SonicWall Mobile Connect

Acceso seguro y sencillo basado en políticas a las aplicaciones y los datos de misión crítica para dispositivos móviles iOS, OS X, Android, Chrome OS, Kindle Fire y Windows.

Proporcione a sus empleados acceso seguro y sencillo a los datos y recursos que necesitan para ser productivos desde una variedad de dispositivos, como iOS, OS X, Android™, Chrome OS, Kindle Fire y Windows. Al mismo tiempo, asegúrese de que la red corporativa esté protegida contra las amenazas de seguridad móviles.

La aplicación SonicWall™ Mobile Connect™ funciona en combinación con SonicWall Secure Mobile Access (SMA) o dispositivos de firewall de próxima generación. Los trabajadores móviles solo tienen que instalar e iniciar la aplicación Mobile Connect en su dispositivo móvil iOS, OS X, Android, Chrome OS o Windows para establecer una conexión segura a un dispositivo SMA o a un firewall de próxima generación. La conexión SSL VPN cifrada evita que el tráfico sea interceptado y protege los datos durante su transmisión. La autenticación sensible al contexto garantiza que solo accedan a los recursos los usuarios autorizados y los equipos fiables.

Los responsables de TI pueden implementar y gestionar políticas de acceso fácilmente mediante dispositivos SonicWall a través de una única interfaz de gestión. Asimismo pueden, por ejemplo, restringir el acceso VPN a un conjunto de aplicaciones móviles de confianza autorizadas por el administrador. Además, la solución de SonicWall se integra fácilmente con la mayoría de los sistemas de autenticación back-end, incluida la autenticación de doble factor, de modo que puede extender de manera eficaz las prácticas de autenticación que usted prefiera a sus trabajadores móviles.

Prestaciones y ventajas

Facilidad de uso

Los usuarios de iOS, OS X, Windows 10, Android, Chrome OS y Kindle pueden descargar e instalar fácilmente la aplicación Mobile Connect a través de App Store™, Google Play, Chrome Web Store, Amazon App Store o Windows Store. Para los usuarios de dispositivos móviles Windows 8.1, Mobile Connect está embebida en el sistema operativo Windows 8.1 para que no haya necesidad de descargar e instalar otra aplicación de cliente VPN.

Gestión centralizada de políticas

Los responsables de TI pueden proporcionar acceso para equipos móviles y gestionarlo a través de los dispositivos SonicWall—incluido el control de todos los recursos Web, archivos compartidos y recursos cliente-servidor—utilizando una única interfaz de gestión. A diferencia de otras soluciones VPN, la solución de SonicWall le permite establecer rápidamente políticas basadas en roles para dispositivos móviles y portátiles, así como para usuarios con una única norma para todos los objetos. Como resultado, la gestión de políticas le llevará tan solo unos minutos en lugar de horas.

Verificación del usuario y el dispositivo

El sistema solo permite el acceso de un usuario de Mobile Connect a la red corporativa una vez que ha sido autenticado y que se ha verificado la integridad de su dispositivo móvil. End Point Control es capaz de determinar si un dispositivo iOS ha sido modificado mediante "jailbreaking", si un dispositivo Android ha sido rooteado o si un certificado o la versión del SO son actuales para a continuación rechazar o poner en cuarentena la conexión en caso necesario.

Ventajas:

- Facilidad de uso
- Gestión centralizada de políticas
- Verificación del usuario y el dispositivo
- Acceso sencillo a los recursos apropiados
- Protección contra malware
- Registro de dispositivos móviles y gestión de autorizaciones
- VPN por aplicación
- Búsqueda segura de archivos de Intranet con un solo clic y protección de datos integrada en el dispositivo
- VPN de inicio automático
- Integración sencilla
- Inteligencia y control de aplicaciones

Proporcione acceso móvil rápido y seguro a través de una aplicación intuitiva fácil de instalar, iniciar y usar tanto en teléfonos inteligentes como en tablets.

Compatibilidad

SonicWall SMA y firewall de próxima generación
Dispositivos de las series TZ, NSA, E-Class NSA o Super Massive 9000 con SonicOS 5.9, 6.2 o superior
Dispositivos de las series SMA 100/SRA con 7.5 o superior
Dispositivos de las series SMA 1000/E-Class SRA con 10.7 o superior

SonicWall Mobile Connect
Dispositivos con iOS, versión 7.0 o superior
Dispositivos con OS X 10.9 o superior
Dispositivos con Android 4.1 o superior
Dispositivos Kindle Fire basados en Android 4.1 o superior
Dispositivos con ChromeOS 45 o superior
Dispositivos con Windows 8.1
Dispositivos con Windows Phone 8.1
Dispositivos con Windows 10

Acceso sencillo a los recursos apropiados

Los dispositivos móviles iOS, Android, Chrome OS, Kindle y Windows pueden conectarse a todos los recursos permitidos de la red, incluidas las aplicaciones cliente/servidor, back-connect y basadas en Web, servidor o host. Una vez que el usuario y el dispositivo han sido verificados, Mobile Connect ofrece marcadores preconfigurados para acceder con un solo clic a las aplicaciones y los recursos corporativos para los que el usuario y el dispositivo tienen privilegios.

Protección contra malware

Cuando se implementa con un firewall de próxima generación de SonicWall, Mobile Connect establece una Clean VPN™, una capa adicional de protección que descifra y escanea todo el tráfico SSL VPN en busca de malware antes de que acceda a la red.

Registro de dispositivos móviles y gestión de politicas de autorización

Con Mobile Connect y Secure Mobile Access OS (versiones 11.0 y superiores) para dispositivos de la serie Secure Mobile Access 1000, antes de conceder acceso a la red, si un dispositivo móvil no ha sido registrado previamente con el dispositivo SMA, el sistema presenta al usuario una política de autorización del dispositivo que éste debe aceptar. Para poder registrar el dispositivo y acceder a los recursos y datos corporativos autorizados, el usuario debe aceptar los términos de la política. El administrador puede personalizar los términos de la política.

VPN por aplicación

Mobile Connect, en combinación con Secure Mobile Access OS (versiones 11.0 y superiores) para los dispositivos de la serie Secure Mobile Access 1000, permite a los administradores establecer y reforzar políticas con el fin de determinar para qué aplicaciones de un dispositivo móvil puede concederse acceso VPN a la red. De este modo se garantiza que solo las aplicaciones móviles de negocio autorizadas puedan utilizar el acceso VPN. Mobile Connect es la única solución que no requiere modificar las aplicaciones móviles para proporcionar un acceso VPN por aplicación. Puede soportarse cualquier aplicación móvil o contenedor seguro sin necesidad de modificar ni envolver las aplicaciones ni de recurrir a un SDK.

Búsqueda segura de archivos de Intranet con un solo clic y protección de datos integrada en el dispositivo

Proteja los datos de la empresa en reposo en los dispositivos móviles. Los usuarios autenticados pueden examinar y visualizar los archivos y recursos compartidos de archivos permitidos de Intranet de forma segura desde la aplicación Mobile Connect. Los administradores pueden establecer y reforzar políticas de gestión de las aplicaciones móviles para que la aplicación Mobile Connect controle si los archivos visualizados pueden abrirse en otras aplicaciones, copiarse en el portapapeles, imprimirse o guardarse en caché de forma segura en la aplicación Mobile Connect. Para los dispositivos iOS, esto permite a los administradores separar los datos de negocio de los datos personales almacenados en el dispositivo con el fin de reducir el riesgo de pérdida de datos. Asimismo, si el sistema revoca las credenciales del usuario, el contenido almacenado en la aplicación Mobile Connect es bloqueado, de manera que no puede accederse a él ni puede ser visualizado.

VPN de inicio automático

Gracias al control de URL, las aplicaciones que requieren una conexión VPN para las actividades de negocio (incluido Safari) pueden crear un perfil VPN e iniciar o desconectar Mobile Connect automáticamente cuando se inician (se requiere firmware de servidor compatible). Además, con el fin de proporcionar una conexión segura y sencilla desde dispositivos iOS u OS X, la VPN a demanda inicia automáticamente una sesión SSL VPN segura cuando un usuario solicita datos, aplicaciones, páginas Web o hosts internos.

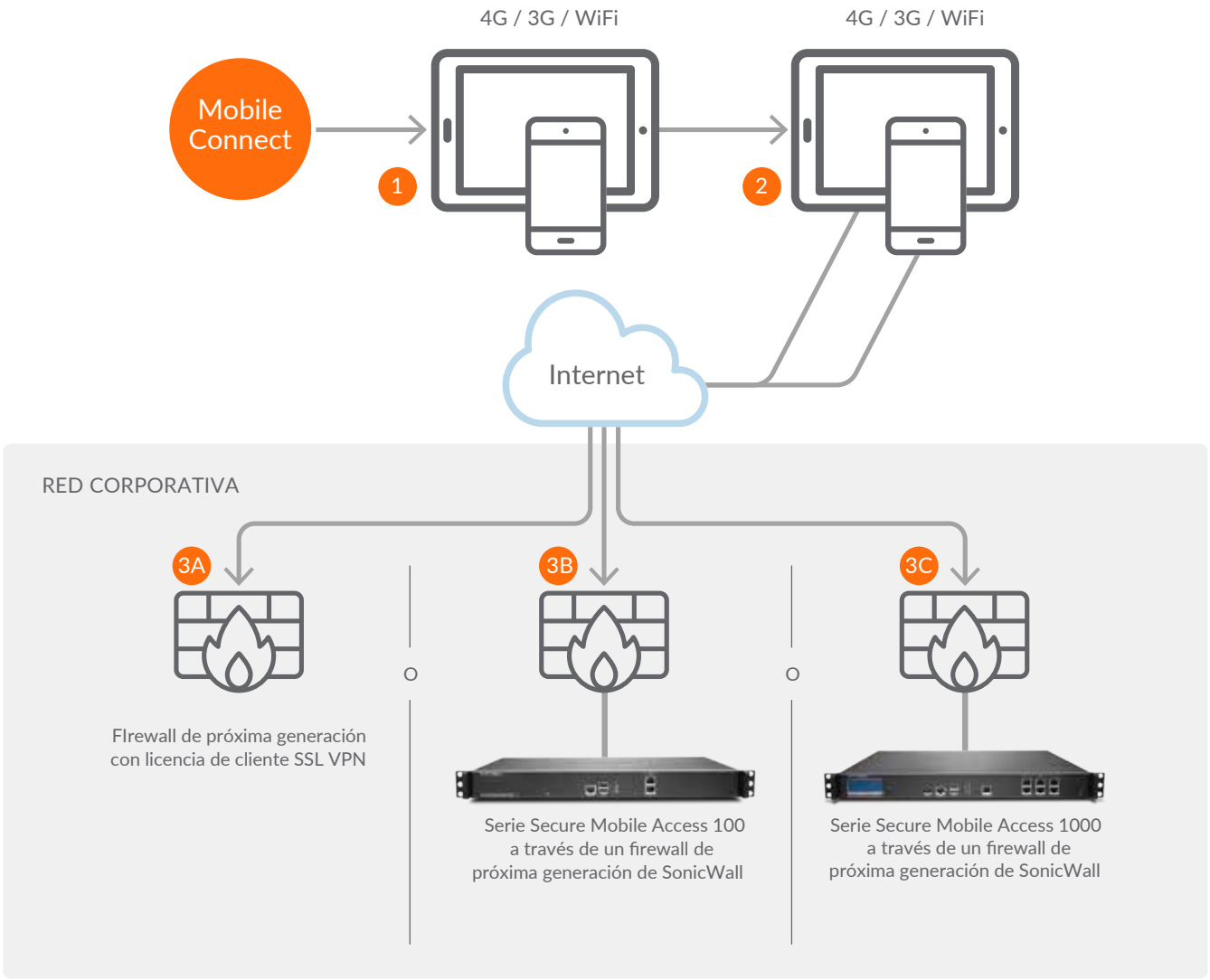
Integración con las soluciones de autenticación existentes

La solución de SonicWall soporta la integración sencilla con la mayoría de sistemas de autenticación back-end, como LDAP, Active Directory y Radius, para que pueda aplicar de manera eficaz las prácticas de autenticación que usted prefiera a sus trabajadores móviles. Para aumentar el nivel de seguridad, puede generar una contraseña de un solo uso e integrar fácilmente tecnologías de autenticación de doble factor en su solución.

Inteligencia y control de aplicaciones

Cuando se implementa con un firewall de próxima generación, esta prestación permite a los responsables de TI definir y reforzar reglas para el uso de las aplicaciones y del ancho de banda.

Acceso al software



1. Descargue e instale SonicWall Mobile Connect en su dispositivo móvil.
2. Cree un perfil de conexión para conectarse a su red corporativa.
3A. Conéctese a un firewall de próxima generación de SonicWall.

    Ventajas: Ofrece escaneo DPI antimalware, así como inteligencia y control de aplicaciones.

3B. Conéctese a un dispositivo de la serie SonicWall Secure Mobile Access 100 a través de un firewall de próxima generación de SonicWall.

    Ventajas: Ofrece escaneo DPI antimalware y control de puntos terminales para poner en cuarentena o rechazar las conexiones de los dispositivos móviles que hayan sido modificados mediante "jailbreaking" o rooteados.

3C. Conéctese a un dispositivo de la serie SonicWall Secure Mobile Access 1000 a través de un firewall de próxima generación de SonicWall.

    Ventajas: Ofrece escaneo DPI antimalware y control de puntos terminales para poner en cuarentena o rechazar las conexiones de los dispositivos móviles que hayan sido modificados mediante "jailbreaking" o rooteados. Asimismo, permite a los administradores restringir el acceso VPN a un conjunto de aplicaciones móviles de confianza y gestionar los términos de las políticas de seguridad BYOD reforzadas.

Prestaciones	iOS	OS X/ Mac	Android	Kindle Fire	Windows 8.1	Windows Phone 8.1	Windows 10	Chrome OS
Distribución de las aplicaciones	App Store	App Store de Mac	Google Play	App Store de Amazon	Preinstalado	Windows Phone Store	Windows Store	Chrome Web Store
Conectividad VPN capa 3 (SSL VPN)	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Conexión a demanda	Sí[3]	Sí[3]	—	—	Sí	Solo MDM	MDM/ PowerShell	Sí
Redes fiables configurables	Sí[3]	Sí[3]	—	—	Sí	Sí	Sí	—
Reconocimiento de redes	Sí[3]	Sí[3]	Sí[3]	Sí[3]	—	—	—	—
Caché de credenciales	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Soporte de Touch ID/huella dactilar	Sí[2]	—	Sí[2]	—	—	—	—	—
Soporte de Face ID	Sí	—	—	—	—	—	—	—
Control de URL	Sí	Sí	Sí	Sí	—	—	—	—
Autenticación básica (nombre de usuario/contraseña)	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Autenticación de doble factor (Dell Defender\TOTP\RADIUS)	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Autenticación de certificado de cliente	Sí[3]	Sí[3]	Sí[3]	Sí[3]	Sí	Sí	Sí	—
Cambio de contraseña	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
SSO en dominio Windows para VPN	—	—	—	—	Sí	Sí	Sí	—
Enrutamineto split-tunnel\tunnel-all	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Soporte para IPv6	Sí[4]	Sí[4]	Sí[4]	Sí[4]	Sí[4]	Sí[4]	Sí[4]	—
Compresión de datos mediante VPN	Sí[3]	Sí[3]	Sí[3]	Sí[3]	Sí[3]	Sí[3]	Sí[3]	Sí[3]
Modo ESP (transporte UDP)	Sí[3]	Sí[3]	Sí[3]	Sí[3]	—	—	—	—
Resolución de conflictos de red	Sí[3]	Sí[3]	Sí[3]	Sí[3]	Sí[3]	Sí[3]	Sí[3]	Sí[3]
End Point Control	Jailbreaking, Certificado, versión del SO, ID del dispositivo[3]	ID del dispositivo, versión del SO, certificado de cliente[1]	Root, Certificado, versión del SO, ID del dispositivo, software antivirus[3]	Root, Certificado, versión del SO, ID del dispositivo, software antivirus	ID del dispositivo, versión del SO[1]	ID del dispositivo, versión del SO[1]	ID del dispositivo, versión del SO[1]	ID del dispositivo, versión del SO[1]
Lector de archivos/ Marcadores	Sí[2]	—	Sí[2]	Sí[2]	—	—	—	—
Marcadores RDP	2X RDP, Microsoft Remote Desktop para RDP	—	2X RDP, Remote RDP Lite/ Enterprise, Microsoft Remote Desktop para RDP	2X RDP, Microsoft Remote Desktop para RDP	—	—	—	—
Marcadores de receptores Citrix	Sí[2]	—	Sí[2]	Sí[2]	—	—	—	—
Marcadores VNC	Remoter VNC	—	android-vnc-viewer	—	—	—	—	—
Marcadores Web	Safari, Chrome	—	Cualquier navegador—configurados en los ajustes del sistema Android	Navegador Silk	—	—	—	—
Marcadores de terminal	iSSH, Server Auditor para SSH	—	ConnectBot, JuideSSH	JuideSSH	—	—	—	—
Marcadores HTML5 nativos	RDP, VNC, SSH, Telnet[2]	—	RDP, VNC, SSH, Telnet[2]	—	—	—	—	—
Gestión MDM de perfiles de conexiones VPN	Sí	—	—	—	Sí	Sí	Sí	Consola de gestión de Google

[1] *Solo soportan esta prestación los dispositivos de las series E-Class SRA/SMA 1000. Consulte las notas de la versión para informarse sobre la versión de software específico necesaria para soportar esta prestación.*
[2] *Solo soportan esta prestación los dispositivos de las series SRA/SMA 100.*
[3] *Solo soportan esta prestación los dispositivos de las series SRA/SMA 100 y E-Class SRA/SMA 1000. Consulte las notas de la versión para informarse sobre la versión de software específico necesaria para soportar esta prestación.*
[4] *Solo soportan esta prestación los dispositivos de las series SRA/SMA 100, E-Class SRA/SMA 1000 y los firewalls de próxima generación. Consulte las notas de la versión para informarse sobre la versión específica de software necesaria para soportar esta prestación.*

Acerca de nosotros

SonicWall lleva más de 25 años combatiendo la industria del crimen cibernético, defendiendo a las empresas pequeñas, medianas y grandes de todo el mundo. Nuestra combinación de productos y partners nos ha permitido crear una solución de defensa cibernética en tiempo real adaptada a las necesidades específicas de más de 500.000 negocios en más de 150 países, para que usted pueda centrarse por completo en su negocio sin tener que preocuparse por las amenazas.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Para más información, consulte nuestra página Web.
www.sonicwall.com

Datasheet-MobileConnectSMA200_400-US-KJ-MKTG3044