	●			●
Private Network Discovery (non-approved applications accessed by user or devices)	●			n/a
IaaS Resource Discovery	●			n/a
SaaS Application Discovery (Beta)	n/a			●
Operations and Automation				
Private Edge Deployment: Host SonicWall's identity-aware gateway in your own infrastructure		●	n/a	n/a
Services and Support				
24x7 Support	●	●	●	●
Premier Support		add-on		add-on
Remote Implementation Services		add-on		add-on

Summary

SonicWall Cloud Secure Edge is a transformative cloud-delivered SSE solution that is more than just a replacement for outdated, legacy perimeter appliances. It's a scalable, modern approach to securing connectivity between users, the internet, and internal resources. By continuously verifying users, devices, applications, and resources, it delivers true Zero Trust access for employees and third parties, regardless of location.

Easily deployed through SonicWall firewalls, Cloud Secure Edge also supports multi-tenant management which is tailored to organizations of all sizes and the MSPs that support them. With Cloud Secure Edge, organizations can effectively address security gaps, deliver superior end user experience, and adopt a proactive, risk-limiting approach to networking and security. Ready to elevate and secure access across your organization? Speak to our team today or request a demo.

Contact your account executive if you want to add Cloud Secure Edge to your existing SonicWall Gen 7 Firewalls.

Authorized Distributor :

SecureOne
Optimize with SECURITY

HQ Office (KL)
SecureOne Distribution Sdn Bhd
200801027033 (828358 - X)
No.7, Jalan 1/109E, Desa Business Park,
Taman Desa, Jalan Kelang Lama,
58100 Kuala Lumpur, Malaysia.

Tel: +6(03) 7984 6086 Fax: +6(03) 7984 6032
Email: sales@secureone.com.my

Northern Office
SecureOne Distribution (Northern) Sdn Bhd
201201003647 (977172 - H)
1A-2-02 @ One Precint (1160),
Lengkok Mayang Pasir,
11950 Bayan Baru, Penang, Malaysia.

Tel: +6(04) 619 2692 Fax: +6(04) 619 2699
Email: northern@secureone.com.my