SonicWall Mobile Connect

Einfacher, regelbasierter und sicherer Zugriff auf geschäftskritische Anwendungen und Daten für iOS-, OS X-, Android-, Chrome OS-, Kindle Fire- und Windows-Mobilgeräte

Bieten Sie Ihren Mitarbeitern einen geschützten und einfachen Zugriff auf alle benötigten Daten und Ressourcen von einer Vielzahl an Geräten wie iOS, OS X, Android™, Chrome OS, Kindle Fire und Windows. Ihre Mitarbeiter können so ihre Produktivität steigern, während Sie Ihr Unternehmensnetzwerk vor mobilen Sicherheitsbedrohungen schützen.

Die SonicWall™ Mobile Connect™-Anwendung lässt sich mit SonicWall Secure Mobile Access (SMA) oder Next-Generation Firewall-Appliances kombinieren. Mobile Mitarbeiter müssen nur die Mobile Connect-Anwendung auf ihrem iOS-, OS X-, Android-, Chrome OS- oder Windows-Mobilgerät installieren und ausführen, um eine sichere Verbindung zu einer SMA- oder Next-Generation Firewall-Appliance herzustellen. Die verschlüsselte SSL-VPN-Verbindung sorgt dafür, dass der Verkehr nicht abgefangen wird und die Daten während der Übertragung sicher sind. Eine kontextsensible Authentifizierung garantiert, dass nur autorisierte Benutzer und vertrauenswürdige Geräte Zugang erhalten.

Mit den SonicWall-Appliances kann die IT im Hintergrund spielend leicht über eine einzige Verwaltungsoberfläche Zugriffsregeln erstellen und verwalten. So kann der Administrator den VPN-Zugriff auf bestimmte vertrauenswürdige mobile Apps einschränken. Außerdem lässt sich die SonicWall-Lösung ohne Weiteres mit den meisten Backend-Authentifizierungssystemen – einschließlich Zwei-Faktor-Authentifizierung – integrieren. Auf diese Weise können Sie Ihre bevorzugten Authentifizierungsmethoden effizient für Ihre mobilen Mitarbeiter nutzen.

Funktionen und Vorteile

Leichte Handhabung

iOS-, OS X-, Windows 10-, Android-, Chrome OS- und Kindle-Nutzer können die Mobile Connect-App einfach im App Store™, Chrome Web Store, Amazon App Store, Windows Store oder über Google Play herunterladen und installieren. Anwender von Windows 8.1-Mobilgeräten haben es sogar noch leichter: Mobile Connect ist bereits im Windows 8.1-Betriebssystem eingebettet, sodass keine weitere VPN-Client-App heruntergeladen und installiert werden muss.

Zentralisierte Regelverwaltung

Mit den SonicWall-Appliances kann die IT den mobilen Zugriff über eine einzige Oberfläche bereitstellen und verwalten, wobei sie u. a. die Kontrolle über sämtliche Web- und Client-Server-Ressourcen sowie Dateifreigaben behält. Im Gegensatz zu anderen VPN-Lösungen können Sie mit SonicWall innerhalb kurzer Zeit rollenbasierte Richtlinien für sämtliche Mobilgeräte, Laptops und Nutzer mit einer einzigen Regel für alle Objekte definieren. Damit lässt sich der Aufwand für das Policy-Management von mehreren Stunden auf nur wenige Minuten reduzieren.

Nutzer- und Geräteauthentifizierung

Der Zugriff auf das Unternehmensnetzwerk wird erst dann gewährt, wenn der Mobile Connect-Nutzer authentifiziert und die Integrität des Mobilgeräts verifiziert wurden. Mittels End Point Control lässt sich ermitteln, ob ein iOS-Gerät per Jailbreaking verändert oder ein Android-Gerät „gerootet“ wurde, ob ein Zertifikat vorhanden ist oder ob die Version des Betriebssystems aktuell ist. Im Verdachtsfall wird die Verbindung abgewiesen oder unter Quarantäne gestellt.

Vorteile:

- Hohe Benutzerfreundlichkeit
- Zentralisierte Richtlinienverwaltung
- Nutzer- und Geräteauthentifizierung
- Einfacher Zugriff auf zugelassene Ressourcen
- Malware-Schutz
- Anmeldung von Mobilgeräten und Autorisierungsverwaltung
- Per-App-VPN
- Sicheres Durchsuchen von Dateien im Intranet und integrierte Datensicherheit mit nur einem Klick
- Autostart-VPN
- Einfache Integration
- Application Intelligence and Control

Schneller und sicherer mobiler Zugriff über eine intuitive, benutzerfreundliche App, die sich sowohl auf Smartphones als auch auf Tablets einfach installieren und starten lässt.

Kompatibilitätsdaten

SonicWall SMA und Next-Generation Firewall
Appliances der TZ, NSA, E-Class NSA oder Super Massive 9000 Series mit SonicOS 5.9, 6.2 oder höher
Appliances der SMA 100 Series/ SRA mit 7.5 oder höher
Appliances der SMA 1000 Series/ E-Class SRA mit 10.7 oder höher

SonicWall Mobile Connect
Geräte mit iOS 7.0 oder höher
Geräte mit OS X 10.9 oder höher
Geräte mit Android 4.1 oder höher
Kindle Fire-Geräte auf Basis von Android 4.1 oder höher
Geräte mit ChromeOS 45 oder höher
Geräte mit Windows 8.1
Geräte mit Windows Phone 8.1
Geräte mit Windows 10

Einfacher Zugriff auf zugelassene Ressourcen

iOS-, Android-, Chrome OS-, Kindle- und Windows-Mobilgeräte können auf alle freigegebenen Netzwerkressourcen zugreifen, darunter web-, server-, hostbasierte und Client-Server-Anwendungen sowie Back-Connect-Applikationen. Sobald der Nutzer und das Gerät geprüft wurden, stellt Mobile Connect vorkonfigurierte Lesezeichen bereit. So kann der Nutzer mit nur einem Mausklick auf die Unternehmensanwendungen und -ressourcen zugreifen, für die er und das Gerät Zugriffsrechte haben.

Malware-Schutz

Bei Einsatz mit einer SonicWall Next-Generation Firewall stellt Mobile Connect ein Clean VPN™ bereit, das als zusätzliche Schutzschicht sämtlichen SSL-VPN-Verkehr entschlüsselt und auf Malware überprüft, bevor dieser das Netzwerk erreicht.

Anmeldung von Mobilgeräten sowie Verwaltung der Autorisierungsrichtlinien

Mit Mobile Connect und Secure Mobile Access OS (Versionen 11.0 und höher) für Secure Mobile Access 1000 Series-Appliances: Wurde das Mobilgerät zuvor nicht auf einer SMA-Appliance angemeldet, wird der Nutzer, bevor er auf das Netzwerk zugreifen kann, dazu aufgefordert, den Richtlinien für die Geräte-Autorisierung zuzustimmen. Der Nutzer muss den Richtlinien zustimmen, um das Gerät anzumelden und Zugriff auf zugelassene Unternehmensdaten und -ressourcen zu erhalten. Die Richtlinien können durch den Administrator angepasst werden.

Per-App-VPN

Mobile Connect ermöglicht es Administratoren, in Kombination mit Secure Mobile Access OS (Versionen 11.0 und höher) für Secure Mobile Access 1000 Series-Appliances Regeln zu erstellen und durchzusetzen. So können sie bestimmen, welchen Apps auf einem Mobilgerät ein VPN-Zugriff auf das Netzwerk gewährt wird. Auf diese Weise wird sichergestellt, dass nur autorisierte mobile Geschäftsanwendungen den VPN-Zugriff nutzen. Mobile Connect ist die einzige Lösung, die für den Per-App-VPN-Zugriff keine Änderungen an mobilen Apps erfordert. Sämtliche mobile Apps oder sichere Container können ohne Modifizierungen, App-Wrapping oder SDK unterstützt werden.

Sicheres Durchsuchen von Dateien im Intranet und integrierte Datensicherheit mit nur einem Klick

Schützen Sie gespeicherte Unternehmensdaten auf Mobilgeräten. Authentifizierte Benutzer können zugelassene Intranetdateifreigaben und Dateien innerhalb der Mobile Connect-Anwendung sicher durchsuchen und anzeigen. Administratoren können für Mobile Connect Regeln zur Verwaltung mobiler Anwendungen erstellen und durchsetzen. Auf diese Weise lässt sich kontrollieren, ob die angezeigten Dateien auch in anderen Anwendungen geöffnet, in die Zwischenablage kopiert, gedruckt oder in der Mobile Connect-Anwendung sicher zwischengespeichert werden können. Dies ermöglicht die Trennung von Unternehmensdaten und privat genutzten Daten auf iOS-Geräten und minimiert das Risiko von Datenverlusten. Wenn außerdem die Zugriffsrechte des Benutzers widerrufen wurden, werden in Mobile Connect gespeicherte Inhalte gesperrt und können nicht mehr genutzt oder angezeigt werden.

Autostart-VPN

URL-Kontrolle ermöglicht Anwendungen, die eine VPN-Verbindung für den geschäftlichen Einsatz benötigen (einschließlich Safari), ein VPN-Profil zu erstellen und Mobile Connect beim Starten automatisch aufzurufen oder zu beenden (erfordert kompatible Server-Firmware). Wird eine sichere Verbindung bei einem iOS- oder OS X-Gerät benötigt, startet VPN on Demand automatisch eine sichere SSL-VPN-Sitzung, sobald ein Benutzer interne Daten, Applikationen, Websites oder Hosts aufruft.

Integration mit bestehenden Authentifizierungslösungen

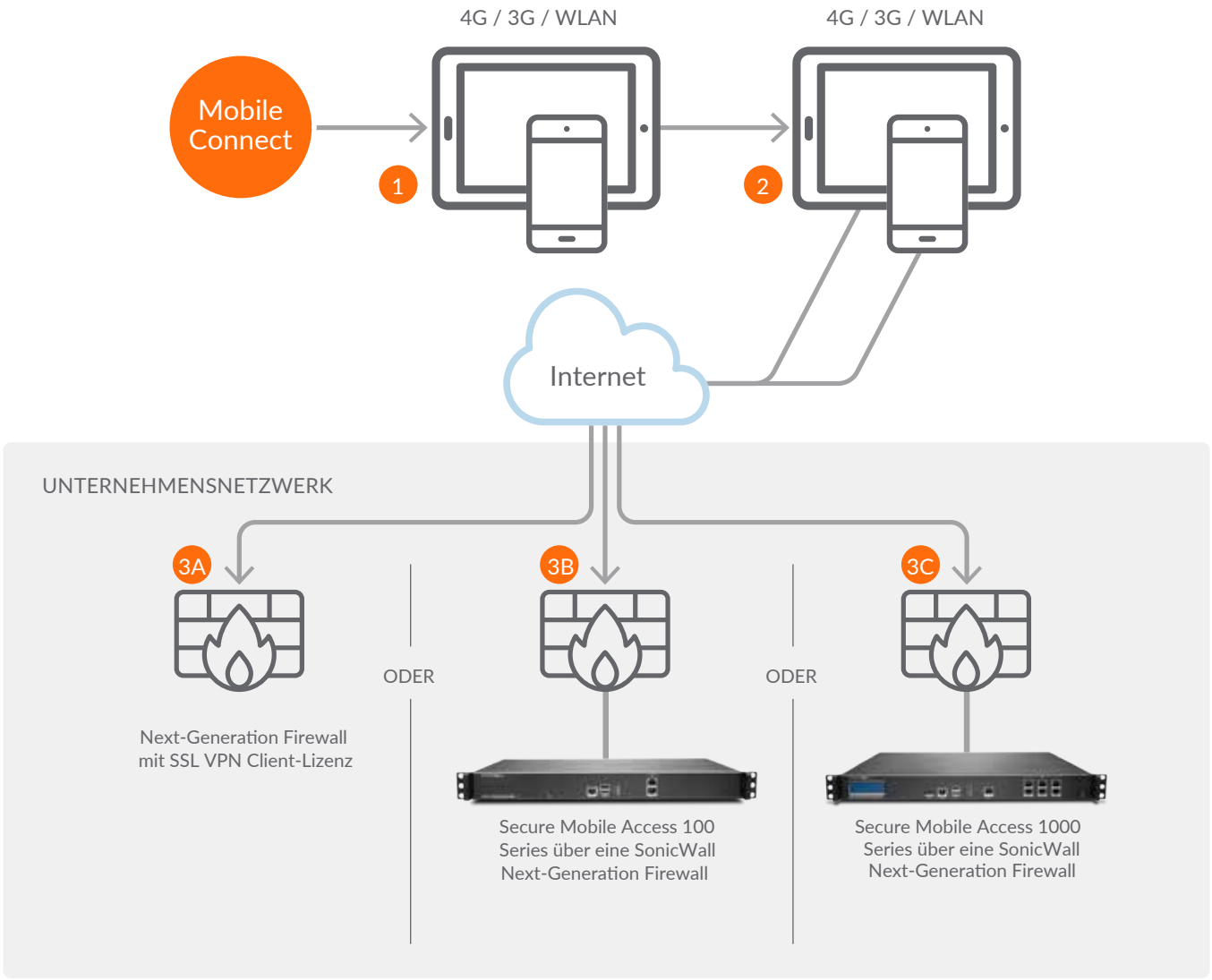
Die SonicWall-Lösung lässt sich ohne Weiteres mit den meisten Backend-Authentifizierungssystemen wie LDAP, Active Directory und Radius integrieren. Auf diese Weise können Sie Ihre bevorzugten Authentifizierungsmethoden effizient für Ihre mobilen Mitarbeiter nutzen. Um die Sicherheit zu verbessern, können einfach Einmalpasswörter generiert und Zwei-Faktor-Authentifizierungstechnologien integriert werden.

Application Intelligence and Control

Bei Einsatz mit einer Next-Generation Firewall kann der IT-Administrator spielend leicht festlegen und kontrollieren, wie die Anwendungs- und Bandbreitenressourcen genutzt werden.

SONICWALL®

Software-Verfügbarkeit



1. Laden Sie SonicWall Mobile Connect herunter und installieren Sie es auf Ihrem Mobilgerät.
2. Erstellen Sie für Verbindungen zum Unternehmensnetzwerk ein Verbindungsprofil.
3A. Verbinden Sie sich mit einer SonicWall Next-Generation Firewall.
   Vorteile: Bietet eine DPI-Prüfung auf Malware sowie Application Intelligence and Control.
3B. Verbinden Sie sich mit einer SonicWall Secure Mobile Access 100 Series-Appliance über eine SonicWall Next-Generation Firewall.
   Vorteile: Bietet eine DPI-Prüfung auf Malware. Mit der Funktion End Point Control werden außerdem Verbindungen von Mobilgeräten, die „gerootet" oder per Jailbreaking verändert wurden, abgewiesen oder unter Quarantäne gestellt.
3C. Verbinden Sie sich mit einer SonicWall Secure Mobile Access 1000 Series-Appliance über eine SonicWall Next-Generation Firewall.
   Vorteile: Bietet eine DPI-Prüfung auf Malware. Mit der Funktion End Point Control werden außerdem Verbindungen von Mobilgeräten, die „gerootet" oder per Jailbreaking verändert wurden, abgewiesen oder unter Quarantäne gestellt. Darüber hinaus können Administratoren den VPN-Zugriff auf eine zugelassene Auswahl vertrauenswürdiger mobiler Apps einschränken und BYOD-Sicherheitsrichtlinien verwalten und durchsetzen.

Funktionen	iOS	OS X / Mac	Android	Kindle Fire	Windows 8.1	Windows Phone 8.1	Windows 10	Chrome OS
App-Distribution	App Store	Mac App Store	Google Play	Amazon App Store	Vorinstalliert	Windows Phone Store	Windows Store	Chrome Web Store
Layer-3-VPN-Konnektivität (SSL-VPN)	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
Connect on Demand	Ja[3]	Ja[3]	—	—	Ja	Nur MDM	MDM/ PowerShell	Ja
Konfigurierbare, vertrauenswürdige Netzwerke	Ja[1]	Ja[1]	—	—	Ja	Ja	Ja	—
Netzwerkerkennung	Ja[1]	Ja[1]	Ja[1]	Ja[1]	—	—	—	—
Zwischenspeicherung von Authentifizierungsdaten	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
Touch ID-/Fingerprint-Unterstützung	Ja[2]	—	Ja[2]	—	—	—	—	—
Face ID-Unterstützung	Ja	—	—	—	—	—	—	—
URL-Kontrolle	Ja	Ja	Ja	Ja	—	—	—	—
Basisauthentifizierung (Benutzername/Passwort)	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
Zwei-Faktor-Authentifizierung (Dell Defender\TOTP\RADIUS)	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
Client-Zertifikat-Authentifizierung	Ja[3]	Ja[3]	Ja[3]	Ja[3]	Ja	Ja	Ja	—
Passwortänderung	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
Windows Domain SSO für VPN	—	—	—	—	Ja	Ja	Ja	—
Split-Tunnel/„Tunnel all"-Routing	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
IPv6-Unterstützung	Ja[4]	Ja[4]	Ja[4]	Ja[4]	Ja[4]	Ja[4]	Ja[4]	—
Datenkomprimierung über VPN	Ja[3]	Ja[3]	Ja[3]	Ja[3]	Ja[1]	Ja[1]	Ja[1]	Ja[3]
ESP-Modus (UDP-Transport)	Ja[1]	Ja[1]	Ja[1]	Ja[1]	—	—	—	—
Lösung von Netzwerkkonflikten	Ja[1]	Ja[1]	Ja[1]	Ja[1]	Ja[1]	Ja[1]	Ja[1]	Ja[1]
End Point Control	Jailbreak, Zertifikat, OS-Version, Geräte-ID[2]	Geräte-ID OS-Version, Client-Zertifikat[1]	Root, Zertifikat, OS-Version, Geräte-ID, Anti-virensoftware[3]	Root, Zertifikat, OS-Version, Geräte-ID, Anti-virensoftware	Geräte-ID, OS-Version[1]	Geräte-ID, OS-Version[1]	Geräte-ID, OS-Version[1]	Geräte-ID, Chrome OS-Version[1]
File-Reader / Lesezeichen	Ja[2]	—	Ja[2]	Ja[2]	—	—	—	—
RDP-Lesezeichen	2X RDP, Microsoft Remote Desktop für RDP	—	2X RDP, Remote RDP Lite/ Enterprise, Microsoft Remote Desktop für RDP	2X RDP, Microsoft Remote Desktop für RDP	—	—	—	—
Citrix Receiver-Lesezeichen	Ja[2]	—	Ja[2]	Ja[2]	—	—	—	—
VNC-Lesezeichen	Remoter VNC	—	android-vnc-viewer	—	—	—	—	—
Web-Lesezeichen	Safari, Chrome	—	Jeder Browser – in den Android-Systemeinstellungen konfiguriert	Silk Browser	—	—	—	—
Terminal-Lesezeichen	iSSH, Serverauditor für SSH	—	ConnectBot, JuideSSH	JuideSSH	—	—	—	—
Native HTML5-Lesezeichen	RDP, VNC, SSH, Telnet[2]	—	RDP, VNC, SSH, Telnet[2]	—	—	—	—	—
Mobile-Device-Management von VPN-Verbindungsprofilen	Ja	—	—	—	Ja	Ja	Ja	Google Mgmt Console

[1] *Diese Funktion wird nur auf den Appliances der E-Class SRA/SMA 1000 Series unterstützt. Angaben darüber, welche Softwareversion diese Funktion unterstützt, entnehmen Sie bitte den Versionsinformationen.*
[2] *Diese Funktion wird nur auf den Appliances der SRA/SMA 100 Series unterstützt.*
[3] *Diese Funktion wird nur auf den Appliances der SRA/SMA 100 Series und E-Class SRA/SMA 1000 Series unterstützt. Angaben darüber, welche Softwareversion diese Funktion unterstützt, entnehmen Sie bitte den Versionsinformationen.*
[4] *Diese Funktion wird auf den Appliances der SRA/SMA 100 Series und E-Class SRA/SMA 1000 Series sowie auf Next-Generation Firewalls unterstützt. Angaben darüber, welche Softwareversion diese Funktion unterstützt, entnehmen Sie bitte den Versionsinformationen.*

Über uns

Seit über 25 Jahren schützt SonicWall kleine, mittlere und große Unternehmen weltweit vor Cyberkriminalität. Mit unseren Produkten und Partnerschaften können wir eine Echtzeit-Cyberabwehrlösung für die individuellen Anforderungen von über 500.000 Organisationen in über 150 Ländern bereitstellen, damit sie sich voll und ganz auf ihr Geschäft konzentrieren können.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, Kalifornien 95035, USA
Weitere Informationen erhalten Sie auf unserer Website.
www.sonicwall.com

Datasheet-MobileConnectSMA200_400-US-KJ-MKTG3044