Cloud Secure Edge

Remote Access, Better Security

SonicWall Cloud Secure Edge™ is a highly effective and easily adopted Security Service Edge (SSE) solution, enabling your workforce to securely access any resource from any device. It delivers simple, secure, zero trust access to private and internet resources for all your employees and third parties, regardless of their network location. It combines the functionality of multiple traditional network appliances – remote access VPN, web proxy, firewall and more – into a unified cloud-delivered solution, improving the security posture and user experience for the entire workforce.

Note: Customers with SonicWall Gen 7 Firewalls already deployed can connect them to Cloud Secure Edge out-of-box and manage access policies via a unified dashboard.

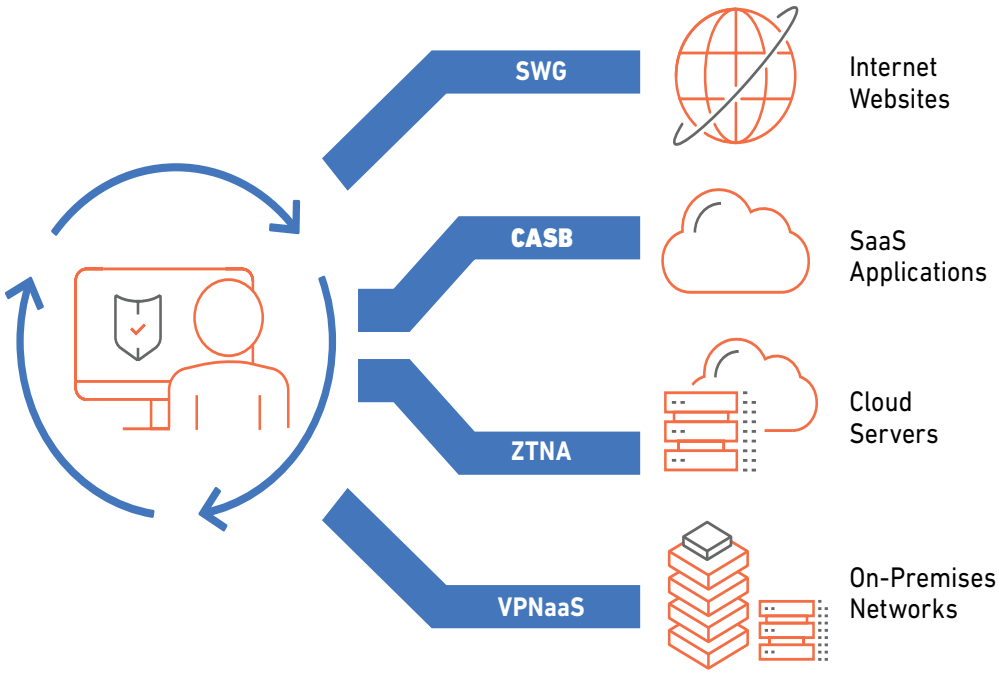

Figure 1: SonicWall Cloud Secure Edge protecting access to any resource from any device

DATASHEET

Why SonicWall Cloud Secure Edge?

EASY TO DEPLOY AND MANAGE

Cloud Secure Edge can be standalone or added to your existing SonicWall Gen 7 Firewalls as a monthly subscription. It is ideal for MSPs and DIY organizations with overstretched resources looking for low TCO and fast ROI.

PROTECT AGAINST MODERN 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.

It 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 / M&A)

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. Secure 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. Secure Internet Access provides three core capabilities:
   - DNS-Layer Security (DNS): Domain-level threat protection blocking malicious domains and enforcing acceptable use policies.
   - 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.

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 Gen7 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 CSE objects in the Control Plane

API Clients – pybanyan, terraform

Python library and terraform for automation and management

Zero Touch Device Registration

Roll out the CSE app to your device fleet without requiring any end-user interaction

	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		✓		
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			✓	✓
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)		✓		✓

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		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 Security Service Edge solution combining industry-leading TCO with enterprise-grade zero trust security. It delivers simple, secure zero trust access to private and internet resources for employees and third parties, regardless of their physical location or device. Cloud Secure Edge combines the functionality of multiple traditional network appliances - remote access VPN, web proxy, firewall, etc - into a unified multi-tenant cloud-delivered solution that is simple to deploy and easy to manage for organizations of all sizes, maximizing ROI for you and your customers.

Want to learn more about SonicWall Cloud Secure Edge?

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

About SonicWall

SonicWall is a cybersecurity forerunner with more than 30 years of expertise and a relentless focus on its partners. With the ability to build, scale and manage security across the cloud, hybrid and traditional environments in real time, SonicWall can quickly and economically provide purpose-built security solutions to any organization around the world. Based on data from its own threat research center, SonicWall delivers seamless protection against the most evasive cyberattacks and supplies actionable threat intelligence to partners, customers and the cybersecurity community.

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