SONICWALL

SonicWall Cloud Edge Secure Access

Bénéficiez d'une sécurité basée sur une vérification systématique (« zéro confiance ») en quelques minutes seulement

SonicWall Cloud Edge Secure Access est un service cloud puissant qui fournit un réseau à la demande en toute simplicité pour la connectivité de site à site et par cloud hybride à AWS, Azure, Google Cloud et bien plus encore. Ce service regroupe les approches de sécurité « zéro confiance » et « droit d'accès minimal » dans une seule offre intégrée.

L'approche de droit d'accès minimal restreint l'accès d'un utilisateur spécifique à ce qui est nécessaire et à rien d'autre, à l'instar du « principe de connaissance sélective ». En limitant l'exposition aux autres zones sensibles du réseau, les entreprises peuvent sécuriser leurs ressources sans avoir à renoncer à leur souplesse opérationnelle.

Le service SonicWall Cloud Edge Secure Access applique une sécurité « zéro confiance » basée sur quatre actions de sécurité majeures :

- Vérification des identifiants de l'utilisateur et du périphérique, même pour le trafic interne
- Contextualisation de la demande pour garantir l'authenticité et le respect des directives de l'entreprise
- Micro-segmentation de l'accès au réseau pour empêcher tout déplacement latéral des menaces
- Octroi d'un accès aux applications demandées, et rien de plus

Au cœur de l'infrastructure du service Cloud Edge Secure Access se trouve l'architecture SDP (paramètre à base de logiciel), qui allie modernité et sécurité de par sa conception.

L'architecture SDP dissocie le contrôleur (qui authentifie les utilisateurs et les appareils) des passerelles (qui servent d'intermédiaires de confiance). En distribuant les passerelles à proximité des sites des utilisateurs finaux, le service Cloud Edge Secure Access peut évoluer rapidement pour maintenir des performances élevées et offrir la meilleure expérience possible sur le cloud.

En outre, la séparation des fonctions neutralise efficacement les cybermenaces courantes, comme les attaques DDoS, le piratage du Wi-Fi public, les inondations SYN et le script Slowloris, et permet à SonicWall de proposer une plateforme de sécurité « zéro confiance » hautement intégrée.

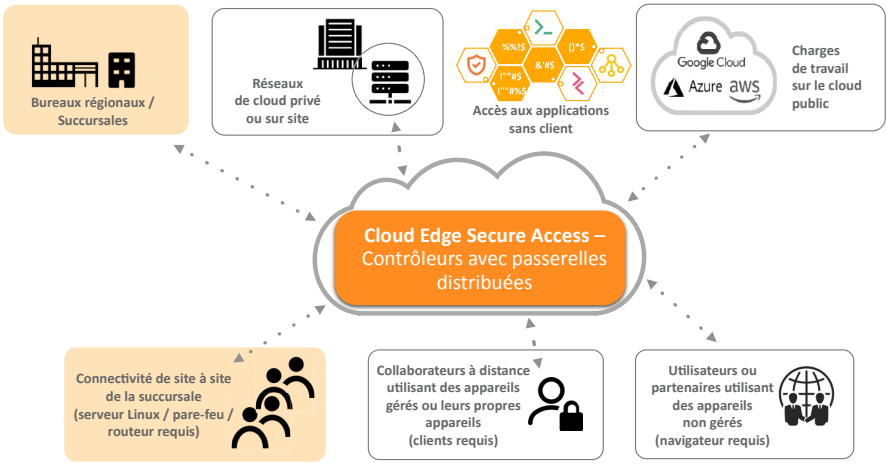

Illustration 1 – SonicWall Cloud Edge Secure Access

Avantages :

- Sécurise les entreprises distribuées et le personnel à distance
- Accès sécurisé instantané à tous les sites et ressources sur des clouds hybrides
- Politiques de vérification systématique par réseaux, applications, profils utilisateurs et terminaux
- Micro-segmentation intégrée pour empêcher les mouvements latéraux non autorisés
- Capacité d'évolution de 100 à plusieurs milliers d'utilisateurs
- 15 minutes suffisent au responsable informatique pour la configuration
- L'utilisateur final peut déployer le service en 5 minutes
- Aucune limite d'utilisation ni de bande passante
- Sécurité du Wi-Fi public
- Chiffrement WireGuard haute performance
- Intégration du fournisseur d'identité cloud
- Intégration moderne des protocoles d'authentification SSO et MFA
- Neutralise les attaques DDoS, les scripts Slowloris et les inondations SYN
- Mutualisation pour les MSSP
- Surveillance et élaboration de rapports complets pour les audits de conformité
- Passerelles cloud dédiées et adresses IP par client
- Service disponible aux États-Unis, en Europe, au Moyen-Orient et en Asie

L'évolution du VPN traditionnel vers une sécurité « zéro confiance »

À l'ère de la transformation numérique où les collaborateurs peuvent travailler depuis n'importe où et où les ressources sont dans le cloud, la solution VPN traditionnelle est trop compliquée à déployer et comporte trop de restrictions.

Le déploiement d'un VPN classique peut prendre plusieurs jours, voire des semaines, entravé par une offre insuffisante et la difficulté à programmer des temps d'arrêt.

Un VPN traditionnel peut également ouvrir une porte dérobée à une violation potentielle, dans la mesure où une connexion réussie offre à un utilisateur un large accès au réseau et lui permet de se déplacer latéralement dans le sous-réseau.

Pour finir, le VPN induit une latence supplémentaire qui nuit à l'expérience cloud des utilisateurs, car le trafic des utilisateurs passe par le concentrateur VPN sur site au lieu d'aller directement au cloud.

Selon les prévisions de Gartner, d'ici 2023, 60 % des entreprises élimineront progressivement la plupart de leurs réseaux privés virtuels (VPN) d'accès à distance au profit d'un accès au réseau « zéro confiance ».

Le service SonicWall Cloud Edge Secure Access surmonte les problèmes décrits ci-dessus et propose un accès au réseau « zéro confiance » avec ces trois capacités essentielles :

Principe de droit d'accès minimal pour protéger les actifs de l'entreprise

Déploiement rapide et en libre-service

Accès direct et fiable au cloud depuis n'importe où

Illustration 2 – Capacités de SonicWall Cloud Edge Secure Access

Principaux cas d'utilisation

Déploiement rapide et en libre-service

- **Déploiement rapide –** Moins de 15 minutes suffisent à un responsable informatique pour inscrire un utilisateur, instancier une passerelle et configurer des politiques granulaires en fonction des réseaux et du contexte utilisateur.
- **Intégration rapide des utilisateurs –** Un utilisateur final a la possibilité de se connecter via une application client mobile ou de bureau ou de contourner complètement une installation client lorsqu'il utilise un ordinateur public, à condition qu'un navigateur soit disponible. Grâce au modèle de déploiement en libre-service, un utilisateur peut être opérationnel en 5 minutes.
- **Accès fiable au cloud hybride –** Lorsque le déploiement est terminé, les utilisateurs bénéficient d'un accès rapide, simple et sécurisé aux ressources sur site et au cloud public, partout dans le monde.

Protection des personnes qui travaillent depuis n'importe où qui se connectent via des points d'accès de confiance et publics

- **Sécurité Wi-Fi automatique –** Les applications agent Cloud Edge Secure Access pour Windows et macOS surveillent de manière proactive l'environnement et activent automatiquement une connexion sécurisée dans les points d'accès publics. Cela protège les utilisateurs des interceptions Wi-Fi bien trop fréquentes qui peuvent entraîner des vols de données et une violation de la conformité.
- **Coupe-circuit –** Pour neutraliser une cyberattaque potentielle, lorsqu'une connexion sécurisée est interrompue, la connexion Internet de l'appareil sera instantanément coupée pour empêcher les données de quitter l'appareil.
- **Réseaux Wi-Fi de confiance –** Lorsqu'un SSID est spécifié comme fiable, la fonction de sécurité Wi-Fi automatique ne s'activera pas.
- **VPN / Applications accessibles en permanence –** Cette fonction pratique reconnecte automatiquement un utilisateur ou un appareil à l'application ou à un ensemble d'applications sans nécessiter de nouvelle connexion ou de réauthentification.

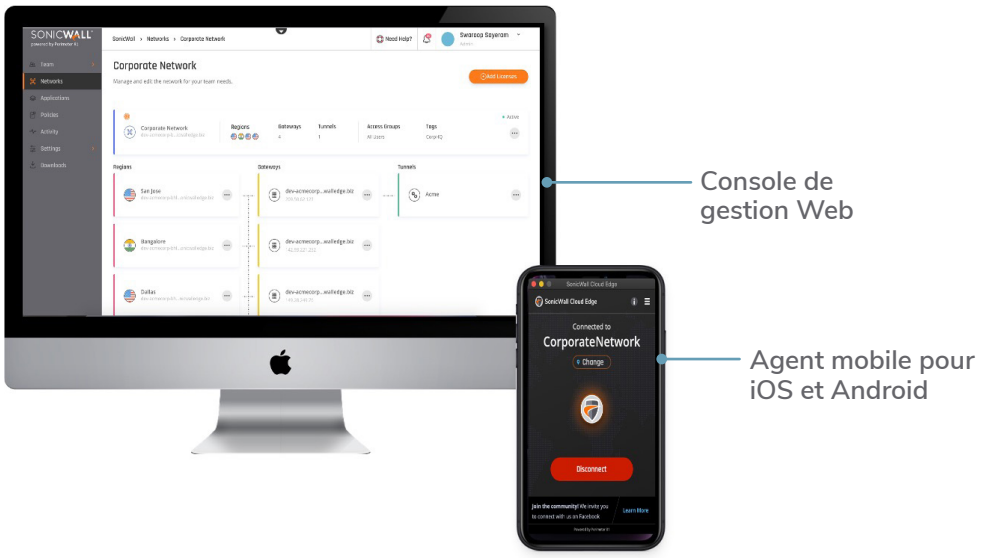

Illustration 3 – Console de gestion SonicWall Cloud Edge Secure Access et application agent mobile pour Apple iOS

Accès aux applications « zéro confiance »

Cloud Edge Secure Access offre aux organisations numériques l'outil nécessaire pour protéger les ressources de l'entreprise tout en autonomisant et responsabilisant simultanément le personnel distant.

Grâce aux politiques « zéro confiance » de Secure Access, les utilisateurs externes qui jouissent d'un ensemble contextuel approprié peuvent accéder en toute sécurité à une multitude d'applications de bureau et Web à distance sans exposer le réseau de l'entreprise aux cybermenaces.

- **Contrôle par droit d'accès minimal strictement appliqué –** Les organisations peuvent contrôler les interactions avec les ressources en fonction d'attributs pertinents, notamment l'identité de l'utilisateur et du groupe et la sensibilité des données consultées.
- **Service basé sur le contexte –** La solution garantit un accès centré sur l'utilisateur et basé sur les politiques aux ressources sur site et hébergées dans le cloud.
- **Compatible avec les fournisseurs majeurs de gestion d'identité basée sur le cloud –** Les organisations peuvent prolonger la durée de vie des anciens actifs sur site ou procéder à une migration vers des services modernes de gestion d'identité basée sur le cloud proposés par des fournisseurs comme Azure AD, Google Authenticator et Okta.
- **Micro-segmentation –** En segmentant précisément chaque flux de trafic entrant, la micro-segmentation empêche les logiciels malveillants ou les utilisateurs non autorisés de se déplacer latéralement, réduisant ainsi la surface d'attaque et l'exposition globale aux cybermenaces.
- **Authentification unique fédérée et authentification à facteurs multiples –** Cette combinaison crée un portail unique pour authentifier les utilisateurs dans un environnement informatique hybride, offrant une expérience cohérente et transparente.
- **Système d'audit de conformité –** Chaque activité liée à un accès « zéro confiance » est entièrement surveillée et consignée pour les audits futurs.

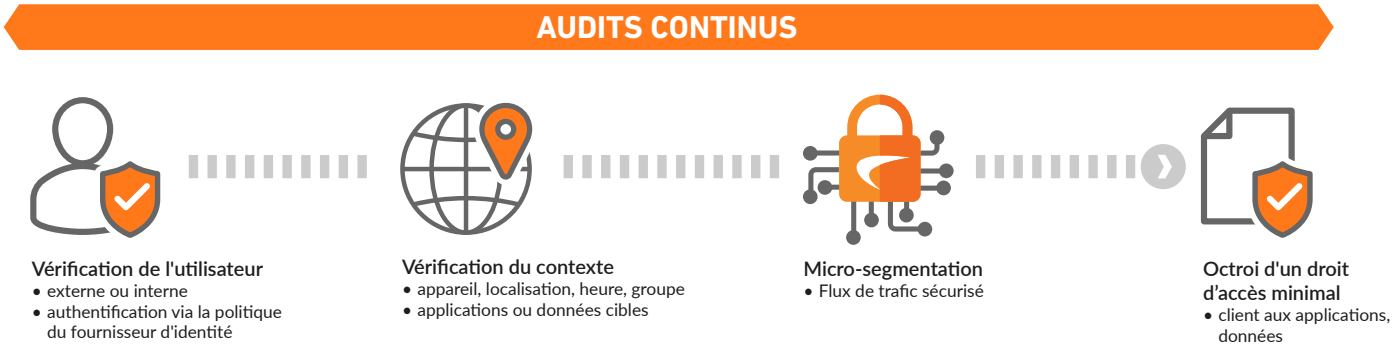

Illustration 4 – Processus d'accès au réseau « zéro confiance » de SonicWall Cloud Edge Secure Access

Interconnectivité de site à site ou réseau à la demande (NaaS)

Cloud Edge Secure Access offre un service de connectivité de site à site ou un réseau à la demande (NaaS) pour intégrer rapidement des succursales dans des sites dispersés d'un point de vue géographique.

Grâce à la fonction NaaS, un responsable informatique peut connecter rapidement et en toute sécurité des kiosques mobiles, des commerces de détail et des points de vente aux ressources hébergées dans le cloud sans avoir à se fier à la technologie MPLS onéreuse.

- **Service d'interconnexion de site à site ou de site au cloud –** La solution se connecte facilement aux environnements cloud populaires, notamment AWS, Azure et Google Cloud, ou crée un lien de communication sécurisé entre deux réseaux distincts situés sur différents sites.
- **Déploiement dans plusieurs régions –** Les administrateurs peuvent déployer des passerelles Cloud Edge dédiées à divers endroits pour mieux servir les succursales internationales et les employés à une vitesse optimale.
- **Pilier mondial haute performance –** Le service Cloud Edge de SonicWall est disponible dans le monde entier. L'infrastructure offre une latence minimale en distribuant des passerelles à proximité des sites des clients et en répartissant la charge liée au trafic entre les serveurs.
- **Tunnel WireGuard de pointe –** Un responsable informatique peut exploiter tous les routeurs ou les pare-feu d'une succursale avec IPsec pour se connecter à la passerelle Cloud Edge la plus proche.

  Pour profiter de performances optimales, SonicWall recommande la fonction de connecteur WireGuard qui nécessite qu'un serveur Linux de succursale exécute le service de tunnel WireGuard vers la passerelle la plus proche.
- **Audit et suivi du réseau –** Obtenez plus d'informations sur l'intégrité, l'activité et la sécurité de votre réseau, en bénéficiant notamment d'une visibilité sur la création des groupes et des serveurs, l'authentification des membres de l'équipe, les changements des mots de passe et bien plus encore.

Caractéristiques

Catégorie	Fonctionnalité	Avantages
Évolutivité et performances	Utilisateurs	100 à + de 10 000
	Performances	1 Gbit/s par passerelle client ; évolutivité cloud horizontale avec davantage de passerelles
Plateforme cloud	Plateforme de gestion cloud	Plateforme de gestion cloud pour créer facilement le réseau de votre organisation. Incluse sur site et sur le cloud
	Déploiement rapide et facile du réseau	Déploiement automatique de votre réseau en moins de 15 minutes
	Disponibilité	Gestion automatique assurée par le service. Le statut actuel du service Cloud Edge est disponible sur https://status.sonicwall.com/
	Répartition de la charge	Fournie par des passerelles partagées/dédiées dans plus de 30 points de présence mondiaux, hébergées et gérées par SonicWall
	Interconnectivité de site à site	Connectivité entre deux sites (sur site, hors site ou dans le cloud). Prend en charge IPsec et WireGuard
	DNS personnalisé	Pour utiliser vos propres serveurs DNS internes, après avoir défini un tunnel, vous pouvez également définir un serveur DNS personnalisé au lieu d'utiliser le DNS par défaut
	Accès aux applications sans client	Accès aux applications « zéro confiance » pour HTTP, HTTPS, RDP, VNC, SSH
	Accès client	Disponible pour les plateformes Windows, Mac, iOS et Android
	Applications et environnement	Convient mieux aux environnements hybrides et aux charges de travail cloud
Capacités « zéro confiance »	Applications accessibles en permanence	Les applications accessibles en permanence fournissent un accès sécurisé à Internet lorsque vous vous connectez à un réseau non fiable, ce qui vous protège des menaces pour la sécurité
	Segmentation basée sur les politiques	Politiques appliquées par utilisateur et par application
	Politiques granulaires de contrôle d'accès	Basées sur l'utilisateur, l'application, la localisation de l'adresse IP, la géolocalisation (pays), le type de navigateur, le système d'exploitation, la date et l'heure
	Séparation des flux (split tunneling)	Vous permet de décider par quel sous-réseau transitera votre trafic
	Coupe-circuit	Pour neutraliser une cyberattaque potentielle, lorsqu'une connexion sécurisée est interrompue, la connexion Internet de l'appareil sera instantanément coupée pour empêcher les données de quitter l'appareil
	Sécurité Wi-Fi automatique	Notre fonctionnalité brevetée protège automatiquement les appareils des employés lorsqu'ils se connectent à un réseau Wi-Fi public non sécurisé
	Filtrage des DNS	Empêchez les utilisateurs de votre réseau d'accéder à certains sites Web, catégories de sites et adresses IP via un navigateur
Authentification	Capacités d'authentification unique	Mettez en place un protocole de connexion unifié via des fournisseurs d'authentification unique comme Okta, G Suite, Azure AD et Active Directory LDAP
	Authentification à deux facteurs	Empêchez les attaques à distance grâce à l'intégration de l'authentification à deux facteurs SMS, DUO Security et Google Authenticator
Surveillance, connexion et assistance	Assistance 24 h/24, 7 j/7	Solution cloud entièrement gérée avec assistance incluse
	Audits et rapports d'activité	Surveillance des connexions, des déploiements de passerelles et des connexions applicatives
	Intégration SIEM	Saisie, conservation et transmission des informations et événements de sécurité en temps réel à toutes les applications SIEM, notamment via une intégration facile par simple clic avec Splunk
	Statut du service cloud	Rendez-vous sur https://www.sonicwall.com/support
Interopérabilité	Pare-feu d'entreprise	SonicWall, Check Point, Fortinet, Palo Alto Networks, WatchGuard, Sophos, Xyxel, UniFi, pfSense, Cisco et Untangle
Intégrations personnalisées	API disponible	Notre API complète basée sur REST permet une intégration rapide et facile aux outils de gestion, d'automatisation et d'orchestration tiers, garantissant la protection des applications virtualisées nouvellement créées ou délocalisées
Conformité	Normes ISO 27001 et 27002, SOC-2 de type 2	Infrastructure cloud conforme à la norme SOC 2 de type 2
Commande	Abonnement	Prenez contact avec votre MSSP, votre revendeur ou votre distributeur pour souscrire un abonnement au service Cloud Edge Secure Access

À propos de SonicWall

SonicWall offre une solution de cybersécurité sans limites pour l'ère de l'hyper-distribution dans une réalité professionnelle où tout le monde est mobile, travaille à distance et sans sécurité. En connaissant l'inconnu, en offrant une visibilité en temps réel et en permettant de véritables économies, SonicWall comble le fossé commercial en matière de cybersécurité pour les entreprises, les gouvernements et les PME du monde entier. Pour en savoir plus, rendez-vous sur www.sonicwall.com.

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

Datasheet-CloudEdge-US-VG-2807