SonicWall Secure Mobile Access (SMA)

SonicWall SMA est une passerelle d'accès sécurisé unifiée, destinée aux entreprises confrontées aux thématiques de la mobilité, du BYOD et de la migration vers le cloud.

SonicWall SMA est une passerelle d'accès sécurisé unifiée qui permet aux entreprises de fournir un accès aux ressources stratégiques de l'entreprise partout, tout le temps et depuis n'importe quel appareil. Le moteur de règles de contrôle d'accès granulaire, l'autorisation contextuelle des appareils, le VPN au niveau applicatif et l'authentification avancée avec SSO de SMA permettent aux entreprises d'adopter le BYOD et la mobilité dans un environnement informatique hybride.

Mobilité et BYOD

SMA devient un allié essentiel pour les entreprises qui souhaitent adopter le BYOD, la flexibilité du travail ou l'accès pour des tiers. La solution SMA de SonicWall fournit une sécurité de pointe permettant de réduire à un minimum les menaces en surface. La prise en charge des tout derniers algorithmes et méthodes de chiffrement assure, elle, une protection en profondeur. Elle permet aux administrateurs de configurer un accès mobile sécurisé et des privilèges en fonction de rôles, de manière à ce que les utilisateurs finaux puissent accéder rapidement et facilement aux applications, données et ressources dont ils ont besoin. Parallèlement, les entreprises peuvent établir des règles de sécurisation BYOD pour protéger leur réseau et leurs données des accès indésirables et des logiciels malveillants.

Passage au cloud

Pour les entreprises qui se lancent dans la migration vers le cloud, SMA offre une infrastructure à authentification unique (SSO, Single Sign-On) qui utilise un portail Web unique pour authentifier les utilisateurs dans un environnement informatique hybride. Qu'une ressource soit en local, sur le Web ou dans un cloud hébergé, l'expérience d'accès est fluide et homogène. SMA s'intègre aussi aux principales technologies d'authentification multi-facteurs pour une sécurité accrue.

Fournisseurs de services gérés

Pour les organisations qui hébergent leur propre infrastructure ou pour les fournisseurs de services gérés, SMA fournit une solution clés en main permettant une continuité des activités et une évolutivité optimales. SMA peut prendre en charge jusqu'à 20 000 connexions simultanées sur une seule appliance avec la possibilité d'évoluer jusqu'à des centaines de milliers d'utilisateurs grâce au clustering intelligent. Les datacenters peuvent réduire les coûts grâce au clustering actif/actif et un équilibreur de charge dynamique intégré qui redirige en temps réel le trafic global vers le datacenter le mieux optimisé en fonction de la demande des utilisateurs. Les ensembles d'outils SMA permettent aux fournisseurs de proposer leurs services sans la moindre interruption pour respecter les SLA les plus stricts.

SMA permet aux services informatiques de fournir la meilleure expérience et l'accès le plus sécurisé en fonction du scénario utilisateur. Disponible sous forme d'appliances physiques renforcées ou de puissantes appliances virtuelles, SMA s'intègre de manière transparente dans l'infrastructure informatique existante. Les entreprises peuvent choisir entre une série d'accès sécurisés Web sans client pour les tiers ou les employés sur des périphériques personnels ou bien un accès total plus traditionnel par tunnel VPN avec client destiné aux dirigeants et compatible avec tous les types d'appareils. Qu'une entreprise doive fournir un accès sécurisé fiable à cinq utilisateurs en un seul endroit ou s'adapter à des milliers d'utilisateurs dans des datacenters sur toute la planète, SonicWall SMA a la solution.

SonicWall SMA permet aux entreprises d'adopter sans crainte la mobilité et le BYOD et de migrer facilement vers le cloud. SMA donne plus de moyens au personnel et lui fournit une expérience d'accès cohérente.

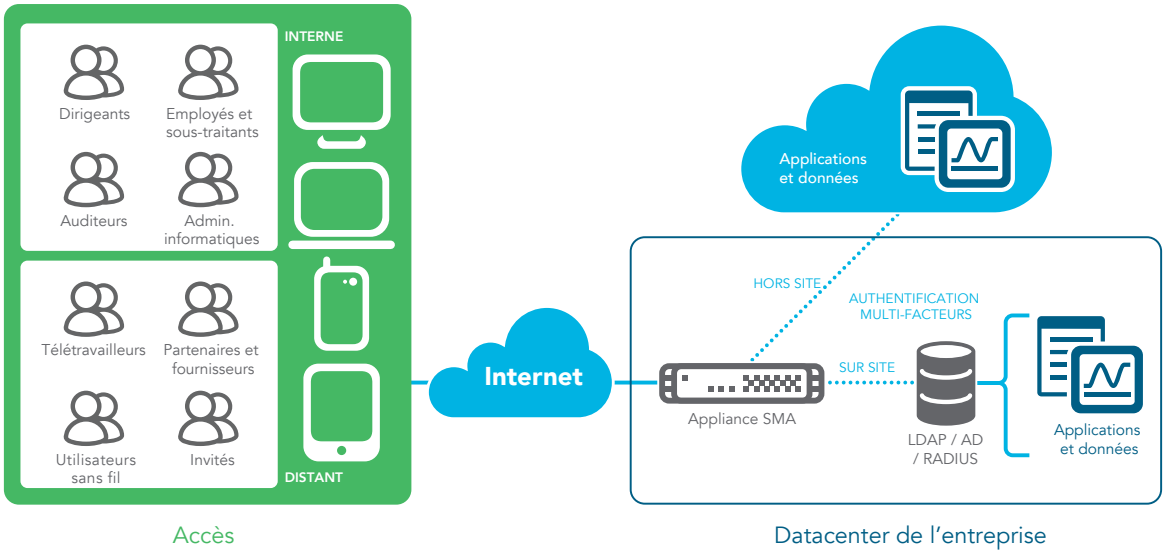
Avantages :

- Accès sécurisé unifié à toutes les ressources réseau et cloud à tout moment, sur tous les appareils et applications
- Contrôle des accès aux ressources par la définition de règles granulaires avec le moteur robuste de contrôle d'accès
- Augmentation de la productivité grâce à l'authentification unique fédérée pour n'importe quelle application SaaS ou hébergée localement avec une seule URL
- Réduction du coût total de possession et simplification de la gestion des accès par la consolidation des éléments de l'infrastructure dans un environnement informatique hybride
- Gain de visibilité sur tous les appareils connectés et octroi des accès en fonction des règles et de la santé du terminal
- Prévention des logiciels malveillants par l'analyse de tous les fichiers chargés sur le réseau avec la sandbox Capture ATP
- Protection contre les attaques Web et conformité PCI avec le complément Web Application Firewall
- Blocage des attaques de zombies et DDoS grâce à la détection Geo IP et à la protection contre les botnets
- Fonctionnalité d'agent sécurisée native par un accès navigateur sans client HTML5, ce qui élimine les coûts d'installation et de gestion d'agents sur les terminaux
- Informations exploitables pour prendre les bonnes décisions avec surveillance en temps réel et reporting exhaustif
- Déploiement facilité par des options flexibles d'appliances virtuelles et physiques s'adaptant à votre entreprise
- Octroi dynamique de licences d'accès en fonction de la demande en temps réel avec orientation automatisée du terminal vers la connexion présentant la meilleure performance et la plus faible latence
- Réduction du coût initial avec équilibrage de charge intégré sans matériel ou services supplémentaires et zéro impact en cas de basculement d'appliances
- Assurance contre les interruptions d'activité ou les pics saisonniers par l'adaptation instantanée des capacités

Appliance SMA et déploiement

Une passerelle renforcée pour un accès sécurisé partout, tout le temps, depuis tous les terminaux

SMA est une passerelle avancée qui offre un accès sécurisé aux ressources réseau et cloud depuis n'importe quel appareil. SMA applique les règles granulaires centralisées d'accès distant et mobile à toutes les ressources de l'entreprise à l'aide d'une appliance renforcée basée sur Linux. Disponible sous forme d'appliances physiques renforcées ou de puissantes appliances virtuelles, SMA s'intègre de manière transparente dans toutes les infrastructures informatiques existantes.



Les solutions SMA fournissent un accès sécurisé pour tous les utilisateurs, appareils et applications.

Déploiement flexible avec appliances physiques et virtuelles

La solution SonicWall SMA peut être déployée sous la forme d'une appliance hautes performances renforcée ou d'une appliance virtuelle s'appuyant sur les ressources informatiques partagées pour optimiser l'utilisation, faciliter la migration et réduire les coûts d'investissement. Les appliances matérielles reposent sur une architecture multiprocesseur qui allie accélération SSL et débit VPN hautes performances à de puissants proxys pour fournir un accès sécurisé fiable. SMA est aussi disponible avec la certification FIPS 140-2 niveau 2 pour les organisations réglementées et fédérales. Les appliances virtuelles offrent les mêmes fonctionnalités robustes d'accès sécurisé sur les principales plateformes virtuelles, dont Microsoft Hyper-V et VMware ESX.

Licences utilisateurs partagées sur les appliances

Les organisations qui possèdent des appliances distribuées à l'échelle internationale peuvent bénéficier de la fluctuation des demandes de licences utilisateurs en raison du décalage horaire. Si une organisation déploie des licences VPN complètes ou des licences ActiveSync de base, la gestion centralisée SMA réalloue les licences des appliances qui connaissent une diminution des besoins en dehors des heures de travail/pendant la nuit au profit des appliances gérées d'une autre zone géographique soumises à un pic de demandes.

Visibilité du réseau avec profilage contextuel des appareils

L'authentification contextuelle inégalée garantit que seuls les utilisateurs autorisés et les appareils de confiance peuvent accéder au réseau. Les ordinateurs de bureau et portables sont interrogés pour confirmer la présence ou l'absence de logiciels de sécurité, de certificats clients et d'identifiant d'appareil. Avant d'obtenir l'accès, les appareils mobiles sont interrogés pour obtenir des informations essentielles à la sécurité, telles que le statut de déblocage, l'identifiant, le statut des certificats et les versions des systèmes d'exploitation. Les appareils qui ne respectent pas les exigences de ces règles ne peuvent avoir accès au réseau et l'utilisateur est informé du non-respect des règles.

Une expérience cohérente depuis un portail Web unique

Les utilisateurs n'ont pas besoin de se souvenir des URL de chaque application ni de constituer des listes de signets. SMA fournit un portail d'accès centralisé et donne aux utilisateurs une URL pour accéder à toutes les applications vitales depuis un navigateur Web standard. Une fois que l'utilisateur s'est connecté par le navigateur, un portail utilisateur personnalisable s'affiche dans la fenêtre. Une vue unifiée sur un seul écran permet d'accéder à toutes les applications SaaS ou locales. Ce portail n'affiche que les liens et signets personnalisés pertinents pour le terminal, l'utilisateur ou le groupe en particulier. Le portail prend en charge les principales plateformes, dont les appareils Windows, Mac OS, Linux, iOS et Android, ainsi qu'une large gamme de navigateurs sur tous les terminaux.

Authentification unique fédérée sur les applications SaaS et locales

Supprimez la nécessité des mots de passe multiples et mettez un frein aux mauvaises pratiques de sécurité comme la réutilisation des mots de passe. SMA offre l'authentification unique fédérée aux applications SaaS hébergées sur le Cloud et aux applications hébergées sur site. SMA s'intègre à de nombreux serveurs d'authentification, d'autorisation et de traçabilité et aux principales technologies d'authentification multi-facteurs pour plus de sécurité. Le SSO sécurisé n'est attribué qu'aux terminaux autorisés, à l'issue de contrôles concernant leur état de santé et de conformité. Le

moteur de règles d'accès garantit que les utilisateurs ne puissent voir que les applications autorisées et n'accorde l'accès qu'après une authentification réussie.

Empêchez les brèches et bloquez les menaces évoluées

SonicWall SMA renforce la sécurité des accès pour améliorer votre système de sécurité et réduire la surface d'exposition aux menaces.

- SMA s'intègre avec la sandbox multimoteur cloud, SonicWall Capture ATP, pour analyser tous les fichiers chargés par des utilisateurs avec des terminaux non gérés ou en dehors du réseau de l'entreprise. Les utilisateurs sont ainsi assurés de bénéficier du même niveau de protection face aux menaces évoluées, ransomwares ou zero-day, qu'ils soient en déplacement ou au bureau[1].
- Le service SonicWall Web Application Firewall offre aux entreprises une solution bien intégrée et abordable pour sécuriser les applications Web internes. Cela permet aux clients de garantir la confidentialité des données et les services Web internes restent protégés même en cas d'accès indésirable ou malveillant par un utilisateur authentifié.
- La détection Geo-IP et des botnets protège les entreprises des attaques de zombies et DDoS ainsi que des terminaux compromis zombifiés.

Accès sans client par navigateur transparent et sécurisé

L'absence de client sur l'appliance SonicWall SMA signifie que l'administrateur n'a pas besoin d'installer manuellement un lourd composant client sur un ordinateur qui sera utilisé pour l'accès à distance. Cela élimine toute dépendance à Java et supprime les coûts informatiques, ce qui élargit considérablement le concept d'accès distant. Comme aucune préinstallation ou préconfiguration n'est nécessaire, un travailleur distant autorisé peut utiliser n'importe quel ordinateur, partout sur la planète, et accéder en toute sécurité aux ressources de l'entreprise. Dans sa forme la plus épurée, l'accès sécurisé est strictement basé sur navigateur avec HTML5 et fournit une expérience utilisateur transparente et unifiée.

Expérience de disponibilité permanente

Pour assurer la fluidité de l'expérience utilisateur, SMA fournit un VPN disponible en permanence pour les appareils Windows gérés. Les administrateurs peuvent configurer des paramètres permettant d'établir automatiquement une connexion VPN dès que le client d'un terminal autorisé détecte un réseau public ou non fiable. Un simple login sur l'appareil Windows procure à l'utilisateur une connexion sécurisée aux ressources de l'entreprise. Nul besoin de se connecter à son client VPN ni de conserver plusieurs mots de passe. Il en résulte une expérience fluide qui permet aux utilisateurs nomades d'accéder aux ressources vitales comme s'ils étaient au bureau et aux administrateurs informatiques de garder le contrôle des appareils gérés, ce qui améliore les conditions de sécurité de l'entreprise.

Gestion intuitive et rapports exhaustifs

La plateforme Web de gestion intuitive fournie par SonicWall permet de rationaliser la gestion des appliances et propose des fonctionnalités de reporting étendues. L'interface utilisateur conviviale apporte de la clarté dans la gestion d'une ou plusieurs appliances et règles. Chaque page montre comment les paramètres sont configurés sur toutes les machines sous votre contrôle. La gestion unifiée des règles vous permet de créer et de surveiller des règles et configurations d'accès. Une seule règle peut contrôler l'accès de vos utilisateurs, appareils et applications aux données, serveurs et réseaux. Le service informatique peut automatiser des tâches de routine et programmer des activités, les équipes de sécurité n'ont donc plus à se soucier des tâches répétitives et peuvent se concentrer sur les missions stratégiques comme la réaction aux incidents. Le service informatique obtient des informations sur les tendances en matière d'accès et sur la santé de l'ensemble du système grâce au reporting convivial et à la journalisation centralisée.

Offrez la disponibilité des services 24h/24 7j/7

Les entreprises sont tenues de maintenir de leurs services et d'assurer leur disponibilité avec un haut degré de fiabilité pour fournir un accès sécurisé permanent aux applications vitales. Les appliances SMA prennent en charge la haute disponibilité (HA) active/passive traditionnelle pour les entreprises avec des datacenters uniques ou la haute disponibilité globale avec clustering actif/actif pour les datacenters locaux et distribués. Les deux modèles HA offrent une expérience fluide aux utilisateurs avec basculement zéro impact et persistance de session.

Déployez le client VPN qui correspond à vos besoins

Faites votre choix parmi une large gamme de clients VPN pour fournir un accès distant sécurisé à base de règles pour différents terminaux, dont les ordinateurs portables, smartphones et tablettes.

Client VPN	SE pris en charge	Modèles SMA pris en charge	Point fort
Mobile Connect	iOS, OS X, Android, Chrome OS, Windows 10	Tous les modèles	Authentification biométrique, VPN par application et application des règles au niveau du terminal
Connect Tunnel (client léger)	Windows, Mac OS et Linux	6200, 7200, 8200v, 9000	Environnement de type « au bureau » complet et contrôle des terminaux robuste
NetExtender (client léger)	Windows et Linux	200, 400, 500v	Application des règles d'accès granulaires et extension de l'accès au réseau par des clients natifs

Réduisez le coût initial avec un équilibreur de charge intégré

La fonctionnalité d'équilibrage de charge intégrée à l'appliance SMA offre le niveau d'évolutivité attendu pour les déploiements de grandes et moyennes entreprises. Certains modèles d'appliances SMA offrent l'équilibrage de charge dynamique pour affecter intelligemment les charges des sessions et allouer les licences utilisateurs en temps réel en fonction de la demande. Les entreprises n'ont pas besoin d'investir dans des équilibreurs de charge externes, ce qui réduit le coût initial.

Protégez-vous contre les événements imprévus

Pour être complète, une solution antisinistre et de continuité des activités doit être à même de traiter un pic important de trafic à distance, tout en conservant le niveau de sécurité et le contrôle des coûts. Les packs SonicWall Spike License pour SMA sont des licences complémentaires qui permettent aux entreprises distribuées de s'adapter au nombre d'utilisateurs et d'atteindre la capacité maximale instantanément, en vue de garantir la continuité des activités. Les licences Spike fonctionnent comme une police d'assurance destinée à couvrir tout pic d'activité futur, planifié ou non, nécessitant l'ajout de dizaines, voire de centaines d'utilisateurs supplémentaires.

Fonctionnalités

Authentification avancée

Authentification unique fédérée[2]	SMA utilise l'authentification SAML 2.0 pour assurer le SSO fédéré via un portail unique vers les ressources sur site et dans le cloud, tout en appliquant l'authentification multi-facteurs à plusieurs niveaux pour plus de sécurité.
Authentification multi-facteurs	Certificats numériques X.509 Certificats numériques côté serveur et côté client RSA SecurID, Dell Defender, Google Authenticator, Duo Security et autres jetons d'authentification par mot de passe unique/à deux facteurs Carte CAC (Common Access Card) Authentification double ou à plusieurs niveaux Prise en charge Captcha, nom d'utilisateur/mot de passe
Authentification SAML	SMA peut être configurée comme fournisseur d'identité (IdP) SAML, fournisseur de services (SP) SAML ou servir de proxy à un IdP sur site pour assurer le SSO fédéré via l'authentification SAML 2.0.
Référentiels d'authentification	SMA offre une intégration simple aux référentiels standard pour une gestion facilitée des comptes et mots de passe utilisateurs. Il est possible de définir des groupes d'utilisateurs dynamiquement à partir de référentiels d'authentification RADIUS, LDAP ou Active Directory, y compris les sous-groupes. Les attributs LDAP communs ou personnalisés peuvent être interrogés pour une autorisation spécifique ou la vérification de l'enregistrement de l'appareil.
Proxy applicatif des couches 3 à 7	SMA propose des options de proxy flexibles. Par exemple, un accès fournisseurs peut être fourni par proxy direct, un accès sous-traitants par proxy inverse et un accès employés à Exchange par ActiveSync.
Proxy inverse	Le service de proxy inverse étendu avec authentification permet aux administrateurs de configurer les signets et le portail de déchargement d'applications pour que les utilisateurs puissent se connecter de manière transparente aux ressources et applications distantes, RDP et HTTP inclus. Cette fonctionnalité est compatible avec tous les navigateurs, dont IE, Chrome et Firefox.
Délégation Kerberos contrainte	SMA prend en charge l'authentification par une infrastructure Kerberos existante qui n'a pas besoin de faire confiance aux services front-end pour déléguer un service.

Gestion des accès

Access Control Engine (ACE)	Les administrateurs octroient ou refusent l'accès en fonction de règles organisationnelles et définissent des actions correctives lors de la mise en quarantaine de sessions. Les règles ACE orientées objet se basent sur les éléments du réseau, les ressources, l'identité, l'appareil, l'application, les données et l'heure.
End Point Control (EPC)	EPC permet à l'administrateur d'appliquer des règles d'accès granulaires en fonction de l'état de santé de l'appareil connecté. Grâce à une intégration profonde dans le système d'exploitation, de nombreux éléments sont combinés pour la classification des types et l'évaluation du facteur de risque. L'interrogation EPC simplifie la configuration des profils d'appareils à partir d'une large liste prédéfinie d'antivirus, de pare-feux personnels et de solutions anti-spyware pour les platesformes Windows, Mac et Linux comprenant la version et l'applicabilité de la mise à jour du fichier de signature.
App Access Control (AAC)	Les administrateurs peuvent définir quelles applications mobiles spécifiques sont autorisées à accéder à quelles ressources sur le réseau par des tunnels applicatifs individuels. Les règles AAC sont exécutées aussi bien sur le client que le serveur pour une protection du périmètre robuste.

Sécurité supérieure

VPN SSL de couche 3	La gamme SMA x000 Series offre des fonctionnalités hautes performances de tunnelisation de couche 3 pour une grande variété de périphériques clients dans n'importe quel environnement.
Prise en charge du chiffrement	Durée de vie de la session configurable Méthodes de chiffrement : AES 128 + 256 bits, Triple DES, RC4 128 bits Méthodes de hachage : MD5, SHA-256, SHA-1 Elliptic Curve Digital Signature Algorithm (ECDSA)
Prise en charge des méthodes de chiffrement avancées	Les appliances SMA x000 offrent un système de sécurité solide prêt à l'emploi pour répondre aux exigences de conformité, avec des méthodes de chiffrement configurées par défaut. Les administrateurs peuvent les affiner dans une optique de performance, de renforcement de la sécurité ou de compatibilité.
Certifications de sécurité	FIPS 140-2 niveau 2, ICSA SSL-TLS
Partage de fichiers sécurisé	Blocage des attaques inconnues et zero-day comme les ransomwares au niveau de la passerelle avec correction automatisée. Les fichiers chargés à l'aide de terminaux non gérés avec accès sécurisé aux réseaux d'entreprise sont inspectés par Capture ATP, notre sandbox multimoteur cloud.
Web Application Firewall	Prévention des attaques de protocole et basées sur le Web contribuant à assurer la conformité des entreprises du secteur financier, de la santé, du commerce en ligne et autres avec le top 10 de l'OWASP et la norme PCI.
Détection Geo IP et protection contre les botnets	La détection Geo IP et la protection contre les botnets permet aux clients d'autoriser ou de restreindre l'accès des utilisateurs de différentes régions géographiques.

Expérience utilisateur intuitive

VPN permanent	Établit automatiquement une connexion sécurisée au réseau de l'entreprise sur des appareils Windows fournis par l'entreprise, en vue d'améliorer la sécurité et la visibilité du trafic et de garantir la conformité.
Détection sécurisée des réseaux (SND)	Le client VPN de SMA sensible au réseau détecte quand l'appareil n'est plus sur site et reconnecte automatiquement le VPN pour le désactiver dès que l'appareil retourne sur un réseau de confiance.
Accès sans client aux ressources	SMA fournit un accès sans client sécurisé aux ressources par des navigateurs HTML5 compatibles avec les protocoles RDP, ICA, VNC, SSH et Telnet.
Portail d'authentification unique	Le portail WorkPlace offre une vue unifiée conviviale et personnalisable pour l'accès sécurisé avec authentification unique (SSO, Single Sign-On) à toutes les ressources dans un environnement informatique hybride. Aucune connexion supplémentaire ni VPN n'est nécessaire.
Tunnelisation de couche 3	Les administrateurs peuvent choisir la séparation des flux ou appliquer le flux unique avec tunneling SSL/TLS et reprise ESP en option pour des performances maximales.
Explorateur de fichiers HTML5[1]	L'explorateur de fichiers moderne facilite l'accès au partage de fichiers pour les utilisateurs depuis n'importe quel navigateur Web.
Intégration aux plateformes mobiles	Mobile Connect est pris en charge par tous les systèmes d'exploitation, ce qui donne aux utilisateurs une flexibilité totale dans le choix de leurs appareils mobiles.

Capacité de récupération

Global Traffic Optimizer (GTO)	SMA offre un équilibrage de charge du trafic mondial avec zéro impact sur les utilisateurs. Le trafic est dirigé vers les datacenters les plus optimisés et les plus performants.
Haute disponibilité dynamique[2]	SMA offre la haute disponibilité en configuration active/passive et active/active déployée dans un seul datacenter ou dans plusieurs datacenters dispersés géographiquement.
Persistance de session universelle[1]	Les utilisateurs bénéficient d'une expérience fluide avec un basculement zéro impact. Si une appliance connaît une défaillance, le clustering intelligent de SMA réalloue les utilisateurs avec leurs données de sessions sans qu'ils aient besoin de s'identifier à nouveau.
Performances évolutives	Les performances des appliances SMA x000 peuvent évoluer de manière exponentielle par le déploiement de plusieurs appliances, ce qui élimine les points de défaillance uniques. Le clustering horizontal prend pleinement en charge la combinaison d'appliances SMA physiques et virtuelles.
Octroi dynamique de licences	Les licences utilisateurs n'ont plus besoin d'être appliquées individuellement aux appliances SMA. Les utilisateurs peuvent être distribués et réaffectés dynamiquement parmi les appliances gérées en fonction de la demande.

Gestion et surveillance centralisées

Central Management System (CMS)	CMS permet la gestion Web centralisée de toutes les fonctionnalités SMA.
Alertes personnalisées	Les alertes peuvent être configurées pour générer des traps SNMP surveillés par n'importe quel NMS (Network Management System) de l'infrastructure informatique. Les administrateurs peuvent également configurer des alertes pour les scans de fichiers Capture ATP et l'utilisation de disque pour un traitement immédiat.
Surveillance SONAR	SonicWall SONAR permet à l'administrateur informatique de diagnostiquer rapidement et facilement les problèmes d'accès et d'obtenir des renseignements utiles pour le dépannage.
Intégration SIEM	La sortie de données en temps réel vers des collecteurs SIEM centraux permet aux équipes de sécurité de corréler des activités événementielles pour comprendre le workflow de bout en bout d'un utilisateur ou d'une application en particulier. C'est essentiel pour la gestion des incidents de sécurité et l'analyse forensique.
Planificateur	Le planificateur permet aux utilisateurs de programmer les tâches de maintenance comme le déploiement des règles, la duplication des paramètres de configuration ou le redémarrage des services sans intervention manuelle.

Extensibilité

API de gestion	Les API de gestion offrent le contrôle administratif total de la programmation pour tous les objets au sein d'un environnement SMA unique ou CMS global.
API utilisateurs finaux	Les API utilisateurs finaux permettent le contrôle total de tout le workflow des terminaux, de l'ouverture de session et de l'authentification.
Authentification à deux facteurs (2FA)	SMA offre l'authentification à deux facteurs via l'intégration de solutions leaders de mots de passe à usage unique basés sur le temps (TOTP) comme Google Authenticator, Microsoft Authenticator, Duo security, etc.
Intégration MDM	SMA s'intègre aux principaux produits de gestion de la mobilité d'entreprise (EMM) comme Airwatch et Mobile Iron.
Intégration d'autres tiers	SMA s'intègre aux principaux fournisseurs du secteur comme OPSWAT pour offrir une protection avancée contre les menaces.

[1]*Disponible avec SMA OS 12.1 ou version supérieure*

[2]*Version étendue dans SMA 12.1*

Récapitulatif des fonctionnalités (comparaison par modèle)

Catégorie	Fonctionnalité	200	400	500v	6200	7200	9000	8200v
Débit	Sessions simultanées max.	50	250	250	2 000	10 000	20 000	5 000
	Débit SSL/TLS max.	100 Mbit/s	368 Mbit/s	186 Mbit/s	400 Mbit/s	3,75 Gbit/s	3,75 Gbit/s	1,58 Gbit/s
Accès client	Tunnel de couche 3	•	•	•	•	•	•	•
	Séparation des flux et flux unique	•	•	•	•	•	•	•
	VPN permanent	•	•	•	•	•	•	•
	Encapsulation ESP automatique	–	–	–	•	•	•	•
	HTML5 (RDP, VNC, ICA, SSH, Telnet, Network Explorer)	•	•	•	•	•	•	•
	Détection sécurisée des réseaux	–	–	–	•	•	•	•
	Explorateur de fichiers (CIFS/NFS)	•	•	•	•	•	•	•
	Citrix XenDesktop/XenApp	•	•	•	•	•	•	•
	VMware View	–	–	–	•	•	•	•
	Tunnel à la demande	–	–	–	•	•	•	•
	Extension Chrome/Firefox	–	–	–	•	•	•	•
	Prise en charge pour tunnel CLI	–	–	–	•	•	•	•
	Mobile Connect (iOS, Android, Chrome, Win 10, Mac OSX)	•	•	•	•	•	•	•
	NetExtender (Windows, Linux)	•	•	•	–	–	–	–
	Connect Tunnel (Windows, Mac OSX, Linux)	–	–	–	•	•	•	•
	Exchange ActiveSync	•	•	•	•	•	•	•
Accès mobile	VPN par application	–	–	–	•	•	•	•
	Contrôle applicatif	–	–	–	•	•	•	•
	Validation de l'identifiant d'application	–	–	–	•	•	•	•
Portail utilisateur	Branding	•	•	•	•	•	•	•
	Personnalisation	–	–	–	•	•	•	•
	Localisation	•	•	•	•	•	•	•
	Signets définis par l'utilisateur	•	•	•	•	•	•	•
	Prise en charge d'URL personnalisée	•	•	•	•	•	•	•
	Prise en charge des applications SaaS	–	–	–	•	•	•	•
Sécurité	FIPS 140-2	–	–	–	•	•	•	–
	ICSA SSL-TLS	–	–	–	•	•	•	•
	Algorithmes de chiffrement Suite B	–	–	–	•	•	•	•
	Interrogation EPC dynamique	•	•	•	•	•	•	•
	Contrôle d'accès à base de rôles (RBAC)	–	–	–	•	•	•	•
	Enregistrement des terminaux	•	•	•	•	•	•	•
	Partage de fichiers sécurisé (Capture ATP)	•	•	•	•	•	•	•
	Protection anti-malware Capture	–	–	–	•	•	•	•
	Quarantaine des terminaux	•	•	•	•	•	•	•
	Validation CRL OCSP	–	–	–	•	•	•	•
	Sélection du chiffrement	–	–	–	•	•	•	•
	PKI et certificats clients	•	•	•	•	•	•	•
	Filtrage Geo IP	•	•	•	–	–	–	–
	Filtrage des botnets	•	•	•	–	–	–	–
	Proxy	•	•	•	•	•	•	•
	Proxy inverse	•	•	•	•	•	•	•
Services d'authentification et d'identité	SAML 2.0	–	–	–	•	•	•	•
	LDAP, RADIUS	•	•	•	•	•	•	•
	Kerberos (KDC)	•	•	•	•	•	•	•
	NTLM	•	•	•	•	•	•	•
	Fournisseur d'identité SAML (IdP)	–	–	–	•	•	•	•
	Prise en charge des appareils biométriques	•	•	•	•	•	•	•
	Prise en charge de Face ID pour iOS	•	•	•	•	•	•	•
	Authentification à deux facteurs (2FA)	•	•	•	•	•	•	•
	Authentification multi-facteurs (MFA)	–	–	–	•	•	•	•

Récapitulatif des fonctionnalités (comparaison par modèle — suite)

Catégorie	Fonctionnalité	200	400	500v	6200	7200	9000	8200v
Services d'authentification et d'identité (suite)	Authentification chaînée	–	–	–	•	•	•	•
	Mot de passe à usage unique (OTP)	•	•	•	•	•	•	•
	Prise en charge Common Access Card (CAC)	–	–	–	•	•	•	•
	Prise en charge des certificats X.509	•	•	•	•	•	•	•
	Intégration Captcha	–	–	–	•	•	•	•
	Changement de mot de passe distant	•	•	•	•	•	•	•
	SSO à base de formulaires	•	•	•	•	•	•	•
	SSO fédéré	–	–	–	•	•	•	•
	Persistance de session	–	–	–	•	•	•	•
	Ouverture de session automatique	•	•	•	•	•	•	•
Contrôle d'accès	AD groupe	•	•	•	•	•	•	•
	Attributs LDAP	•	•	•	•	•	•	•
	Règles de géolocalisation	•	•	•	–	–	–	–
	Surveillance continue des terminaux	•	•	•	•	•	•	•
Dirigeants	Interface de gestion (Ethernet)	–	–	–	•	•	•	•
	Interface de gestion (console)	–	–	–	•	•	•	•
	Administration HTTPS	•	•	•	•	•	•	•
	Administration SSH	–	–	–	•	•	•	•
	MIB SNMP	•	•	•	•	•	•	•
	Syslog et NTP	•	•	•	•	•	•	•
	Surveillance de l'utilisation	•	•	•	•	•	•	•
	Rollback de configuration	•	•	•	•	•	•	•
	Gestion centralisée	–	–	–	•	•	•	•
	Reporting centralisé	–	–	–	•	•	•	•
	Gestion des API REST	–	–	–	•	•	•	•
	Authentification des API REST	–	–	–	•	•	•	•
	Comptabilité RADIUS	–	–	–	•	•	•	•
	Tâches programmées	–	–	–	•	•	•	•
	Octroi centralisé de licences de session	–	–	–	•	•	•	•
	Audit événementiel	–	–	–	•	•	•	•
Gestion de réseau	IPv6	•	•	•	•	•	•	•
	Équilibrage de charge global	–	–	–	•	•	•	•
	Équilibrage de charge des serveurs	•	•	•	–	–	–	–
	Réplication de l'état TCP	•	•	•	•	•	•	•
	Basculement de l'état du cluster	–	–	–	•	•	•	•
	Haute disponibilité active/passive	–	•	•	•	•	•	•
	Haute disponibilité active/active	–	–	–	•	•	•	•
	Évolutivité horizontale	–	–	–	•	•	•	•
	Un ou plusieurs FQDN	–	–	–	•	•	•	•
	Proxy tunnel intelligent des couches 3 à 7	•	•	•	•	•	•	•
	Proxy applicatif de couche 7	•	•	•	•	•	•	•
Intégration	Prise en charge 2FA pour appli. mobiles	•	•	•	•	•	•	•
	Prise en charge des produits EMM et MDM	–	–	–	•	•	•	•
	Prise en charge des produits SIEM	–	–	–	•	•	•	•
	Archivage de mots de passe TPAM	–	–	–	•	•	•	•
	Prise en charge de l'hyperviseur ESX	–	–	•	–	–	–	•
	Prise en charge de l'hyperviseur Hyper-V	–	–	–	–	–	–	•
Options de licence	Licence par abonnement	–	–	–	•	•	•	•
	Licence perpétuelle avec support	•	•	•	•	•	•	•
	Web Application Firewall (WAF)	•	•	•	–	–	–	–
	Licenses Spike	•	•	•	•	•	•	•
	Licences échelonnées	–	–	–	•	•	•	•
	Virtual Assist	•	•	•	–	–	–	–

** Pour en savoir plus sur les clients VPN, rendez-vous sur : https://www.sonicwall.com/en-us/products/remote-access/vpn-client*

SONICWALL®

Avantages de la mise à niveau vers des appliances haut de gamme

Meilleures performances | Débit accéléré | Fonctionnalités avancées | Meilleure évolutivité

Caractéristiques des appliances

Faites votre choix parmi une série d'appliances d'accès mobile sécurisé (SMA) spécialisées. Bénéficiez d'options de déploiement flexibles avec les appliances virtuelles et physiques.

Caractéristiques des appliances physiques

Performances	SMA 200	SMA 400	SMA 6200	SMA 7200	SRA EX9000
Sessions simultanées/utilisateurs	Jusqu'à 50	Jusqu'à 250	Jusqu'à 2 000	Jusqu'à 10 000	Jusqu'à 20 000
Débit VPN SSL* (avec nombre max. d'utilisateurs simultanés)	Jusqu'à 100 Mbit/s	Jusqu'à 368 Mbit/s	Jusqu'à 400 Mbit/s	Jusqu'à 3,75 Gbit/s	Jusqu'à 3,75 Gbit/s
Format	1 U	1 U	1 U	1 U	2 U
Dimensions	43 x 26 x 4,5 cm (16,92 x 10,23 x 1,75 in)	43 x 26 x 4,5 cm (16,92 x 10,23 x 1,75 in)	43 x 41,5 x 4,5 cm (17,0 x 16,5 x 1,75 in)	43 x 41,5 x 4,5 cm (17,0 x 16,5 x 1,75 in)	68,6 x 48,2 x 8,8 cm (27,0 x 18,9 x 3,4 in)
Poids de l'appliance	5 kg (11 lb)	5 kg (11 lb)	7,3 kg (16 lb)	8,3 kg (18,3 lb)	22,3 kg (49,1 lb)
Accélération du chiffrement des données (AES-NI)	NON	NON	OUI	OUI	OUI
Port de gestion dédiée	NON	NON	OUI	OUI	OUI
Accélération SSL	NON	NON	OUI	OUI	OUI
Stockage	2 Go (mémoire Flash)	2 Go (mémoire Flash)	2 X 500 Go SATA	2 X 500 Go SATA	2 X 2 To SATA
Interfaces	(2) GB Ethernet, (2) USB, (1) console	(4) GB Ethernet, (2) USB, (1) console	6 (6 ports 1 GE)	8 (6 ports 1 GE + 2 ports 10 Gb SFP+)	12 (8 ports 1 GE + 4 ports 10 Gb SFP+)
Mémoire	2 Go	4 Go	8 Go DDR3	16 Go DDR3	32 Go DDR3
Puce TPM	NON	NON	OUI	OUI	NON
Processeur	2 cœurs	4 cœurs	4 cœurs	4 cœurs	2 X 4 cœurs
Temps de fonctionnement entre deux pannes (à 25 °C ou 77 °F) en heures	61 815	60 151	200 064	233 892	129 489
Fonctionnement et conformité	**SMA 200**	**SMA 400**	**SMA 6200**	**SMA 7200**	**SRA EX9000**
Alimentation	Système d'alimentation fixe	Système d'alimentation fixe	Système d'alimentation fixe	Système d'alimentation double, remplaçable à chaud	Système d'alimentation double, remplaçable à chaud
Valeurs d'entrée	100-240 V CA, 50-60 MHz	100-240 V CA, 50-60 MHz	100-240 V CA, 1,1 A	100-240 V CA, 1,79 A	100-240 V CA, 2,85 A
Consommation	26,9 W	31,9 W	78 W	127 W	320 W
Dissipation thermique totale	92 BTU	109 BTU	266 BTU	432 BTU	1091 BTU
Environnement	DEEE, EU RoHS, China RoHS				
Choc à l'arrêt	110 g, 2 msec				
Émissions	FCC, ICES, CE, C-Tick, VCCI ; MIC				
Sécurité	TÜV/GS, UL, CE PSB, CCC, BSMI, CB Scheme				
Température de fonctionnement	0 à 40 °C (32 à 104 °F)				
Certification FIPS	NON	NON	FIPS 140-2 niveau 2 avec protection anti-piratage		

** Le débit peut varier en fonction du déploiement et de la connectivité. Les chiffres communiqués sont basés sur les conditions internes au laboratoire.*

Caractéristiques des appliances virtuelles

Caractéristiques	SMA 500v (ESX/ESXI)	SMA 8200v (ESX/ESXI)	SMA 8200v (Hyper-V)
Sessions simultanées	Jusqu'à 250 utilisateurs	Jusqu'à 5000	Jusqu'à 250
Débit VPN SSL* (avec nombre max. d'utilisateurs simultanés)	Jusqu'à 186 Mbit/s	Jusqu'à 1,58 Gbit/s	Jusqu'à 1,2 Gbit/s
Mémoire allouée	2 Go	8 Go	
Processeur	1 cœur	4 cœurs	
Accélération SSL	NON	OUI	
Taille de disque appliquée	2 Go	64 Go (par défaut)	Configurable par l'administrateur
Système d'exploitation installé	Linux	Linux renforcé	
Port de gestion dédiée	NON	OUI	

** Le débit peut varier en fonction du déploiement et de la connectivité. Les chiffres communiqués sont basés sur les conditions internes au laboratoire. SMA 8200v sur Hyper-V peut gérer jusqu'à 5 000 sessions concurrentes et fournit jusqu'à 1,58 Gbit/s de débit VPN SSL lorsque SMA OS 12.1 fonctionne avec Windows Server 2016.*

Informations de commande

RÉFÉRENCE	APPLIANCE SONICWALL SECURE MOBILE ACCESS (SMA)
01-SSC-2231	SMA 200 avec 5 licences utilisateurs
01-SSC-2243	SMA 400 avec 25 licences utilisateurs
01-SSC-8469	SMA 500v avec 5 licences utilisateurs
01-SSC-2301	SMA 7200 avec licence d'essai administrateur
01-SSC-2300	SMA 6200 avec licence d'essai administrateur
01-SSC-9574	SRA EX9000 appliance de base
01-SSC-8468	SMA 8200v (appliance virtuelle)
RÉFÉRENCE	**LICENCES UTILISATEURS SONICWALL SMA**
01-SSC-9182	Ajout de 5 utilisateurs SMA 500V (aussi disponible pour SMA 200)
01-SSC-2414	Ajout de 100 utilisateurs SMA 500V (aussi disponible pour SMA 400)
01-SSC-7856	Licence 5 utilisateurs SMA – extensible pour 6200, 7200, EX9000, 8200v
01-SSC-7860	Licence 100 utilisateurs SMA – extensible pour 6200, 7200, EX9000, 8200v
01-SSC-7865	Licence 5 000 utilisateurs SMA – extensible pour 7200, EX9000, 8200v
01-SSC-5286	Licence 5 utilisateurs HA SMA – extensible pour 6200, 7200, EX9000
01-SSC-5290	Licence 100 utilisateurs HA SMA – extensible pour 6200, 7200, EX9000
01-SSC-5295	Licence 5 000 utilisateurs HA SMA – extensible pour 7200, EX9000
RÉFÉRENCE	**CONTRAT DE SUPPORT SONICWALL SMA**
01-SSC-9188	Support 8x5 pour SMA 500V jusqu'à 25 utilisateurs 1 an (aussi disponible pour SMA 200 et 400)
01-SSC-9191	Support 24x7 pour SMA 500V jusqu'à 25 utilisateurs 1 an (aussi disponible pour SMA 200 et 400)
01-SSC-8434	Support 24x7 pour SMA 8200V 5 utilisateurs 1 an – extensible (aussi disponible pour SMA 6200, 7200 et EX9000)
01-SSC-8446	Support 24x7 pour SMA 8200V 100 utilisateurs 1 an – extensible (aussi disponible pour SMA 6200, 7200 et EX9000)
01-SSC-7913	Support 24x7 pour SMA 8200V 5000 utilisateurs 1 an – extensible (aussi disponible pour SMA 6200, 7200 et EX9000)
RÉFÉRENCE	**GESTION CENTRALISÉE POUR 6200, 7200, EX9000, 8200V**
Licence pour appliance CMS	
01-SSC-8535	Base CMS + 3 licences d'appliances (gratuites, pour essai et utilisation avec licences utilisateurs par abonnement)
01-SSC-8536	Licence CMS 100 appliances 1 an (pour utilisation avec licences utilisateurs par abonnement)
01-SSC-3369	Base CMS + 3 appliances (gratuites, pour utilisation avec licences utilisateurs perpétuelles)
01-SSC-3402	Licence CMS 100 appliances 1 an (pour utilisation avec licences utilisateurs perpétuelles)
Licences utilisateurs centralisées (abonnement)	
01-SSC-2298	Licences mutualisées CMS 10 utilisateurs 1 an
01-SSC-8539	Licences mutualisées CMS 1000 utilisateurs 1 an
01-SSC-5339	Licences mutualisées CMS 50000 utilisateurs 1 an
Licences utilisateurs centralisées (perpétuelles)	
01-SSC-2053	Licence perpétuelle CMS 10 utilisateurs
01-SSC-2058	Licence perpétuelle CMS 1 000 utilisateurs
01-SSC-2063	Licence perpétuelle CMS 50 000 utilisateurs
Support pour licences utilisateurs centralisées (perpétuelles)	
01-SSC-2065	Support 24x7 CMS 1 an 10 utilisateurs
01-SSC-2070	Support 24x7 CMS 1 an 1 000 utilisateurs
01-SSC-2075	Support 24x7 CMS 1 an 50 000 utilisateurs

Informations de commande (suite)

Licences ActiveSync centralisées (abonnement)	
01-SSC-2088	Licence e-mail mutualisée CMS 10 utilisateurs 1 an
01-SSC-2093	Licence e-mail mutualisée CMS 1 000 utilisateurs 1 an
01-SSC-2087	Licence e-mail mutualisée CMS 50 000 utilisateurs 1 an
Licences Spike centralisées	
01-SSC-2111	CMS Spike 1 000 utilisateurs 5 jours
01-SSC-2115	CMS Spike 50 000 utilisateurs 5 jours
Module complémentaire Capture (abonnement)	
01-SSC-2116	CMS Capture essai 1 an pour SMA
** Le support 24X7 est inclus dans les licences par abonnement*	
RÉFÉRENCE	**MODULES COMPLÉMENTAIRES SONICWALL SMA**
01-SSC-2406	Module complémentaire SMA 7200 FIPS
01-SSC-2405	Module complémentaire SMA 6200 FIPS
01-SSC-9185	Web Application Firewall SMA 500V 1 an (aussi disponible pour SMA 200 et 400)
RÉFÉRENCE	**MODULES COMPLÉMENTAIRES SONICWALL SMA**
01-SSC-5967	Virtual Assist 1 intervention simultanée max. (SMA 200, 400, 500v)
01-SSC-5971	Virtual Assist jusqu'à 10 interventions simultanées (SMA 200, 400, 500v)
RÉFÉRENCE	**LICENCE SPIKE POUR SMA (NOMBRE VARIABLE POUR ATTEINDRE LA CAPACITÉ NÉCESSAIRE)**
01-SSC-2240	SMA 200 licence Spike 10 jours 50 utilisateurs (aussi disponible pour SMA 400 et 500v)
01-SSC-7873	SMA 8200v licence Spike 10 jours -2 500 utilisateurs (aussi disponible pour SMA 6200, 7200 et EX9000)

** Des références et contrats de support pluriannuels sont également disponibles. Pour obtenir la liste complète des références, veuillez contacter votre revendeur ou votre responsable commercial.*

À propos de nous

SonicWall s'engage depuis plus de 25 ans dans la lutte contre la cybercriminalité, défendant PME et grands comptes dans le monde entier. Notre alliance de produits et de partenaires nous a permis de mettre sur pied une solution de cyberdéfense en temps réel, adaptée aux besoins spécifiques de plus de 500 000 entreprises dans plus de 150 pays, leur permettant de se concentrer sans crainte sur leur cœur de métier.

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

Datasheet-SecureMobileAccess-US-KJ-MKTG3047