SonicWall Mobile Connect

Un accès simple et sécurisé, sur la base de règles, à des applications et à des données vitales sur appareils mobiles iOS, OS X, Android, Chrome OS, Kindle Fire et Windows.

Offrez à vos employés un accès sûr et facile aux données et aux ressources dont ils ont besoin pour être productifs, et ce depuis tout un éventail d'appareils, notamment iOS, OS X, Android™, Chrome OS, Kindle Fire et Windows. Et en même temps, assurez la protection du réseau de l'entreprise contre les menaces mobiles.

L'application SonicWall™ Mobile Connect™ fonctionne avec les appliances Secure Mobile Access (SMA) ou les pare-feux de nouvelle génération SonicWall. Les travailleurs nomades n'ont qu'à installer et lancer l'application Mobile Connect sur leur appareil mobile iOS, OS X, Android, Chrome OS ou Windows pour établir une connexion sécurisée avec une appliance SMA ou un pare-feu de nouvelle génération. La connexion VPN SSL chiffrée protègera le trafic de toute interception et assurera la sécurité des données en circulation. L'authentification contextuelle garantit que seuls les utilisateurs autorisés et les appareils de confiance peuvent accéder au réseau.

En coulisses, les services informatiques peuvent facilement élaborer et gérer des politiques d'accès via des appliances SonicWall grâce à une interface de gestion unique, notamment la restriction par l'administrateur de l'accès VPN à un ensemble d'applications mobiles de confiance. De plus, la solution SonicWall s'intègre aisément à la plupart des systèmes d'authentification en arrière-plan, y compris aux systèmes d'authentification à deux facteurs, ce qui vous permet d'appliquer efficacement vos pratiques dans ce domaine à vos utilisateurs mobiles.

Caractéristiques et avantages

Convivialité

Les utilisateurs d'appareils fonctionnant avec iOS, OS X, Windows 10, Android, Chrome OS ou Kindle peuvent aisément télécharger et installer l'application Mobile Connect via l'App Store™, Google Play, le Chrome Web Store, l'Amazon App Store ou le Windows Store. Dans le cas de Windows 8.1, Mobile Connect est intégré au système d'exploitation. Nul besoin donc de télécharger et d'installer une autre application de client VPN.

Gestion centralisée des règles

Les services informatiques peuvent fournir et gérer l'accès d'appareils mobiles, notamment contrôler toutes les ressources en ligne, les partages de fichiers et les ressources client-serveur, au moyen d'appliances SonicWall, le tout sur une interface de gestion unique. Contrairement aux autres VPN, la solution SonicWall vous permet de mettre en place rapidement des règles liées à des rôles pour les appareils mobiles, les ordinateurs portables et leurs utilisateurs, en appliquant une règle unique pour tous les objets ; la gestion des règles peut ainsi ne prendre que quelques minutes, contre plusieurs heures avec d'autres solutions.

Vérification de l'utilisateur et de l'appareil

L'utilisateur de Mobile Connect n'a accès au réseau de l'entreprise qu'après avoir été authentifié et l'intégrité de l'appareil mobile vérifiée. End Point Control peut déterminer si un appareil iOS ou Android a été débloqué, et si un certificat est présent ou si la version du système d'exploitation est à jour, puis, au besoin, rejeter la connexion ou la mettre en quarantaine.

Accès facile aux ressources appropriées

Les appareils mobiles iOS, Android, Chrome OS, Kindle et Windows peuvent se connecter à toutes les ressources réseau autorisées, notamment aux applications en ligne, client/serveur, serveur, hôtes et back-connect. Une fois que l'utilisateur et son appareil ont été vérifiés, Mobile Connect propose des signets préconfigurés pour un accès rapide

Avantages :

- Convivialité
- Gestion centralisée des règles
- Vérification de l'utilisateur et de l'appareil
- Accès facile aux ressources appropriées
- Protection anti-malware
- Enregistrement des appareils mobiles et gestion de la politique d'autorisation
- VPN par application
- Consultation sécurisée des fichiers intranet en un clic et protection des données sur l'appareil
- Lancement automatique du VPN
- Intégration aisée
- Surveillance et contrôle des applications

Assurez un accès mobile rapide et sécurisé grâce à une application intuitive et conviviale, facile à installer et à lancer sur smartphones et tablettes.

Données de compatibilité

SonicWall SMA et pare-feux de nouvelle génération
Appliances TZ, NSA, E-Class NSA ou Super Massive 9000 Series avec SonicOS 5.9, 6.2 ou version supérieure
Appliances SMA 100 Series/SRA avec 7.5 ou version supérieure
Appliances SMA 1000 Series/E-Class SRA avec 10.7 ou version supérieure

SonicWall Mobile Connect
Appareils équipés d'iOS 7.0 ou version supérieure
Appareils équipés d'OS X 10.9 ou version supérieure
Appareils équipés d'Android 4.1 ou version supérieure
Appareils Kindle Fire reposant sur Android 4.1 ou version supérieure
Appareils équipés de ChromeOS 45 ou version supérieure
Appareils équipés de Windows 8.1
Appareils équipés de Windows Phone 8.1
Appareils équipés de Windows 10

aux applications et aux ressources de l'entreprise pour lesquelles l'utilisateur et l'appareil disposent de privilèges.

Protection anti-malware

Associée à un pare-feu SonicWall de nouvelle génération, Mobile Connect met en place un Clean VPN™, un système de protection supplémentaire qui déchiffre et analyse tout le trafic VPN SSL afin de détecter les logiciels malveillants avant qu'ils ne pénètrent sur le réseau.

Enregistrement des appareils mobiles et gestion de la politique d'autorisation

Avec Mobile Connect et Secure Mobile Access OS (version 11.0 et supérieures) pour les appliances Secure Mobile Access 1000 Series : avant d'octroyer l'accès au réseau, si un appareil mobile n'a pas été enregistré précédemment sur l'appliance SMA, l'utilisateur voit s'afficher une politique d'autorisation de son appareil. Il doit en accepter les termes pour enregistrer l'appareil et accéder aux ressources et données autorisées de l'entreprise. L'administrateur peut adapter cette politique.

VPN par application

Mobile Connect associé à Secure Mobile Access OS (version 11.0 et supérieures) pour les appliances Secure Mobile Access 1000 Series permet aux administrateurs de mettre en place et d'appliquer des règles déterminant quelles applications d'un appareil mobile peuvent bénéficier d'un accès VPN au réseau. Cela garantit que seules les applications mobiles professionnelles autorisées utilisent l'accès par VPN. Mobile Connect est la seule solution qui ne requiert aucune modification des applications mobiles pour l'accès VPN par application. N'importe quelle application mobile ou conteneur sécurisé peut être pris en charge sans modification, encapsulation ni SDK.

Consultation sécurisée des fichiers intranet en un clic et protection des données sur l'appareil

Protégez les données de l'entreprise stockées sur les appareils mobiles. Les utilisateurs authentifiés peuvent naviguer en toute sécurité et consulter les partages de fichiers et les fichiers intranet autorisés depuis l'application Mobile Connect. Les administrateurs peuvent mettre en place et faire appliquer une politique de gestion des applications mobiles pour que Mobile Connect vérifie si les fichiers consultés peuvent être ouverts dans d'autres applications, copiés dans le presse-papiers, imprimés ou mis en cache en toute sécurité au sein de l'application Mobile Connect. Pour les appareils iOS, cela permet aux administrateurs de séparer les données d'entreprise des données personnelles stockées sur l'appareil et réduit le risque de perte de données. En outre, si les informations de connexion de l'utilisateur sont révoquées, le contenu enregistré dans l'application Mobile Connect est verrouillé et ne peut plus être utilisé ni consulté.

Lancement automatique du VPN

Le filtrage des URL permet aux applications qui ont besoin d'une connexion VPN pour fonctionner (notamment Safari) de créer un profil VPN et de lancer ou de déconnecter Mobile Connect automatiquement au démarrage (nécessite un firmware serveur compatible). De plus, sur les appareils iOS ou OS X, afin de simplifier la connexion, le VPN à la demande initie automatiquement une session VPN SSL sécurisée lorsqu'un utilisateur désire accéder à des données internes, des applications, des sites Web ou des hôtes.

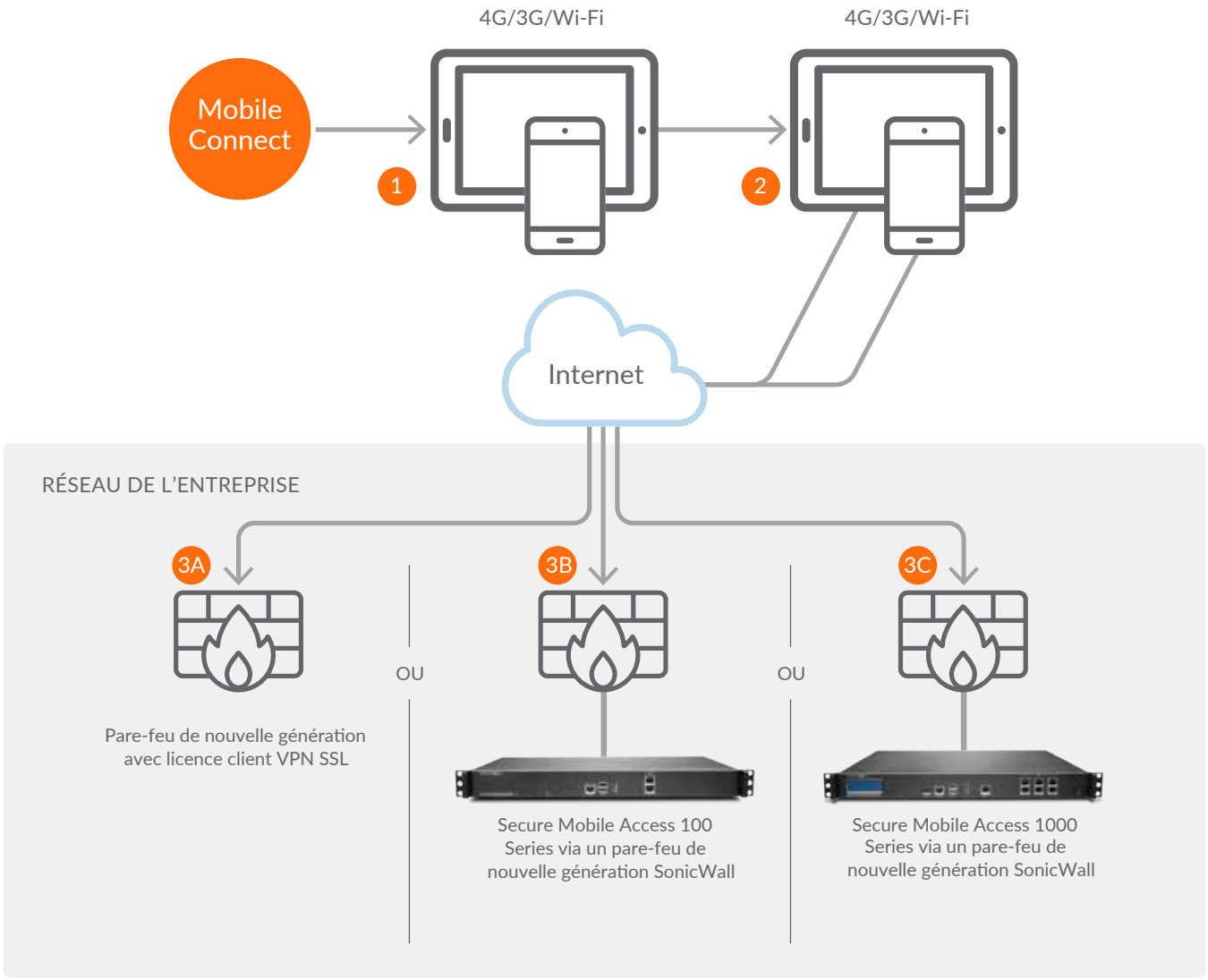
Intégration aux solutions d'authentification existantes

La solution SonicWall s'intègre aisément à la plupart des systèmes d'authentification en arrière-plan, tels que LDAP, Active Directory et Radius ; vous pouvez ainsi appliquer efficacement vos pratiques dans ce domaine à vos utilisateurs mobiles. Pour plus de sécurité, il est possible d'activer la génération de mots de passe uniques et de l'intégrer aisément à des technologies d'authentification à deux facteurs.

Surveillance et contrôle des applications

En association avec un pare-feu de nouvelle génération, cela permet au service informatique de définir et de régler facilement l'utilisation de la bande passante et des applications.

Accès logiciel



1. Téléchargez et installez SonicWall Mobile Connect sur votre appareil mobile.
2. Créez un profil de connexion pour accéder au réseau de l'entreprise.
3A. Connectez-vous à un pare-feu de nouvelle génération SonicWall.
   Avantages : filtrage DPI anti-malware et services de surveillance et de contrôle des applications.
3B. Connectez-vous à une appliance SonicWall Secure Mobile Access 100 Series via un pare-feu de nouvelle génération SonicWall.
   Avantages : filtrage DPI anti-malware et contrôle de terminal (EPC) en vue de mettre en quarantaine ou de rejeter toute connexion provenant d'appareils débloqués.
3C. Connectez-vous à une appliance SonicWall Secure Mobile Access 1000 Series via un pare-feu de nouvelle génération SonicWall.
   Avantages : filtrage DPI anti-malware et contrôle de terminal (EPC) en vue de mettre en quarantaine ou de rejeter toute connexion provenant d'appareils débloqués. Permet également aux administrateurs de restreindre l'accès VPN à un ensemble d'applications mobiles de confiance autorisées et de gérer la politique de sécurité BYOD.

Fonctionnalités	iOS	OS X/Mac	Android	Kindle Fire	Windows 8.1	Windows Phone 8.1	Windows 10	Chrome OS
Distribution	App Store	Mac App Store	Google Play	Amazon App Store	Intégré au système	Windows Phone Store	Windows Store	Chrome Web Store
Connectivité VPN de couche 3 (VPN SSL)	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Connexion à la demande	Oui[3]	Oui[3]	—	—	Oui	MDM uniquement	MDM/ PowerShell	Oui
Réseaux sécurisés configurables	Oui[1]	Oui[1]	—	—	Oui	Oui	Oui	—
Sensibilité réseau	Oui[1]	Oui[1]	Oui[1]	Oui[1]	—	—	—	—
Mise en cache des informations de connexion	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Prise en charge Touch ID/empreinte digitale	Oui[2]	—	Oui[2]	—	—	—	—	—
Prise en charge Face ID	Oui	—	—	—	—	—	—	—
Contrôle des URL	Oui	Oui	Oui	Oui	—	—	—	—
Authentification de base (nom d'utilisateur et mot de passe)	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Authentification à deux facteurs (Dell Defender\TOTP\RADIUS)	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Authentification par certificat client	Oui[2]	Oui[2]	Oui[2]	Oui[2]	Oui	Oui	Oui	—
Modification du mot de passe	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Connexion unique pour le domaine Windows sur le VPN	—	—	—	—	Oui	Oui	Oui	—
Routage avec séparation des flux / ou à flux unique	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Prise en charge IPv6	Oui[4]	Oui[4]	Oui[4]	Oui[4]	Oui[4]	Oui[4]	Oui[4]	—
Compression des données sur le VPN	Oui[3]	Oui[3]	Oui[3]	Oui[3]	Oui[3]	Oui[3]	Oui[3]	Oui[3]
Mode ESP (transport UDP)	Oui[1]	Oui[1]	Oui[1]	Oui[1]	—	—	—	—
Résolution des conflits de réseau	Oui[1]	Oui[1]	Oui[1]	Oui[1]	Oui[1]	Oui[1]	Oui[1]	Oui[1]
End Point Control	Détection de déblocage, certificat, version SE, ID de l'appareil[3]	ID de l'appareil, version SE, certificat client[4]	Détection de déblocage, certificat, version SE, ID de l'appareil, antivirus[3]	Détection de déblocage, certificat, version SE, ID de l'appareil, antivirus	ID de l'appareil, version SE[4]	ID de l'appareil, version SE[4]	ID de l'appareil, version SE[4]	ID de l'appareil, version Chrome OS[4]
Lecteur de fichiers/signets	Oui[2]	—	Oui[2]	Oui[2]	—	—	—	—
Signets RDP	2X RDP, Microsoft Remote Desktop pour RDP	—	2X RDP, Remote RDP Lite/ Enterprise, Microsoft Remote Desktop pour RDP	2X RDP, Microsoft Remote Desktop pour RDP	—	—	—	—
Signets récepteur Citrix	Oui[2]	—	Oui[2]	Oui[2]	—	—	—	—
Signets VNC	Remoter VNC	—	android-vnc-viewer	—	—	—	—	—
Signets Web	Safari, Chrome	—	Tout navigateur en configuration système pour Android	Silk	—	—	—	—
Signets sur l'appareil	iSSH, Server Auditor pour SSH	—	ConnectBot, JuideSSH	JuideSSH	—	—	—	—
Signets HTML5 natifs	RDP, VNC, SSH, Telnet[2]	—	RDP, VNC, SSH, Telnet[2]	—	—	—	—	—
Gestion MDM des profils de connexion VPN	Oui	—	—	—	Oui	Oui	Oui	Console de gestion Google

[1] *Cette caractéristique est uniquement prise en charge sur les appliances E-Class SRA/SMA 1000. Veuillez consulter les notes de mise à jour du produit pour connaître la version du logiciel nécessaire pour prendre en charge cette caractéristique.*
[2] *Cette caractéristique est uniquement prise en charge sur les appliances SRA/SMA 100 Series.*
[3] *Cette caractéristique est uniquement prise en charge sur les appliances SRA/SMA 100 Series et E-Class SRA/SMA 1000 Series. Veuillez consulter les notes de mise à jour du produit pour connaître la version du logiciel nécessaire pour prendre en charge cette caractéristique.*
[4] *Cette caractéristique est prise en charge sur les appliances SRA/SMA 100 Series et E-Class SRA/SMA 1000 Series, ainsi que sur les pare-feux de nouvelle génération. Veuillez consulter les notes de mise à jour du produit afin de connaître la version du logiciel nécessaire pour prendre en charge cette caractéristique.*

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-MobileConnectSMA200_400-US-KJ-MKTG3044