SONICWALL

SONICWALL SECURE MOBILE ACCESS (SMA)

Sécuriser partout et à tout instant l'accès aux ressources de l'entreprise dans des environnements multi-cloud en fonction de l'identité, du lieu et de la confiance des utilisateurs et des appareils.

SonicWall SMA offre une passerelle d'accès sécurisée unifiée qui permet aux entreprises de fournir un accès à tout moment, n'importe où et pour n'importe quel appareil, aux ressources essentielles de l'entreprise. Le moteur de règles de contrôle granulaire des accès de SMA, l'autorisation contextuelle d'appareils, le VPN au niveau applicatif et l'authentification avancée par SSO donnent aux entreprises les moyens nécessaires pour adopter le BYOD et la mobilité dans les environnements informatiques multi-cloud.

Mobilité et BYOD
Dès lors que les entreprises envisagent d'adopter le BYOD, des méthodes de travail flexibles ou encore un accès tiers, la série SMA devient un outil incontournable. SMA fournit une sécurité optimale pour réduire les menaces de surface, tout en rendant les organisations plus sécurisées en prenant en charge les derniers algorithmes et codes de chiffrement. La solution SMA de SonicWall permet aux administrateurs de fournir un accès mobile sécurisé et des privilèges basés sur l'identité pour que les utilisateurs finaux puissent bénéficier d'un accès simple et rapide aux applications, données et ressources d'entreprise nécessaires. 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
Les entreprises qui optent pour la migration vers le Cloud disposent avec SMA d'une infrastructure SSO (Single Sign-on) basée sur un portail Web unique pour l'authentification des utilisateurs dans un environnement informatique hybride. Que les ressources de l'entreprise se trouvent sur site, sur le Web ou dans un Cloud hébergé, l'expérience d'accès est cohérente et transparente. Pour plus de sécurité, la solution SMA s'intègre également aux technologies d'authentification multifacteurs leaders de l'industrie.

Fournisseurs de services gérés
Aux entreprises disposant de centres de données ou aux fournisseurs de services gérés, SMA fournit une solution clé en main garantissant un niveau élevé de continuité des activités et d'évolutivité. La technologie SMA permet de prendre en charge jusqu'à 20 000 connexions simultanées sur une seule appliance, avec possibilité d'évolution jusqu'à des centaines de milliers d'utilisateurs grâce au clustering intelligent. Réduisez les coûts des centres de données grâce au clustering actif/actif et à un équilibreur de charge dynamique intégré, qui réalloue le trafic global au centre de données le plus adéquat et ce, en temps réel, à la demande de l'utilisateur. Les ensembles d'outils SMA permettent aux prestataires de services de fournir des services sans interruption, ce qui leur permet de respecter des accords SLA très stricts.

La solution SMA donne aux départements informatiques les moyens d'offrir la meilleure expérience et l'accès le plus sécurisé selon le scénario d'utilisation. Disponible sous la forme d'appliances physiques renforcées ou d'appliances virtuelles puissantes, SMA s'intègre parfaitement à l'infrastructure existante sur site/cloud. Les entreprises peuvent choisir entre diverses possibilités d'accès sécurisé entièrement sans client, via le Web, pour les tiers ou les employés sur des appareils personnels, ou un accès plus classique sur client par tunnel VPN pour les dirigeants sur tous les types d'appareils. Qu'il s'agisse de fournir un accès sécurisé fiable à cinq utilisateurs d'un même emplacement ou à des milliers d'utilisateurs répartis dans des réseaux du monde entier, SonicWall SMA a une solution.

SonicWall SMA permet aux organisations d'adopter la mobilité et le BYOD sans crainte, et de passer facilement au cloud. SMA responsabilise les effectifs et leur fournit une expérience d'accès cohérente.

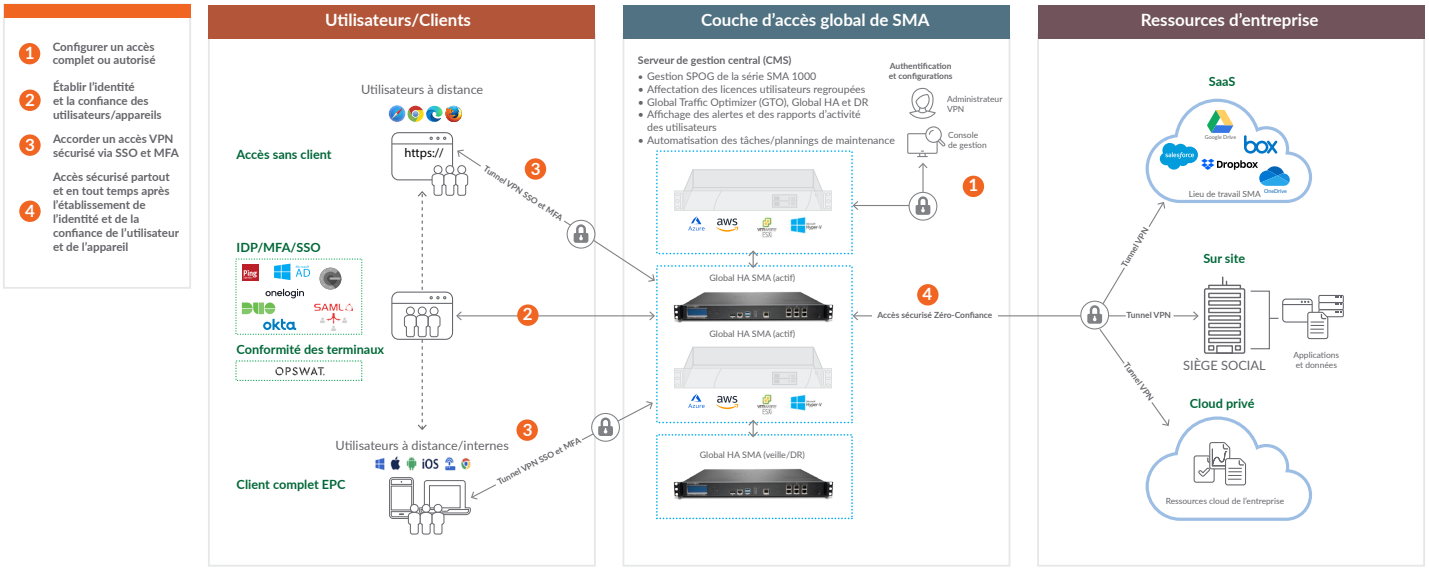
Avantages :

- Accès unifié à tous les réseaux et ressources cloud pour un accès sécurisé « à tout moment, sur tout appareil et toute application »
- Contrôler qui a accès à quelles ressources en définissant des règles granulaires avec le solide moteur de contrôle d'accès
- Augmenter la productivité en fournissant une authentification unique centralisée à n'importe quelle application SaaS ou hébergée localement avec une seule URL
- Réduire le coût total de possession et la complexité de la gestion des accès en regroupant les composants de l'infrastructure dans un environnement informatique hybride
- Obtenir de la visibilité sur chaque dispositif de connexion et accorder l'accès en fonction des règles et de l'état du terminal
- Prévenir les compromissions de logiciels malveillants en scannant tous les fichiers téléchargés dans votre réseau avec la technologie sandbox de Capture ATP
- Protéger contre les attaques basées sur le Web et garantir la conformité PCI avec l'extension Web Application Firewall
- Arrêter les attaques par déni de service (DDoS) et zombies avec filtrage GeoIP et protection contre les réseaux de zombies
- Obtenir une fonctionnalité d'agent native sécurisée en utilisant l'accès HTML5 sans client basé sur un navigateur Web sans les frais d'installation et de maintenance des agents sur les terminaux
- Obtenir les connaissances pratiques dont vous avez besoin pour prendre les bonnes décisions avec un suivi en temps réel et des rapports exhaustifs
- Opter pour un déploiement en tant qu'appliance physique ou virtuelle dans des clouds privés comme ESXi ou Hyper-V, ou dans des environnements cloud publics AWS ou Microsoft Azure
- Permettre la délivrance dynamique de licences d'accès sur la base de la demande en temps réel, avec une direction automatisée des terminaux vers la connexion la plus performante à latence la plus faible
- Réduire les coûts initiaux avec l'équilibrage de charge intégré sans matériel ni services supplémentaires, tout en offrant le basculement des appliances sans aucun impact pour les utilisateurs
- Remédier aux perturbations d'entreprise ou aux pics saisonniers en augmentant instantanément la capacité

Déploiement de SMA

Une passerelle de périphérie renforcée pour un accès sécurisé à tout moment, n'importe où et sur n'importe quel appareil

SMA offre un accès à distance complet et sécurisé de bout en bout aux ressources de l'entreprise hébergées dans les centres de données sur site, dans le cloud et hybrides. Elle applique des contrôles d'accès basés sur l'identité et basés sur des règles, une authentification contextuelle de l'appareil et un VPN au niveau applicatif pour accorder l'accès aux données, aux ressources et aux applications après avoir établi l'identité, l'emplacement et la confiance de l'utilisateur et de l'appareil. Elle peut être facilement déployée en tant qu'appliance Linux renforcée ou qu'appliance virtuelle dans des clouds privés comme ESXi ou Hyper-V, ou dans des environnements cloud publics AWS ou Microsoft Azure.



Déploiement SMA cloud/sur site

Déploiement flexible avec des 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. Pour les entreprises appartenant à des secteurs réglementés et les organismes publics, la solution SMA est également disponible avec la certification FIPS 140-2 niveau 2. Les appliances virtuelles SMA offrent la même robustesse fonctionnelle de l'accès sécurisé sur les principales plateformes virtuelles ou sur le cloud, comme Microsoft Hyper-V, VMware ESX, et AWS.

Des licences utilisateurs partagées sur les appliances

Les entreprises disposant d'appliances réparties dans le monde entier peuvent bénéficier des demandes fluctuantes de licences utilisateur en raison des différences d'heures. Qu'une entreprise déploie des licences VPN complètes ou des licences ActiveSync de base, la gestion centrale de SMA réaffecte les licences aux appliances gérées où les demandes des utilisateurs ont atteint un pic à partir d'appliances situées dans une zone géographique différente, où l'utilisation a diminué en raison des heures de repos/de nuit.

Visibilité réseau avec profilage contextuel des appareils

L'authentification contextuelle de pointe ne donne accès qu'aux appareils de confiance et aux utilisateurs autorisés. Les ordinateurs portables et PC sont également interrogés sur la présence ou l'absence de logiciels de sécurité, de certificats clients et d'ID d'appareil. Les appareils mobiles sont interrogés pour obtenir des informations de sécurité essentielles telles que le statut « jailbreak » ou « root », l'ID de l'appareil, le statut du certificat et les versions du système d'exploitation avant d'accorder l'accès. Les appareils qui ne répondent pas aux exigences des règles ne sont pas autorisés à accéder au réseau et l'utilisateur est informé de la non-conformité.

Expérience cohérente à partir d'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, donnant aux utilisateurs une seule et même URL pour accéder à toutes les applications vitales, avec un simple navigateur Web. Une fois que l'utilisateur se connecte avec un navigateur, un portail d'utilisateur Web personnalisable s'affiche dans la fenêtre du navigateur, offrant une vue unique depuis un seul et même écran pour accéder à n'importe quelle application SaaS ou locale. Le portail affiche uniquement des liens et des signets personnalisés pertinents pour le terminal, l'utilisateur ou le groupe concerné. Le portail fonctionne sur toutes les plateformes et prend en charge toutes les grandes plateformes d'appareils, y compris les appareils Windows, Mac OS, Linux, iOS et Android, ainsi qu'une large prise en charge du navigateur sur tous ces appareils.

Authentification unique centralisée pour les applications SaaS et locales

Éliminez le besoin de plusieurs mots de passe et arrêtez les mauvaises pratiques de sécurité, telles que la réutilisation des mots de passe. SMA fournit une authentification unique centralisée aux applications SaaS hébergées dans le cloud et aux applications hébergées sur le campus. SMA est compatible avec différents serveurs d'authentification, d'autorisation et de comptes ainsi qu'avec les principales technologies d'authentification multifacteurs, pour davantage de sécurité. Le SSO sécurisé n'est attribué qu'aux terminaux autorisés, à l'issue de contrôles par

SMA concernant l'état de santé et de conformité des terminaux. Le moteur de règles d'accès garantit que les utilisateurs ne peuvent voir que les applications autorisées et accorde l'accès après une authentification réussie. La solution prend en charge les SSO centralisés même en cas d'utilisation de clients VPN, offrant aux clients une expérience d'authentification transparente, qu'ils utilisent un accès sécurisé basé ou non sur un client.

Prévenir les violations et les menaces avancées

SonicWall SMA ajoute une couche de sécurité d'accès pour améliorer votre position de sécurité et réduire la zone d'attaque des menaces.

- SMA s'intègre à la technologie sandbox multimoteur SonicWall Capture ATP basée sur le cloud pour scanner tous les fichiers téléchargés par les utilisateurs avec des terminaux non gérés, ou par ceux qui ne sont pas connectés au réseau de l'entreprise. Cela garantit aux utilisateurs le même niveau de protection contre les menaces avancées, telles que les ransomware ou les logiciels malveillants de type « zero-day », qu'ils soient en déplacement ou au bureau[1].
- Le service de pare-feu SonicWall Web Application Firewall offre aux entreprises une solution abordable et bien intégrée pour sécuriser les applications Web internes. Cela permet aux clients de garantir la confidentialité des données, et les services Web internes restent intacts en cas d'accès d'utilisateur malveillant ou non autorisé.
- Le filtrage GeoIP et la détection de réseaux de zombies protègent les entreprises contre les attaques par déni de service (DDoS) et les attaques zombies, ainsi que contre les terminaux compromis fonctionnant comme des botnets.

Accès transparent et sécurisé basé sur un navigateur sans client

La nature « sans client » du SonicWall SMA signifie que l'administrateur n'a pas besoin d'installer manuellement un composant client lourd sur un ordinateur qui sera utilisé pour un accès à distance. Cela élimine toute dépendance vis-à-vis de Java et supprime des frais généraux pour l'informatique, élargissant ainsi considérablement le concept d'accès à distance. Ainsi, comme il n'y a pas de pré-installation ou de pré-configuration nécessaire, un employé à distance autorisé peut s'installer sur n'importe quel ordinateur, n'importe où dans le monde, et accéder en toute sécurité aux ressources de l'entreprise. Dans sa forme la plus pure, l'accès sécurisé est strictement basé sur le navigateur HTML5, offrant une expérience homogène et unifiée aux utilisateurs.

Offrir une expérience « Always On »

Pour une expérience utilisateur fluide, SMA fournit un VPN « Always On » pour les appareils Windows gérés. Les administrateurs peuvent configurer les paramètres pour établir automatiquement une connexion VPN chaque fois qu'un terminal client autorisé détecte un réseau public ou non fiable. Un seul événement de connexion à l'appareil Windows permet à l'utilisateur de se connecter en toute sécurité aux ressources de l'entreprise. Les utilisateurs n'ont pas besoin de se connecter à leurs clients VPN ou de conserver des mots de passe supplémentaires. Cela offre une expérience fluide aux utilisateurs mobiles pour accéder aux ressources essentielles comme s'ils étaient au bureau et permet aux administrateurs informatiques de garder le contrôle sur les appareils gérés, améliorant ainsi la position de sécurité de l'entreprise.

Gestion intuitive et rapports exhaustifs

SonicWall propose une plateforme de gestion Web intuitive, Central Management Server (CMS), qui simplifie la gestion des appliances tout en fournissant un vaste éventail de fonctionnalités de reporting. L'interface utilisateur conviviale met de la clarté dans la gestion d'une ou de plusieurs appliances et règles. Chaque page montre comment les paramètres sont configurés sur toutes les machines sous gestion. 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 par vos utilisateurs, appareils et applications, aux données, serveurs et réseaux. Le service informatique peut automatiser les tâches routinières et les activités planifiées. Ainsi, au lieu de perdre du temps à des travaux répétitifs, vos équipes de sécurité peuvent se concentrer sur les tâches stratégiques, comme la réponse aux incidents. Le service informatique acquiert des informations sur les tendances d'accès des utilisateurs et la santé du système dans son ensemble grâce à des rapports faciles à utiliser et une journalisation centralisée.

Garantir une disponibilité des services 24 h sur 24, 7 j/7

Les entreprises ont des exigences pour maintenir leurs services et faire en sorte qu'ils restent opérationnels avec un degré élevé de fiabilité afin de fournir un accès sécurisé aux applications essentielles en tout temps. Les appliances SMA prennent en charge le mode haute disponibilité (HA) actif-passif traditionnel pour les entreprises avec des centres de données uniques, ou la HA globale avec un clustering actif-actif ou actif-passif pour les centres de données locaux ou distribués. Les deux modèles HA offrent une expérience harmonieuse aux utilisateurs avec un basculement sans impact et une persistance de session.

Déployer le client VPN adapté à vos besoins

Choisissez parmi un large éventail de clients VPN pour fournir un accès à distance sécurisé basé sur les règles pour divers terminaux, y compris les ordinateurs portables, smartphones et tablettes.

Clients VPN	Système d'exploitation pris en charge	Modèle SMA pris en charge	Points forts
Mobile Connect	iOS, OS X, Android, Chrome OS, Windows 10	Tous les modèles	Fournir une authentification biométrique, des VPN par appli et l'application du contrôle des terminaux
Connect Tunnel (Client léger)	Windows, Mac OS et Linux	6200, 6210, 7200, 7210, 8200v, 9000	Offrir une expérience complète comme « au bureau » avec un contrôle rigoureux des terminaux
NetExtender (Client léger)	Windows et Linux	210, 410, 500v	Appliquer des règles d'accès granulaires et étendre l'accès au réseau via des clients natifs

Réduction des coûts initiaux avec équilibreur de charge intégré

La fonctionnalité d'équilibrage de charge intégrée à l'appliance SMA atteint le niveau d'évolutivité attendu pour les déploiements de moyennes entreprises et d'entreprises. Certains modèles d'appliances SMA offrent un équilibrage dynamique des charges pour assigner intelligemment les charges de session et attribuer les licences utilisateur en temps réel en fonction de la demande. Les entreprises n'ont pas besoin d'investir dans des équilibreurs de charge externes, réduisant ainsi les coûts initiaux.

Se protéger contre les imprévus

Une solution complète de continuité d'activité et de reprise après sinistre doit être capable de gérer un pic significatif du trafic d'accès à distance, tout en maintenant la sécurité et le contrôle des coûts. Les packs de licences SonicWall Spike pour le SMA sont des licences complémentaires qui permettent aux entreprises distribuées d'augmenter le nombre d'utilisateurs et d'atteindre une capacité maximale instantanément, ce qui permet une continuité d'activité fluide. Les licences Spike fonctionnent comme une police d'assurance pour tous les pics d'utilisation futurs, planifiés ou non, allant du nombre d'utilisateurs actuels à des dizaines, voire des centaines d'utilisateurs supplémentaires.

Fonctionnalités

Authentification avancée

Authentification unique centralisée[2]	SMA utilise l'authentification SAML 2.0 pour permettre l'authentification unique centralisée via un portail unique pour accéder aux ressources sur site et dans le cloud, tout en appliquant une authentification multifacteurs renforcée pour plus de sécurité.
Authentification multifacteurs	Certificats numériques X.509 Certificats numériques côté serveur et côté client RSA SecurID, Dell Defender, Google Authenticator, Duo Security et autres jetons d'authentification à deux facteurs/mot de passe à usage unique Carte CAC (Common Access Card) Authentification double ou empilée Prise en charge des captcha, nom d'utilisateur/mot de passe
Authentification SAML	SMA peut être configuré en tant que fournisseur d'identité SAML (IdP), prestataire de services SAML (SP) ou proxy d'un IdP sur site existant pour activer l'authentification unique centralisée (SSO) à l'aide de l'authentification SAML 2.0.
Répertoires d'authentification	SMA propose des intégrations simples avec des répertoires industriels standard pour une gestion aisée des comptes utilisateurs et des mots de passe. Les groupes d'utilisateurs peuvent être alimentés dynamiquement à partir des répertoires d'authentification RADIUS, LDAP ou Active Directory, y compris les groupes imbriqués. Les attributs LDAP communs ou personnalisés peuvent être interrogés pour une autorisation spécifique ou une vérification de l'enregistrement de l'appareil.
Proxy d'application sur les couches 3 à 7	SMA fournit des options de proxy flexibles, par exemple l'accès des fournisseurs peut être accordé par proxy direct, l'accès des sous-traitants par proxy inverse et l'accès des employés à Exchange via ActiveSync.
Proxy inverse	Le service de proxy inverse amélioré avec authentification permet aux administrateurs de configurer le portail de déchargement des applications et les signets, permettant aux utilisateurs de se connecter de manière transparente aux applications et aux ressources à distance, y compris RDP et HTTP. Cette fonctionnalité prend en charge tous les navigateurs, y compris IE, Chrome et Firefox.
Délégation limitée de Kerberos	SMA fournit un support d'authentification en utilisant une infrastructure Kerberos existante, qui n'a pas besoin de faire confiance aux services utilisateurs pour déléguer un service.

Gestion des accès

Moteur de contrôle d'accès (ACE)	Les administrateurs accordent ou refusent l'accès en fonction des règles de l'entreprise et définissent des mesures correctives lors de la mise en quarantaine des sessions. La règle basée sur les objets ACE utilise des éléments de réseau, de ressource, d'identité, d'appareil, d'application, de données et de temps.
Contrôle du terminal (EPC)	EPC permet à l'administrateur d'appliquer des règles de contrôle d'accès granulaires basées sur l'état de santé du dispositif de connexion. Avec l'intégration profonde du système d'exploitation, de nombreux éléments sont combinés pour la classification des types et l'évaluation des facteurs de risque. L'interrogation EPC simplifie la configuration des profils d'appareil à l'aide d'une liste complète et prédéfinie de solutions antivirus, de pare-feu personnels et d'anti-espions pour les plateformes Windows, Mac et Linux, y compris la version et l'applicabilité de la mise à jour du fichier de signature.
Contrôle d'accès aux applications (AAC)	Les administrateurs peuvent définir quelles applications mobiles spécifiques sont autorisées à accéder à quelles ressources sur le réseau via des tunnels d'applications individuels. Les règles AAC sont appliquées à la fois chez le client et le serveur, offrant une solide protection du périmètre.

Sécurité supérieure

VPN SSL de couche 3	La série SMA fournit des capacités de tunnellisation de couche 3 haute performance à une grande variété d'appareils clients fonctionnant dans n'importe quel environnement.
Prise en charge cryptographique	Longueur de session paramétrable Codes de chiffrement : AES 128 + 256 bits, Triple DES, RC4 128 bits Hachage : SHA-256 Algorithme de signature numérique à courbes elliptiques (ECDSA)
Prise en charge des codes de chiffrement avancés	Les appliances SMA offrent une position de sécurité hors norme pour la conformité, avec des codes de chiffrement de configuration par défaut, et les administrateurs peuvent affiner davantage en termes de performance, de degré de sécurité ou de compatibilité.
Certifications de sécurité	Certifié FIPS 140-2 Niveau 2, ICSA SSL-TLS, En cours pour Critères Communs, UC-APL
Partage de fichier sécurisé	Bloquer les attaques inconnues « zero-day » comme les ransomware, à la passerelle avec rectification automatique. Les fichiers téléchargés à l'aide de terminaux non gérés avec accès sécurisé aux réseaux d'entreprise sont inspectés par notre technologie Capture ATP multimoteur basée sur le cloud.
Web Application Firewall (WAF)	Prévenir les attaques basées sur le protocole et le Web, en aidant les entreprises des finances, de la santé, du commerce électronique et d'autres entreprises à atteindre le Top 10 OWASP et la conformité PCI.
Filtrage Geo IP et protection contre les réseaux de zombies	Le filtrage Geo IP et la protection contre les réseaux de zombies permettent aux clients disposant d'un mécanisme d'autoriser ou de restreindre l'accès des utilisateurs à partir de différents emplacements géographiques.
Prise en charge de TLS 1.3	Améliorer la sécurité et les performances tout en réduisant la complexité par rapport à ses prédécesseurs.

Expérience utilisateur intuitive

VPN « Always On »	Établir automatiquement une connexion sécurisée au réseau de l'entreprise à partir des appareils Windows fournis par l'entreprise afin d'améliorer la sécurité, d'obtenir une visibilité du trafic et de rester en conformité.
Détection réseau sécurisée (SND)	Le client VPN compatible réseau de la solution SMA détecte lorsque l'appareil est hors campus et reconnecte automatiquement le VPN, le désactivant à nouveau lorsque l'appareil revient sur un réseau de confiance.
Un accès aux ressources sans client	La solution SMA fournit un accès sécurisé et sans client aux ressources via des agents de navigateur HTML5 fournissant les protocoles RDP, ICA, VNC, SSH et Telnet.
Portail d'authentification unique	Le portail WorkPlace fournit un seul et même écran, simple d'utilisation et personnalisable, pour un accès sécurisé avec authentification unique (SSO) à toute ressource dans un environnement informatique hybride. Aucune connexion ou VPN supplémentaire n'est nécessaire.
Tunnellisation de couche 3	Les administrateurs peuvent choisir le mode « Split-Tunnel » ou appliquer le mode « Redirect-All » avec la tunnellisation SSL/TLS et la solution de repli ESP en option pour une performance maximale.
Explorateur de fichiers HTML5[1]	Un navigateur de fichiers moderne permet aux utilisateurs d'accéder facilement aux partages de fichiers à partir de n'importe quel navigateur Web.
Intégration d'un système d'exploitation mobile	Mobile Connect est pris en charge sur toutes les plateformes de système d'exploitation offrant aux utilisateurs une flexibilité totale dans le choix des appareils mobiles.

Résilience

Global Traffic Optimizer (GTO)	SMA offre aux utilisateurs un équilibrage global de la charge de trafic sans impact. Le trafic est acheminé vers le centre de données le plus optimisé et le plus performant.
Haute disponibilité dynamique[2]	La solution SMA prend en charge la configuration active/passive et offre une configuration active/active pour une haute disponibilité, qu'elle soit déployée sur un seul centre de données ou sur plusieurs centres de données géographiquement dispersés.
Persistance de session universelle[1]	Offrir aux utilisateurs une expérience fluide avec un basculement sans impact. En cas de mise hors ligne d'une appliance, le clustering intelligent de SMA réaffecte les utilisateurs avec leurs données de session sans qu'il soit nécessaire de les ré-authentifier.
Des performances évolutives	La performance des appliances SMA augmente de manière exponentielle en déployant plusieurs appliances, éliminant ainsi un seul point de défaillance. Le clustering horizontal prend entièrement en charge le mélange des appliances SMA physiques et virtuelles.
Licence dynamique	Les licences utilisateurs ne doivent plus être appliquées aux appliances SMA individuelles. Les utilisateurs peuvent être répartis et réaffectés dynamiquement entre les appareils gérés, en fonction de la demande des utilisateurs.

Gestion et surveillance centrales

Système de gestion centrale (CMS)	Le système CMS fournit une gestion centralisée basée sur le Web pour toutes les capacités SMA.
Alertes personnalisées	Les alertes peuvent être configurées pour générer des pièges SNMP qui sont surveillés par n'importe quel système de gestion de réseau d'infrastructure informatique (NMS). Les administrateurs peuvent également configurer des alertes pour les analyses de fichiers Capture ATP et l'utilisation du disque pour une action immédiate.
Tableau de bord en temps réel	Un tableau de bord personnalisable en temps réel permet à l'administrateur informatique de diagnostiquer rapidement et facilement les problèmes d'accès, obtenant ainsi des informations précieuses pour le dépannage.
Intégration SIEM	Le rendement en temps réel vers les collecteurs de données SIEM centraux permet aux équipes de sécurité de mettre en corrélation les activités guidées par les événements afin de comprendre le flux de travail de bout en bout d'un utilisateur ou d'une application en particulier. Ceci est essentiel lors de la gestion des incidents de sécurité et de l'analyse forensique.
Planificateur	Le planificateur permet aux utilisateurs de planifier des tâches de maintenance telles que le déploiement de règles, la reproduction de paramètres de configuration et le redémarrage de services, sans intervention manuelle.

Extensibilité

API de gestion	Les API de gestion permettent un contrôle administratif entièrement programmé de tous les objets dans un seul environnement SMA ou CMS global.
API pour utilisateur final	Les API pour utilisateur final fournissent un contrôle complet de tous les processus de connexion, d'authentification et liés aux terminaux.
Authentification à deux facteurs (2FA)	La solution SMA fournit la 2FA en intégrant des solutions de pointe de mots de passe à usage unique basées sur le temps (TOTP) telles que Google Authenticator, Microsoft Authenticator, Duo security, etc.
Intégration MDM	SMA s'intègre aux principaux produits de gestion mobile d'entreprise (EMM) tels qu'Airwatch et Mobile Iron.
Autre intégration tierce	La solution SMA s'associe à des fournisseurs leaders du secteur comme OPSWAT pour fournir une protection avancée contre les menaces.

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

[2]*Amélioré dans SMA 12.1*

Résumé des caractéristiques (comparaison par modèle)

Catégorie	Fonctionnalité	210	410	500v	6210	7210	8200v
Déploiement	Système d'exploitation	v9.0 et ultérieurs	v9.0 et ultérieurs	v9.0 et ultérieurs	v12.1 et ultérieurs	v12.1 et ultérieurs	v12.1 et ultérieurs
	Hyperviseurs pris en charge	–	–	VMware ESXi / Microsoft Hyper-V	–	–	VMware ESXi / Microsoft Hyper-V
	Plateformes de cloud public prises en charge	–	–	AWS/Azure	–	–	AWS/Azure
Débit	Plusieurs sessions simultanées d'utilisateurs	200	400	250	2 000	10 000	5 000
	Débit max SSL/TLS	560 Mbit/s	844 Mbit/s	265 Mbit/s	1,3 Gbit/s	5,0 Gbit/s	1,58 Gbit/s
Accès client	Tunnel de couche 3	•	•	•	•	•	•
	Tunnel divisé et redirection intégrale	•	•	•	•	•	•
	VPN « Always On »	•	•	•	•	•	•
	Encapsulation ESP automatique	–	–	–	•	•	•
	HTML5 (RDP, VNC, ICA, SSH, Telnet, Network Explorer)	•	•	•	•	•	•
	Détection réseau sécurisée	–	–	–	•	•	•
	Navigateur de fichiers (CIFS/NFS)	•	•	•	•	•	•
	Citrix XenDesktop/XenApp	•	•	•	•	•	•
	VMware View	–	–	–	•	•	•
	Tunnel « On Demand »	–	–	–	•	•	•
	Extensions Chrome/Firefox	–	–	–	•	•	•
	Prise en charge de tunnel CLI	–	–	–	•	•	•
	Mobile Connect (iOS, Android, Chrome, Win 10, Mac OSX)	•	•	•	•	•	•
	Net Extender (Windows, Linux)	•	•	•	–	–	–
	Connect Tunnel (Windows, Mac OSX, Linux)	–	–	–	•	•	•
	Exchange ActiveSync	•	•	•	•	•	•
Accès mobile	VPN par application	–	–	–	•	•	•
	Application du contrôle des applications	–	–	–	•	•	•
	Validation de l'ID de l'application	–	–	–	•	•	•
Portail utilisateur	Valorisation de la marque	•	•	•	•	•	•
	Personnalisation	–	–	–	•	•	•
	Localisation	•	•	•	•	•	•
	Signets définis par l'utilisateur	•	•	•	•	•	•
	Prise en charge URL personnalisée	•	•	•	•	•	•
	Prise en charge des applications SaaS	–	–	–	•	•	•
Sécurité	(123) 140-2	–	–	–	•	•	–
	ICSA SSL-TLS	•	•	•	•	•	•
	Codes de chiffrement Suite B	–	–	–	•	•	•
	Interrogation EPC dynamique	•	•	•	•	•	•
	Contrôle d'accès basé sur les rôles (RBAC)	–	–	–	•	•	•
	Enregistrement des terminaux	•	•	•	•	•	•
	Partage sécurisé de fichiers (Capture ATP)	•	•	•	•	•	•
	Quarantaine des terminaux	•	•	•	•	•	•
	Validation CRL OSCP	–	–	–	•	•	•
	Sélection des codes de chiffrement	–	–	–	•	•	•
	Certificats clients et ICP	•	•	•	•	•	•
	Filtrage Geo IP	•	•	•	–	–	–
	Filtrage de réseaux de zombies	•	•	•	–	–	–
	Proxy direct	•	•	•	•	•	•
	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 multifacteurs (MFA)	–	–	–	•	•	•

Résumé des caractéristiques (comparaison par modèle, suite)

Catégorie	Fonctionnalité	210	410	500v	6210	7210	8200v
Services d'authentification et d'identité	Authentification chaînée	–	–	–	•	•	•
	Code à usage unique (OTP) par e-mail ou SMS	•	•	•	•	•	•
	Prise en charge Common Access Card (CAC)	–	–	–	•	•	•
	Prise en charge des certificats X.509	•	•	•	•	•	•
	Intégration Captcha	–	–	–	•	•	•
	Changement de mot de passe à distance	•	•	•	•	•	•
	SSO basée sur des formulaires	•	•	•	•	•	•
	SSO centralisée	–	–	–	•	•	•
	Persistance de la session	–	–	–	•	•	•
	Connexion automatique	•	•	•	•	•	•
Contrôle des accès	Groupe AD	•	•	•	•	•	•
	Attributs LDAP	•	•	•	•	•	•
	Règles de géolocalisation	•	•	•	–	–	–
	Surveillance continue des terminaux	•	•	•	•	•	•
Gestion	Interface de gestion (Ethernet)	–	–	–	•	•	•
	Interface de gestion (console)	–	–	–	•	•	•
	Administration HTTPS	•	•	•	•	•	•
	Administration SSH	–	–	–	•	•	•
	SNMP MIBS	•	•	•	•	•	•
	Syslog et NTP	•	•	•	•	•	•
	Suivi de l'utilisation	•	•	•	•	•	•
	Récupération de configuration	•	•	•	•	•	•
	Gestion centralisée	–	–	–	•	•	•
	Reporting centralisé	–	–	–	•	•	•
	API REST de gestion	–	–	–	•	•	•
	API REST d'authentification	–	–	–	•	•	•
	Comptabilité RADIUS	–	–	–	•	•	•
	Tâches planifiées	–	–	–	•	•	•
	Licence de session centralisée	–	–	–	•	•	•
	Audit guidé par les événements	–	–	–	•	•	•
Gestion de réseau	IPv6	•	•	•	•	•	•
	Équilibrage de charge global	–	–	–	•	•	•
	Équilibrage de charge des serveurs	•	•	•	–	–	–
	Réplication de l'état TCP	•	•	•	•	•	•
	Basculement de l'état des clusters	–	–	–	•	•	•
	Haute disponibilité active/passive	–	•	•	•	•	•
	Haute disponibilité active/active	–	–	–	•	•	•
	Évolutivité horizontale	–	–	–	•	•	•
	FQDN uniques ou multiples	–	–	–	•	•	•
	Proxy de tunnel intelligent L3-7	•	•	•	•	•	•
	Proxy d'application L7	•	•	•	•	•	•
Intégration	Prise en charge TOTP 2FA	•	•	•	•	•	•
	Prise en charge des produits EMM et MDM	–	–	–	•	•	•
	Prise en charge des produits SIEM	–	–	–	•	•	•
	Coffre de mots de passe TPAM	–	–	–	•	•	•
	Prise en charge de l'hyperviseur ESX	–	–	•	–	–	•
	Prise en charge de l'hyperviseur Hyper-V	–	–	•	–	–	•
Options de licence	Licence sur abonnement	–	–	–	•	•	•
	Licence perpétuelle avec support	•	•	•	•	•	•
	Web Application Firewall (WAF)	•	•	•	–	–	–
	Licence Spike	•	•	•	•	•	•
	Licences à plusieurs niveaux	–	–	–	•	•	•
	Aide virtuelle	•	•	•	–	–	–

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

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

Performances supérieures | Débit accru | Fonctionnalités avancées | Meilleure évolutivité

Spécifications des appliances

Choisissez parmi une gamme d'appliances d'accès mobile sécurisé (SMA) spécialement conçues à cet effet. Bénéficiez d'options de déploiement flexibles avec des appliances virtuelles et physiques.

Caractéristiques des appliances physiques

Performances	SMA 210	SMA 410	SMA 6210	SMA 7210
Sessions simultanées/Utilisateurs	Jusqu'à 200	Jusqu'à 400	Jusqu'à 2 000	Jusqu'à 10 000
Débit VPN SSL* (au CCU maximum)	560 Mbit/s	844 Mbit/s	800 Mbit/s	5,0 Gbit/s
Format	1U	1U	1U	1U
Dimensions	43 x 26 x 4,5 cm (16,92 x 10,23 x 1,75 po)	43 x 26 x 4,5 cm (16,92 x 10,23 x 1,75 po)	43 x 41,5 x 4,5 cm (17,0 x 16,5 x 1,75 po)	43 x 41,5 x 4,5 cm (17,0 x 16,5 x 1,75 po)
Poids de l'appliance	5 kg (11 lb)	5 kg (11 lb)	8 kg (17,7 lb)	8,3 kg (18,3 lb)
Accélération des données de chiffrement (AES-NI)	NON	NON	OUI	OUI
Port de gestion dédié	NON	NON	OUI	OUI
Accélération SSL	NON	NON	OUI	OUI
Stockage	4 Go (mémoire flash)	4 Go (mémoire flash)	2 x 1 To SATA ; RAID 1	2 x 1 To SATA ; RAID 1
Interfaces	(2) GB Ethernet, (2) USB, (1) console	(4) GB Ethernet, (2) USB, (1) console	(6)-port 1GE, (2) USB, (1) console	(6)-port 1GE, (2)-port 10Go SFP+, (2) USB, (1) console
Mémoire	4 Go	8 Go	8 Go DDR4	16 Go DDR4
Puce TPM	NON	NON	OUI	OUI
Processeur	4 cœurs	8 cœurs	4 cœurs	4 cœurs
Temps de fonctionnement entre deux pannes (à 25 °C ou 77 °F) en heures	61 815	60 151	70 127	129 601
Opérations et conformité	**SMA 210**	**SMA 410**	**SMA 6210**	**SMA 7210**
Alimentation	Alimentation électrique fixe	Alimentation électrique fixe	Alimentation électrique fixe	Double système d'alimentation, échangeable à chaud
Classification entrante	100-240VAC (-60MHz) :	100-240VAC (-60MHz) :	100 à 240 V CA, 1,1 A	100 à 240 V CA, 1,79 A
Consommation électrique	26,9 W	31,9 W	77 W	114 W
Dissipation thermique totale	92 BTU	109 BTU	264 BTU	389 BTU
Environnement	DEEE, RoHS UE, RoHS Chine			
Choc hors fonctionnement	110 g, 2 ms			
Émissions	FCC, ICES, CE, C-Tick, VCCI ; MIC			
Sécurité	TÜV/GS, UL, CE PSB, CCC, BSMI, schéma CB			
Température de fonctionnement	0°C à 40°C (32°F à 104°F)			
Certification FIPS	NON	NON	FIPS 140-2 Niveau 2 avec protection anti-intrusion	

**Les performances de débit peuvent varier en fonction du déploiement et de la connectivité. Les chiffres publiés sont basés sur les conditions internes en laboratoire*

Spécifications des appliances virtuelles

Caractéristiques	SMA 500v (ESX/ESXi/Hyper-V)	SMA 8200v (ESX/ESXi/Hyper-V)
Sessions simultanées	Jusqu'à 250 utilisateurs	Jusqu'à 5 000
Débit SSL-VPN* (au CCU max)	Jusqu'à 186 Mbit/s	Jusqu'à 1,58 Gbit/s
Mémoire allouée	2 Go	8 Go
Processeur	1 cœur	4 cœurs
Accélération SSL	NON	OUI
Taille du disque appliqué	2 Go	64 Go (par défaut)
Système d'exploitation installé	Linux	Linux renforcé
Port de gestion dédié	NON	OUI

**Les performances de débit peuvent varier en fonction du déploiement et de la connectivité. Les chiffres publiés sont basés sur les conditions internes en laboratoire. SMA 8200v sur Hyper-V peut accueillir jusqu'à 5 000 sessions simultanées et fournit un débit SSL-VPN de 1,58 Gbit/s lors de l'exécution de SMA OS 12.1 avec Windows Server 2016*

Informations de commande

RÉFÉRENCE	APPLIANCE SECURE MOBILE ACCESS (SMA) DE SONICWALL
02-SSC-2800	SMA 210 avec licence 5 utilisateurs
02-SSC-2801	SMA 410 avec licence 25 utilisateurs
01-SSC-8469	SMA 500v avec licence 5 utilisateurs
02-SSC-0978	SMA 7210 avec licence test administrateur
02-SSC-0976	SMA 6210 avec licence test administrateur
01-SSC-8468	SMA 8200v (appliance virtuelle)
RÉFÉRENCE	**LICENCES UTILISATEURS SMA SONICWALL**
01-SSC-9182	SMA 500V avec ajout de 5 utilisateurs (également disponible pour SMA 210)
01-SSC-2414	SMA 500V avec ajout de 100 utilisateurs (également disponible pour SMA 410)
01-SSC-7856	Licence SMA 5 utilisateurs - empilable pour 6210, 7210, 8200v
01-SSC-7860	Licence SMA 100 utilisateurs - empilable pour 6210, 7210, 8200v
01-SSC-7865	Licence SMA 5 000 utilisateurs - empilable pour 7210, 8200v
RÉFÉRENCE	**CONTRAT SUPPORT SMA SONICWALL**
01-SSC-9191	Support 24 h/24, 7 j/7 pour SMA 500V jusqu'à 25 utilisateurs, 1 an (également disponible pour SMA 210 et 410)
01-SSC-2326	Support 24 h/24, 7 j/7 pour SMA 6210 pour 100 utilisateurs, 1 an - empilable
01-SSC-2350	Support 24 h/24, 7 j/7 pour SMA 7210 pour 500 utilisateurs, 1 an - empilable
01-SSC-8434	Support 24 h/24, 7 j/7 pour SMA 8200V pour 5 utilisateurs, 1 an - empilable (également disponible pour SMA 6210, 7210)
01-SSC-8446	Support 24 h/24, 7 j/7 pour SMA 8200V pour 100 utilisateurs, 1 an - empilable (également disponible pour SMA 6210, 7210)
01-SSC-7913	Support 24 h/24, 7 j/7 pour SMA 8200V pour 5000 utilisateurs, 1 an - empilable (également disponible pour SMA 6210, 7210)
RÉFÉRENCE	**GESTION CENTRALE POUR 6210, 7210, 8200V**
Licence d'appliance CMS	
01-SSC-8535	Licence base CMS + 3 appliances (gratuit - pour les essais et utilisation avec les licences utilisateurs sur abonnement)
01-SSC-8536	Licence CMS 100 appliances, 1 an (pour utilisation avec des licences utilisateur sur abonnement)
01-SSC-3369	Base CMS + 3 appliances (gratuit, à utiliser avec des licences utilisateur perpétuelles)
01-SSC-3402	Licence CMS 100 appliances, 1 an (pour utilisation avec des licences d'utilisateur perpétuelles)
Licences utilisateurs centrales (abonnement)	
01-SSC-2298	Licence CMS regroupée 10 utilisateurs, 1 an
01-SSC-8539	Licence CMS regroupée 1 000 utilisateurs, 1 an
01-SSC-5339	Licence CMS regroupée 50 000 utilisateurs, 1 an
Licences utilisateurs centrales (perpétuelles)	
01-SSC-2053	Licence CMS perpétuelle, 10 utilisateurs
01-SSC-2058	Licence CMS perpétuelle, 1 000 utilisateurs
01-SSC-2063	Licence CMS perpétuelle, 50 000 utilisateurs
Support pour les licences utilisateur centrales (perpétuelles)	
01-SSC-2065	Support CMS 24 h/24, 7 j/7, 10 utilisateurs, 1 an
01-SSC-2070	Support CMS 24 h/24, 7 j/7, 1 000 utilisateurs, 1 an
01-SSC-2075	Support CMS 24 h/24, 7 j/7, 50 000 utilisateurs, 1 an
Licences ActiveSync centrales (abonnement)	
01-SSC-2088	Licence CMS regroupée par e-mail, 10 utilisateurs,1 an
01-SSC-2093	Licence CMS regroupée par e-mail, 1 000 utilisateurs,1 an
01-SSC-2087	Licence CMS regroupée par e-mail, 50 000 utilisateurs,1 an

Informations de commande (suite)

RÉFÉRENCE	GESTION CENTRALE POUR 6210, 7210, 8200V
Licences Spike centrales	
01-SSC-2111	Licence CMS Spike 1 000 utilisateurs, 5 jours
01-SSC-2115	Licence CMS Spike 50 000 utilisateurs, 5 jours
Module complémentaire Capture (abonnement)	
Contactez votre revendeur **Les licences d'abonnement ont un support 24 h/24, 7 j/7 inclus*	
RÉFÉRENCE	**MODULES COMPLÉMENTAIRES SMA SONICWALL**
01-SSC-2406	Module complémentaire SMA 7210 FIPS
01-SSC-2405	Module complémentaire SMA 6210 FIPS
01-SSC-9185	SMA 500V Web Application Firewall 1 AN (également disponible pour SMA 210 et 410)
RÉFÉRENCE	**MISE À NIVEAU SMA SECURE UPGRADE SONICWALL**
02-SSC-2794	SMA 210 Secure Upgrade Plus, lot de 5 utilisateurs avec support 24 h/24, 7 j/7 jusqu'à 25 utilisateurs, 1 an
02-SSC-2795	SMA 210 Secure Upgrade Plus, lot de 5 utilisateurs avec support 24 h/24, 7 j/7 jusqu'à 25 utilisateurs, 3 ans
02-SSC-2798	SMA 410 Secure Upgrade Plus, lot de 25 utilisateurs avec support 24 h/24, 7 j/7 jusqu'à 100 utilisateurs, 1 an
02-SSC-2799	SMA 410 Secure Upgrade Plus, lot de 25 utilisateurs avec support 24 h/24, 7 j/7 jusqu'à 100 utilisateurs, 3 ans
02-SSC-2893	SMA 6210 Secure Upgrade Plus, support 24 h/24, 7 j/7 jusqu'à 100 utilisateurs, 1 an
02-SSC-2894	SMA 6210 Secure Upgrade Plus, support 24 h/24, 7 j/7 jusqu'à 100 utilisateurs, 3 ans
02-SSC-2895	SMA 7210 Secure Upgrade Plus, support 24 h/24, 7 j/7 jusqu'à 250 utilisateurs, 1 an
02-SSC-2896	SMA 7210 Secure Upgrade Plus, support 24 h/24, 7 j/7 jusqu'à 250 utilisateurs, 3 ans
02-SSC-0860	SMA 8200V Secure Upgrade Plus, support 24 h/24, 7 j/7 jusqu'à 100 utilisateurs, 1an
02-SSC-0862	SMA 8200V Secure Upgrade Plus, support 24 h/24, 7 j/7 jusqu'à 100 utilisateurs 3 ans
02-SSC-2807	SMA 500V Secure Upgrade Plus, support 24 h/24, 7 j/7 jusqu'à 100 utilisateurs, 1 an
02-SSC-2808	SMA 500V Secure Upgrade Plus, support 24 h/24, 7 j/7 jusqu'à 100 utilisateurs 3 ans
RÉFÉRENCE	**LICENCE SPIKE POUR SMA (NÉCESSITÉ D'INCRÉMENTATION POUR ATTEINDRE LA CAPACITÉ)**
01-SSC-2240	Licence Spike SMA 210 10 jours, 50 utilisateurs (également disponible pour SMA 410 et 500v)
01-SSC-7873	Licence Spike SMA 8200v, 10 jours, 5 à 2 500 utilisateurs (également disponible pour SMA 6210, 7210)
02-SSC-4490	LICENCE SPIKE SMA 500V POUR 250 UTILISATEURS, 30 JOURS
02-SSC-4489	LICENCE SPIKE SMA 500V POUR 250 UTILISATEURS, 60 JOURS
02-SSC-4488	LICENCE SPIKE SMA 200/210 POUR 50 UTILISATEURS, 30 JOURS
02-SSC-4487	LICENCE SPIKE SMA 200/210 POUR 50 UTILISATEURS, 60 JOURS
02-SSC-4486	LICENCE SPIKE SMA 400/410 POUR 250 UTILISATEURS, 30 JOURS
02-SSC-4485	LICENCE SPIKE SMA 400/410 POUR 250 UTILISATEURS, 60 JOURS
02-SSC-4471	LICENCE SPIKE COMPLÉMENTAIRE SMA CMS POUR 100 UTILISATEURS, 30 JOURS
02-SSC-4473	LICENCE SPIKE COMPLÉMENTAIRE SMA CMS POUR 500 UTILISATEURS, 30 JOURS
02-SSC-4475	LICENCE SPIKE COMPLÉMENTAIRE MA CMS POUR 1 000 UTILISATEURS, 30 JOURS
02-SSC-4477	LICENCE SPIKE COMPLÉMENTAIRE SMA CMS POUR 5 000 UTILISATEURS, 30 JOURS
02-SSC-4479	LICENCE SPIKE COMPLÉMENTAIRE SMA CMS POUR 10 000 UTILISATEURS, 30 JOURS
02-SSC-4481	LICENCE SPIKE COMPLÉMENTAIRE MA CMS POUR 25 000 UTILISATEURS, 30 JOURS
02-SSC-4483	LICENCE SPIKE COMPLÉMENTAIRE SMA CMS POUR 50 000 UTILISATEURS, 30 JOURS
02-SSC-4472	LICENCE SPIKE COMPLÉMENTAIRE SMA CMS POUR 100 UTILISATEURS, 60 JOURS
02-SSC-4474	LICENCE SPIKE COMPLÉMENTAIRE SMA CMS POUR 500 UTILISATEURS, 60 JOURS
02-SSC-4476	LICENCE SPIKE COMPLÉMENTAIRE SMA CMS POUR 1 000 UTILISATEURS, 60 JOURS

Informations de commande (suite)

RÉFÉRENCE	LICENCE SPIKE POUR SMA (NÉCESSITÉ D'INCRÉMENTATION POUR ATTEINDRE LA CAPACITÉ)
02-SSC-4478	LICENCE SPIKE COMPLÉMENTAIRE SMA CMS POUR 5 000 UTILISATEURS, 60 JOURS
02-SSC-4480	LICENCE SPIKE COMPLÉMENTAIRE SMA CMS POUR 10 000 UTILISATEURS, 60 JOURS
02-SSC-4482	LICENCE SPIKE COMPLÉMENTAIRE SMA CMS POUR 25 000 UTILISATEURS, 60 JOURS
02-SSC-4484	LICENCE SPIKE COMPLÉMENTAIRE SMA CMS POUR 50 000 UTILISATEURS, 60 JOURS

**Des références pluriannuelles et des contrats de support sont également disponibles. Pour obtenir une liste complète des références, contactez votre revendeur ou votre service commercial*

Partenaire de services

Besoin d'aide pour planifier, déployer ou optimiser votre solution SonicWall ? Le programme avancé Partenaire de services SonicWall a pour objectif de vous fournir des services professionnels de classe mondiale. Pour en savoir plus, rendez-vous sur www.sonicwall.com/fr-fr/partners/partner-enabled-services/.

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. SonicWall protège les organisations qui se mobilisent pour la nouvelle norme des affaires grâce à une protection sans faille qui stoppe les cyberattaques les plus évasives des points d'exposition illimités et des effectifs à distance, mobiles et dans le cloud. 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 ou suivez-nous sur Twitter, LinkedIn, Facebook et Instagram.

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