SonicWall Mobile Connect

Semplice accesso protetto con policy alle applicazioni e ai dati strategici per dispositivi iOS, OS X, Android, Chrome OS, Kindle Fire e Windows.

Offrite ai vostri dipendenti la possibilità di accedere in modo facile e sicuro ai dati e alle risorse di cui hanno bisogno per essere produttivi da una vasta gamma di dispositivi, tra cui iOS, OS X, Android™, Chrome OS, Kindle Fire e Windows. Al tempo stesso, assicuratevi che la rete aziendale sia protetta dalle minacce alla sicurezza mobile.

L'applicazione SonicWall™ Mobile Connect™ funziona in combinazione con SonicWall Secure Mobile Access (SMA) o dispositivi firewall di nuova generazione. I lavoratori mobili installano e lanciano l'applicazione Mobile Connect sui propri dispositivi iOS, OS X, Android, Chrome OS o Windows per stabilire una connessione sicura a una SMA o ad un dispositivo firewall di nuova generazione. La connessione SSL VPN crittografata evita quindi che il traffico venga intercettato e garantisce la sicurezza dei dati durante il trasferimento. L'autenticazione basata sul contesto garantisce che solo gli utenti autorizzati e i dispositivi fidati possano accedere.

Dietro le quinte, l'IT può facilmente fornire e gestire le politiche di accesso tramite le appliance SonicWall attraverso un'unica interfaccia di gestione, ad esempio limitare l'accesso VPN a una serie di app mobili attendibili consentite dall'amministratore. Inoltre, la soluzione SonicWall si integra facilmente con la maggior parte dei sistemi di autenticazione back-end, inclusa l'autenticazione a due fattori, in modo da poter estendere in modo efficiente le pratiche di autenticazione preferite ai lavoratori mobili.

Caratteristiche e vantaggi

Facilità d'uso

Gli utenti iOS, OS X, Windows 10, Android, Chrome OS e Kindle possono facilmente scaricare e installare l'app Mobile Connect dall'App Store™, da Google Play, Chrome Web Store, Amazon App Store o Windows Store. Per gli utenti di dispositivi mobili Windows 8.1, Mobile Connect è incorporato nel sistema operativo Windows 8.1, pertanto non è necessario scaricare e installare un'altra app client VPN.

Gestione centralizzata delle policy

L'IT può fornire e gestire l'accesso ai dispositivi mobili tramite dispositivi SonicWall, incluso il controllo di tutte le risorse Web, le condivisioni dei file e le risorse client-server, attraverso un'unica interfaccia di gestione. A differenza di altre soluzioni VPN, la soluzione SonicWall consente di impostare rapidamente criteri basati sui ruoli per dispositivi mobili e portatili e utenti con un'unica regola su tutti gli oggetti; di conseguenza, la gestione delle policy può richiedere solo pochi minuti anziché ore.

Verifica di utente e dispositivo

Un utente di Mobile Connect riceve l'autorizzazione di accesso alla rete aziendale solo dopo l'autenticazione dell'utente e la verifica dell'integrità del dispositivo mobile. L'End Point Control è in grado di determinare se un dispositivo iOS è stato sottoposto a jailbreak o se è stato effettuato il root di un dispositivo Android, se un certificato è presente o se la versione del sistema operativo è aggiornata e, quindi, rifiutare o mettere in quarantena la connessione a seconda delle necessità.

Vantaggi:

- Facilità d'uso
- Gestione centralizzata delle policy
- Verifica di utente e dispositivo
- Facile accesso alle risorse appropriate
- Protezione anti-malware
- Registrazione dei dispositivi mobili e gestione delle policy di autorizzazione
- VPN per ogni applicazione
- Navigazione dei file intranet protetta con un clic e protezione dei dati su dispositivo
- Avvio automatico della VPN
- Facile integrazione
- Application Intelligence and Control

Fornite un accesso mobile rapido e sicuro per mezzo di un'app intuitiva e facile da usare, semplice da installare e da avviare su smartphone e tablet.

Compatibilità delle specifiche

SonicWall SMA e firewall di nuova generazione
Appliance serie TZ, NSA, E-Class NSA o Super Massive 9000 con sistema operativo SonicOS 5.9, 6.2 o superiore
Appliance serie SMA 100/ appliance SRA con versione 7.5 o superiore
Appliance serie SMA 1000/ appliance E-Class SRA con versione 10.7 o superiore

SonicWall Mobile Connect
Dispositivi con iOS versione 7.0 o superiore
Dispositivi con OS X 10.9 o superiore
Dispositivi con Android 4.1 o superiore
Dispositivi Kindle Fire basati su Android 4.1 o superiore
Dispositivi con ChromeOS 45 o superiore
Dispositivi con Windows 8.1
Dispositivi con Windows Phone 8.1
Dispositivi con Windows 10

Facile accesso alle risorse appropriate

I dispositivi mobili iOS, Android, Chrome OS, Kindle e Windows possono connettersi a tutte le risorse di rete consentite, incluse le applicazioni basate sul Web, client/server, basate su server, su host e back-connect. Dopo aver verificato utente e dispositivo, Mobile Connect propone segnalibri preconfigurati per l'accesso con un solo clic alle applicazioni e alle risorse aziendali per le quali l'utente e il dispositivo dispongono dei privilegi.

Protezione anti-malware

Quando viene implementato con un firewall SonicWall di nuova generazione, Mobile Connect stabilisce una Clean VPN™, un ulteriore livello di protezione che decodifica e analizza tutto il traffico SSL VPN alla ricerca del malware prima che entri nella rete.

Registrazione dei dispositivi mobili e gestione delle policy di autorizzazione

Con Mobile Connect e il sistema operativo Secure Mobile Access (versioni 11.0 e successive) per le appliance Secure Mobile Access della serie 1000, prima di concedere l'accesso alla rete, all'utente viene presentata una policy di autorizzazione da accettare per la periferica, se il dispositivo mobile non è stato precedentemente registrato con l'appliance SMA. L'utente deve accettare i termini della policy per registrare il dispositivo e ottenere l'accesso alle risorse e ai dati aziendali consentiti. I termini della policy sono personalizzabili da parte dell'amministratore.

VPN per ogni applicazione

Mobile Connect in combinazione con il sistema operativo Secure Mobile Access (versioni 11.0 e successive) per appliance Secure Mobile Access della serie 1000 consente agli amministratori di stabilire e applicare policy per designare quali app su un dispositivo mobile possono ottenere l'accesso VPN alla rete. In tal modo si garantisce che solo le app aziendali autorizzate per uso mobile utilizzino l'accesso VPN. Mobile Connect è l'unica soluzione che non richiede alcuna modifica delle app mobili per un accesso VPN per ogni app. Qualsiasi app mobile o contenitore sicuro può essere supportato senza modifiche, wrapping delle app o sviluppo SDK.

Navigazione dei file intranet protetta con un clic e protezione dei dati su dispositivo

Consente di proteggere i dati aziendali conservati sui dispositivi mobili. Gli utenti autenticati possono navigare e visualizzare in modo sicuro le condivisioni dei file nell'intranet e i file stessi consentiti dall'app Mobile Connect. Gli amministratori possono stabilire e applicare le policy di gestione delle applicazioni mobili in modo che l'app Mobile Connect controlli se i file visualizzati possono essere aperti in altre app, copiati negli appunti, stampati o memorizzati nella cache in modo sicuro all'interno dell'app Mobile Connect. Per i dispositivi iOS, questo consente agli amministratori di isolare i dati aziendali dai dati personali memorizzati sul dispositivo e riduce il rischio di perdita di dati. Inoltre, se le credenziali dell'utente vengono revocate, i contenuti memorizzati nell'app Mobile Connect sono bloccati e non possono più essere consultati o visualizzati.

Avvio automatico della VPN

Il controllo URL consente alle app che richiedono una connessione VPN per l'attività lavorativa (incluso Safari) di creare un profilo VPN e di avviare o disconnettere automaticamente Mobile Connect all'avvio (richiede firmware del server compatibile). Inoltre, per dispositivi iOS o OS X, per semplificare l'utilizzo quando è richiesta una connessione protetta, VPN on Demand avvia automaticamente una sessione SSL VPN protetta quando un utente richiede dati interni, applicazioni, siti Web o host.

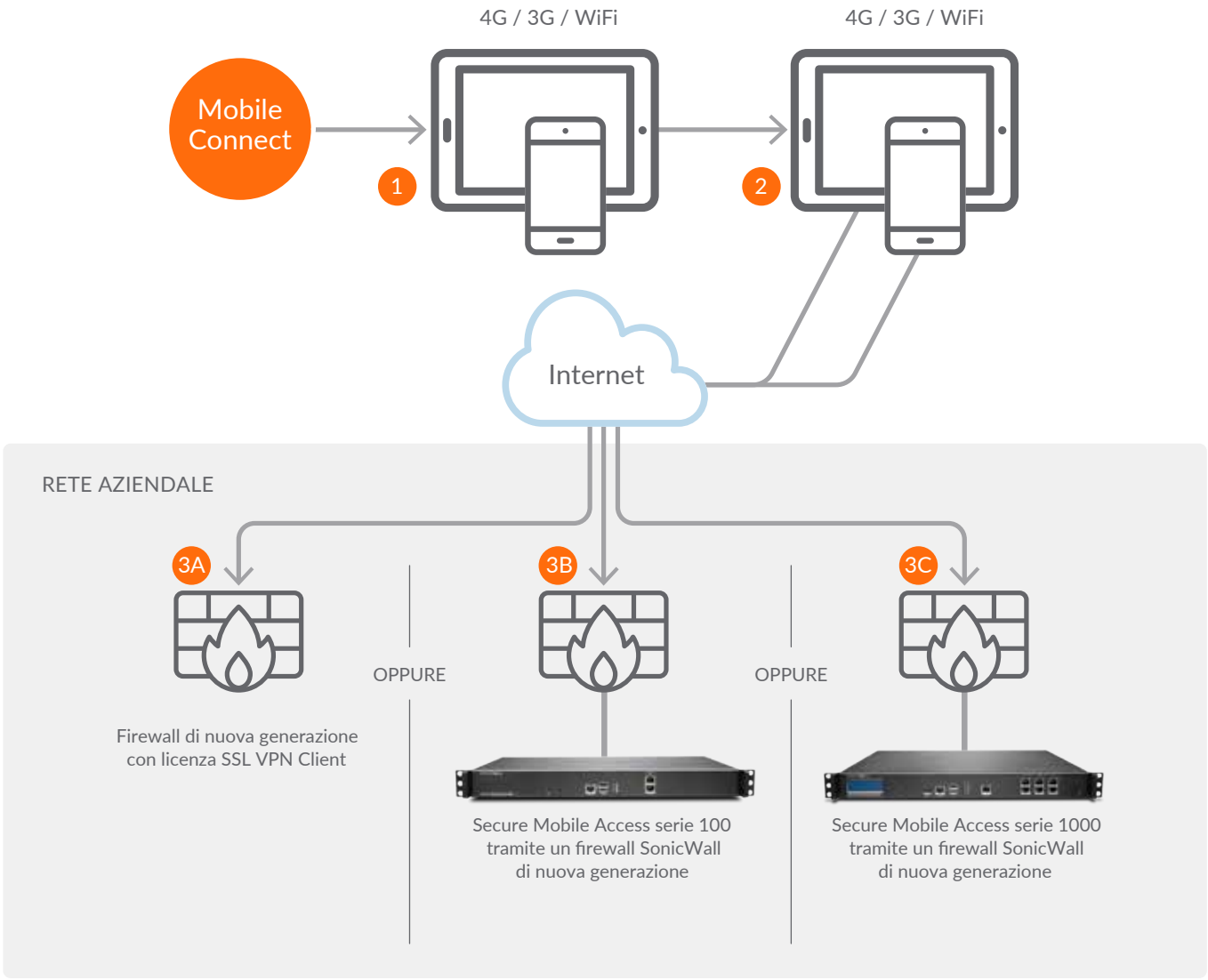
Integrazione con soluzioni di autenticazione esistenti

La soluzione SonicWall supporta una facile integrazione con la maggior parte dei sistemi di autenticazione back-end, come LDAP, Active Directory e Radius, in modo da poter estendere in modo efficiente le pratiche di autenticazione preferite ai lavoratori mobili. Per una maggiore sicurezza, è possibile abilitare la generazione di password *una tantum* e ottenere una facile integrazione con tecnologie di autenticazione a due fattori.

Application Intelligence and Control

In caso di implementazione con un firewall di nuova generazione, l'IT può facilmente definire ed attuare la modalità di utilizzo delle risorse delle applicazioni e della larghezza di banda.

Disponibilità del software



1. Scaricare e installare SonicWall Mobile Connect sul dispositivo mobile.
2. Creare un profilo di connessione per collegarsi alla propria rete aziendale.
3A. Connettersi a un firewall di nuova generazione di SonicWall.
   Vantaggi: fornisce la scansione DPI alla ricerca del malware ed Application Intelligence and Control.
3B. Collegarsi a un'appliance SonicWall Secure Mobile Access serie 100 tramite un firewall di nuova generazione SonicWall.
   Vantaggi: fornisce la scansione DPI alla ricerca del malware e il controllo degli endpoint per mettere in quarantena o rifiutare le connessioni dai dispositivi mobili sottoposti a jailbreak o root.
3C. Collegarsi a un'appliance SonicWall Secure Mobile Access serie 1000 tramite un firewall di nuova generazione SonicWall.
   Vantaggi: fornisce la scansione DPI alla ricerca del malware e il controllo degli endpoint per mettere in quarantena o rifiutare le connessioni dai dispositivi mobili sottoposti a jailbreak o root. Inoltre consente agli amministratori di limitare l'accesso VPN a un set consentito di app mobili affidabili e di gestire i termini delle policy di sicurezza BYOD applicate.

Funzionalità	iOS	OS X/Mac	Android	Kindle Fire	Windows 8.1	Windows Phone 8.1	Windows 10	Chrome OS
Distribuzione app	App Store	Mac App Store	Google Play	Amazon App Store	In scatola	Windows Phone Store	Windows Store	Chrome Web Store
Connettività VPN Layer-3 (SSL VPN)	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
Connect on Demand	Sì[3]	Sì[3]	—	—	Sì	Solo MDM	MDM/ PowerShell	Sì
Reti affidabili configurabili	Sì[3]	Sì[3]	—	—	Sì	Sì	Sì	—
Network awareness	Sì[3]	Sì[3]	Sì[4]	Sì[4]	—	—	—	—
Caching delle credenziali	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
Supporto Touch ID/impronte digitali	Sì[2]	—	Sì[2]	—	—	—	—	—
Supporto Face ID	Sì	—	—	—	—	—	—	—
Controllo URL	Sì	Sì	Sì	Sì	—	—	—	—
Autenticazione di base (nome utente\password)	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
Autenticazione a due fattori (Dell Defender\TOTP\RADIUS)	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
Autenticazione certificato client	Sì[3]	Sì[3]	Sì[3]	Sì[3]	Sì	Sì	Sì	—
Cambio password	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
SSO dominio Windows per VPN	—	—	—	—	Sì	Sì	Sì	—
Routing split-tunnel\tunnel-all	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
Supporto IPv6	Sì[4]	Sì[4]	Sì[4]	Sì[4]	Sì[4]	Sì[4]	Sì[4]	—
Compressione dei dati su VPN	Sì[3]	Sì[3]	Sì[3]	Sì[3]	Sì[3]	Sì[3]	Sì[3]	Sì[3]
Modalità ESP (trasporto UDP)	Sì[3]	Sì[3]	Sì[3]	Sì[3]	—	—	—	—
Risoluzione dei conflitti di rete	Sì[3]	Sì[3]	Sì[3]	Sì[3]	Sì[3]	Sì[3]	Sì[3]	Sì[3]
End Point Control	Jailbreak, certificato, versione del sistema operativo, DeviceID[2]	DeviceID, versione del sistema operativo, certificato client[4]	Root, certificato, versione del sistema operativo, DeviceID, software anti-virus[3]	Root, certificato, versione del sistema operativo, DeviceID, software anti-virus	DeviceID, versione del sistema operativo[3]	DeviceID, versione del sistema operativo[3]	DeviceID, versione del sistema operativo[3]	DeviceID, versione di Chrome OS[3]
Lettore di file/segnalibri	Sì[2]	—	Sì[2]	Sì[2]	—	—	—	—
Segnalibri RDP	2X RDP, Microsoft Remote Desktop per RDP	—	2X RDP, Remote RDP Lite/ Enterprise, Microsoft Remote Desktop per RDP	2X RDP, Microsoft Remote Desktop per RDP	—	—	—	—
Segnalibri ricevitore Citrix	Sì[2]	—	Sì[2]	Sì[2]	—	—	—	—
Segnalibri VNC	Remoter VNC	—	android-vnc-viewer	—	—	—	—	—
Segnalibri Web	Safari, Chrome	—	Qualsiasi browser; configurato nelle impostazioni di sistema Android	Silk Browser	—	—	—	—
Segnalibri del terminale	iSSH, Server Auditor per SSH	—	ConnectBot, JuideSSH	JuideSSH	—	—	—	—
Segnalibri HTML5 nativi	RDP, VNC, SSH, Telnet[2]	—	RDP, VNC, SSH, Telnet[2]	—	—	—	—	—
Gestione MDM dei profili di connessione VPN	Sì	—	—	—	Sì	Sì	Sì	Console Google Mgmt

[1] *Questa caratteristica è supportata solo sulle appliance della serie E-Class SRA/SMA 1000. Consultare le note sulla versione del prodotto per la versione del software specifica richiesta per supportare questa caratteristica.*
[2] *Questa caratteristica è supportata solo sulle appliance della serie SRA/SMA 100.*
[3] *Questa caratteristica è supportata solo sulle appliance della serie SRA/SMA 100 e della serie E-Class SRA/SMA 1000. Consultare le note sulla versione del prodotto per la versione del software specifica richiesta per supportare questa caratteristica.*
[4] *Questa caratteristica è supportata sulle appliance della serie SRA/SMA 100, della serie E-Class SRA/SMA 1000 e sui firewall di nuova generazione. Consultare le note sulla versione del prodotto per la versione del software specifica richiesta per supportare questa caratteristica.*

Informazioni su SonicWall

Da oltre 25 anni SonicWall combatte il crimine informatico, proteggendo piccole, medie e grandi imprese in ogni parte del mondo. La nostra combinazione di prodotti e partner ha permesso di realizzare una soluzione di difesa informatica in tempo reale ottimizzata per le specifiche esigenze di oltre 500.000 aziende internazionali in più di 150 paesi, per consentire loro di fare più affari con maggior sicurezza.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Per maggiori informazioni consultare il nostro sito web.
www.sonicwall.com

Datasheet-MobileConnectSMA200_400-US-KJ-MKTG3044