Cloud Secure Edge

Accès à distance, sécurité renforcée

SonicWall Cloud Secure Edge™, anciennement Banyan Security, est une solution SSE (Security Services Edge) très efficace et facile à adopter, qui permet à vos effectifs d'accéder en toute sécurité à n'importe quelle ressource depuis n'importe quel appareil. Elle offre un accès Zero Trust simple et sécurisé aux ressources privées et Internet pour tous vos employés et les tiers, où que se trouve leur réseau. Elle réunit les fonctionnalités de plusieurs appliances réseau traditionnelles (VPN d'accès à distance, proxy Web, pare-feu et autres) dans une solution unifiée fournie dans le cloud, améliorant ainsi la stratégie de sécurité et l'expérience utilisateur pour l'ensemble du personnel.

Remarque : les clients ayant déjà déployé des pare-feux de 7e génération SonicWall peuvent les connecter directement à Cloud Secure Edge et gérer les règles d'accès via un tableau de bord unifié.

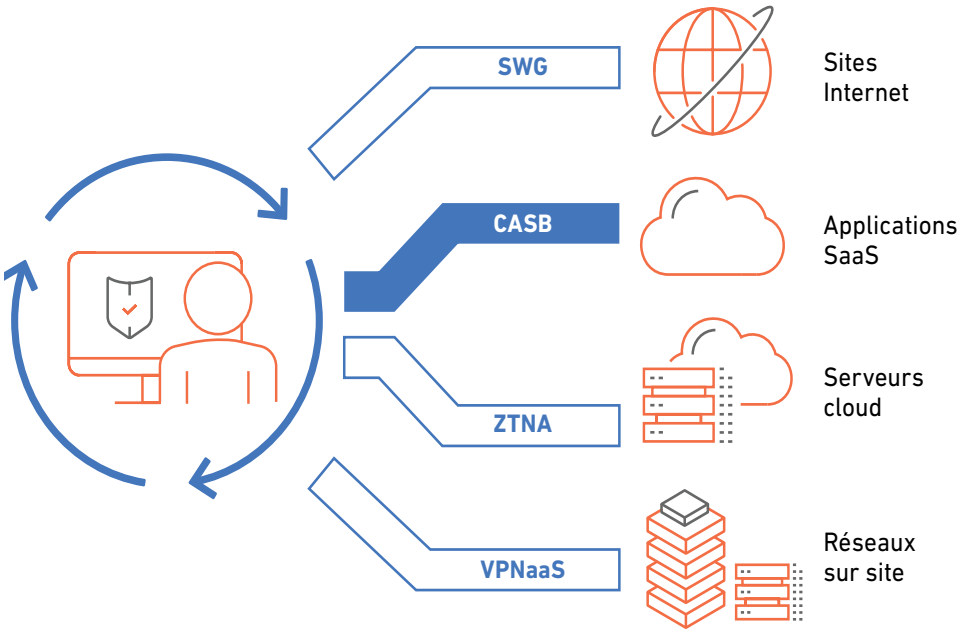

Figure 1 : SonicWall Cloud Secure Edge protège l'accès à toutes les ressources depuis n'importe quel appareil

FICHE TECHNIQUE

Pourquoi SonicWall Cloud Secure Edge ?

FACILITÉ DE DÉPLOIEMENT ET DE GESTION

Cloud Secure Edge peut être autonome ou ajouté sous forme d'abonnement mensuel à vos pare-feux de 7e génération SonicWall existants. C'est la solution idéale pour les MSP et les entreprises dont les ressources sont surchargées et qui recherchent un faible TCO et un retour sur investissement rapide.

PROTECTION CONTRE LES MENACES MODERNES

Cloud Secure Edge intègre des contrôles de sécurité Zero Trust indispensables pour les effectifs hybrides et distants qui doivent pouvoir accéder depuis n'importe où aux ressources privées et Internet sensibles dont ils ont besoin pour travailler. Afin d'offrir une sécurité exceptionnelle avec une excellente expérience utilisateur, il utilise une technologie unique basée à la fois sur une cryptographie éphémère et sur un score de confiance centré sur le terminal et l'identité.

PERFORMANCES ET CONFIDENTIALITÉ

Cloud Secure Edge a été conçu dès le départ pour offrir des performances élevées tout en garantissant la confidentialité. L'administrateur contrôle totalement les données tout en veillant à ce que les utilisateurs bénéficient de la connexion la plus naturelle et la plus efficace possible pour une productivité, une protection des données et une confidentialité maximales.

Cas d'utilisation courants

Modernisation de VPN/pare-feu avec ZTNA

Plutôt que de s'appuyer sur des outils rudimentaires comme les pare-feux et les anciens VPN pour protéger les ressources de l'entreprise, Cloud Secure Edge permet un accès de moindres privilèges à des applications et serveurs spécifiques qui repose sur les facteurs contextuels combinés en temps réel de la confiance de l'utilisateur et de l'appareil, et de la sensibilité des ressources.

La solution est basée sur le cloud et peut être appliquée indépendamment ou conjointement avec des infrastructures de sécurité préexistantes.

Protection contre les menaces Internet et la compromission des identifiants

SonicWall a déployé des POP mondiaux ultraperformants afin de garantir le routage le plus efficace et le plus direct possible, tout en appliquant des contrôles de mise en œuvre cohérents pour se protéger contre tout type d'attaque ou d'exposition aux risques. Cela permet une protection simple et efficace contre les attaques de phishing et les sites Web malveillants, tout en appliquant un filtrage de contenu selon les besoins. La sécurité de l'appareil est vérifiée en amont avant que l'accès ne soit accordé, comme il se doit.

Sécurisation des utilisateurs à haut risque (tiers/BYOD/fusions-acquisitions)

Donnez aux tiers un accès facile et sécurisé aux seules ressources spécifiques dont ils ont besoin, sans surprovisionnement. Cloud Secure Edge garantit un accès basé non seulement sur la stratégie de sécurité de l'utilisateur et de l'appareil, mais aussi sur son rôle et sur ce qu'il est autorisé à voir. Pour une gestion encore plus simplifiée, les groupes et les rôles peuvent être pré-identifiés et appliqués selon les besoins depuis une console centrale. Il n'est pas nécessaire d'appliquer des correctifs ou de configurer le matériel, jamais.

Licences

Deux licences sont proposées lors de l'acquisition de Cloud Secure Edge : Secure Private Access (accès privé sécurisé aux ressources sur les réseaux internes) et Secure Internet Access (accès aux ressources sur l'Internet public).

1. La licence Secure Private Access offre deux fonctionnalités de base :
   - ZTNA par tunnel (également appelé Cloud VPN ou VPNaaS) : accès sécurisé à des segments spécifiques du réseau.
   - ZTNA par proxy : accès sécurisé aux ressources privées telles que les applications HTTP internes et les services TCP.
2. La licence Secure Internet Access offre trois fonctionnalités de base :
   - Sécurisation de la couche DNS (DNS) : protection contre les menaces au niveau du domaine bloquant les domaines malveillants et appliquant des stratégies d'utilisation acceptables.
   - Courtier en sécurité d'accès au cloud (CASB) : application de règles de confiance de l'appareil pour accéder aux applications SaaS.
   - Passerelle Web sécurisée (SWG) : filtrage du contenu Web pour bloquer les malwares et autres menaces cachées dans le trafic chiffré.

Les références Secure Private Access (SPA) et Secure Internet Access (SIA) sont disponibles dans deux échelons : Basic et Advanced. Les licences sont vendues par utilisateur.

Fonctionnalités communes

Plan de données hautes performances

Architecture périphérique dynamique pour des connexions rapides et fiables avec les utilisateurs du monde entier

Prise en charge native de tous les systèmes d'exploitation clients

Ordinateurs de bureau (Windows, macOS, Linux) et appareils mobiles (iOS, Android, ChromeOS)

Interface de gestion cloud

Pour les administrateurs IT et sécurité afin de configurer la connectivité Zero Trust

Score de confiance

Quantification du niveau de confiance et de risque associé à vos utilisateurs et appareils

Visibilité concrète

Vue complète des risques liés aux utilisateurs/appareils et aux applications/ressources

Application continue des règles

Selon la sensibilité des ressources, indépendamment de la localisation de l'utilisateur

Intégrations

Intégration avec les outils existants (IDP, EDR, MDM, SIEM)

Connecteur de pare-feu SonicWall

Intégration immédiate avec les pare-feux de 7e génération en mode Global sur 7.1.2+.

Gestion multilocataires

Règles basées sur le cloud pour une gestion multilocataires

Utilisateurs et appareils

Signature unique (SSO)

Utilisation des règles SSO de l'entreprise avec création d'utilisateurs en flux tendu

Gestion de la stratégie

Analyse de la stratégie d'un appareil, tel que pare-feu, chiffrement du disque, verrouillage de l'écran, version du système d'exploitation, etc.

Profils de confiance

Personnalisation des facteurs et des effets de la règle en fonction des groupes d'utilisateurs et des appareils

Remédiation sur mesure

Configuration des consignes de remédiation de la stratégie de l'appareil, telles que les messages et les liens, visibles par vos utilisateurs finaux

Visibilité et conformité

Flux d'événements en temps réel

Surveillance en temps réel de l'activité des utilisateurs et des appareils

Rapport sur la stratégie de l'appareil

Suivi de tous les appareils, gérés et non gérés, accédant aux ressources de l'entreprise, ainsi que de leur stratégie de sécurité

Rapport sur les activités d'administration

Consignation de toutes les activités d'administration dans le Cloud Command Center

Opérations et automatisation

API Restful

Terminal RESTful pour configurer les objets CSE dans le plan de contrôle

Clients API : pybanyan, terraform

Bibliothèque Python et terraform pour l'automatisation et la gestion

Enregistrement des appareils sans contact (Zero Touch)

Déploiement de l'application Banyan sur le parc d'appareils sans aucune interaction avec l'utilisateur final

	Secure Private Access		Secure Internet Access	
Fonctionnalité	**Basic**	**Advanced**	**Basic**	**Advanced**
Fonctionnalités de base				
Tunnel ZTNA (VPNaaS) pour permettre l'accès à des réseaux spécifiques	✓	✓		
Proxy ZTNA pour une connexion en toute sécurité aux applications HTTP internes et aux services TCP		✓		
Sécurisation de la couche DNS pour la protection contre les menaces Internet			✓	✓
Courtier en sécurité d'accès au cloud (CASB) pour appliquer les règles de confiance de l'appareil pour les applications SaaS				✓
Passerelle Web sécurisée (SWG) pour filtrer les malwares et autres menaces cachés dans le trafic Web chiffré				✓
Accès réseau sécurisé				
Réseaux privés (plages RFC-1918) et domaines (serveurs DNS internes)	✓	✓		
Split-tunneling vers des sous-réseaux et domaines spécifiques (privés ou publics)	✓	✓		
Full-tunneling pour tout le trafic	✓	✓		
Règles de réseau/couche 4 basées sur les CIDR et FQDN	✓	✓		
Accès sécurisé aux ressources privées				
Accès aux sites Web internes à l'aide de flux OpenID Connect réservés aux navigateurs		✓		
SSH vers les serveurs Linux		✓		
RDP vers les machines Windows		✓		
Clients natifs pour accéder aux serveurs de bases de données tels que PostgreSQL et MySQL		✓		
Client Kubernetes pour accéder au cluster		✓		
Authentification par certificat SSH, autorisation des principaux de sécurité et journalisation des audits		✓		
Règles de couche 7 pour accéder aux API, pages Web		✓		
Protection contre les menaces Internet				
Sécurité de la couche DNS bloquant les domaines avec malware, phishing, botnet et autres risques			✓	✓
Catégorisation du contenu			✓	✓
Blocage personnalisé			✓	✓
Sécurisation des applications SaaS				
Visibilité sur les applications cloud/Shadow IT				✓
Liste des adresses IP autorisées pour les applications cloud via SonicWall Edge				✓
Confiance de l'appareil pour Okta				✓
Confiance de l'appareil pour Azure AD				✓
Confiance de l'appareil pour d'autres IDP comme OneLogin, Jumpcloud				✓
Service de filtrage de contenu Web				
Filtrage d'URL				✓
Protection anti-malware				✓
Utilisateurs et appareils				
Authentification sans mot de passe via fédération du fournisseur d'identité		✓		✓
Accès sur la base de règles depuis des appareils non enregistrés avec un certificat d'appareil de confiance		✓		✓
Accès sans client		✓		✓
Comptes de service (jetons d'API pour l'accès programmatique tel que les scripts et l'automatisation via le plan de données)		✓		✓

SONICWALL

Utilisateurs et appareils (suite)				
Intégration SCIM pour gérer les affectations des utilisateurs		✓		✓
Intégrations EDR (p. ex., CrowdStrike, SentinelOne, Microsoft Defender)		✓		✓
Intégrations MDM/UEM (p. ex., JAMF, Kandji, Jumpcloud, Intune, Workspace One)		✓		✓
Visibilité et conformité				
Intégration SIEM (p. ex., Splunk, Elastic, Sumo Logic)		✓		✓
Détection de réseaux privés (applications non approuvées auxquelles l'utilisateur ou les appareils ont accès)		✓		N/A
Détection de ressources IaaS		✓		N/A
Détection d'applications SaaS		N/A		✓
Opérations et automatisation				
Déploiement à la périphérie du réseau privé Hébergement de la passerelle SonicWall basée sur l'identité dans votre propre infrastructure		✗	N/A	N/A
Services et support				
Support 24h/24, 7j/7	✓	✓	✓	✓
Support Premier		complément		complément
Services RIS		complément		complément

Résumé

SonicWall Cloud Secure Edge est une solution Security Service Edge combinant un TCO exceptionnel avec une sécurité Zero Trust haut de gamme. Elle offre aux employés comme aux tiers un accès Zero Trust simple et sécurisé aux ressources privées et Internet, où que se trouve leur réseau. Cloud Secure Edge réunit les fonctionnalités de plusieurs appliances réseau traditionnelles (VPN d'accès à distance, proxy Web, pare-feu, etc.) dans une solution multilocataires unifiée fournie dans le cloud qui est simple à déployer et facile à gérer pour les entreprises de toutes tailles, maximisant ainsi le retour sur investissement pour vous et vos clients.

Vous souhaitez en savoir plus sur SonicWall Cloud Secure Edge ? Commencez ici.

Contactez votre chargé de clientèle si vous souhaitez ajouter Cloud Secure Edge à vos pare-feux de 7e génération SonicWall existants.

À propos de SonicWall

Forte de plus de 30 années d'expertise, SonicWall est une entreprise pionnière dans le domaine de la cybersécurité qui porte une attention constante à ses partenaires. De par sa capacité à créer, faire évoluer et gérer en temps réel la sécurité dans le cloud ainsi que dans les environnements hybrides et traditionnels, SonicWall est en mesure de fournir rapidement et économiquement des solutions de sécurité sur mesure à toute entreprise dans le monde entier. En s'appuyant sur les données de son propre centre de recherche sur les menaces, SonicWall offre une protection sans faille contre les cyberattaques les plus évasives et fournit des renseignements exploitables sur les menaces à ses partenaires, à ses clients et à la communauté de la cybersécurité.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Consultez notre site Internet pour de plus amples informations.
www.sonicwall.com