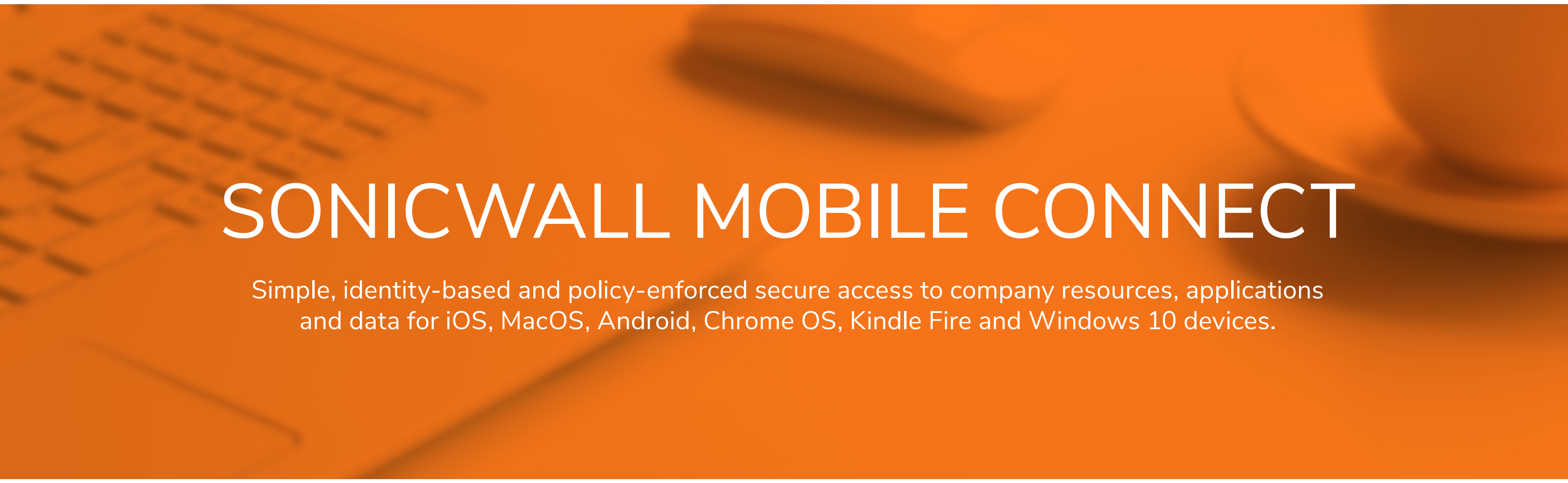
SONICWALL



SONICWALL MOBILE CONNECT

Simple, identity-based and policy-enforced secure access to company resources, applications and data for iOS, MacOS, Android, Chrome OS, Kindle Fire and Windows 10 devices.

Give your employees safe, easy access to the data and resources they need to be productive from any device, running iOS, OS X, Android™, Chrome OS, Kindle Fire and Windows. At the same time, ensure that the corporate network is protected from mobile security threats.

The SonicWall Mobile Connect™ application works in combination with SonicWall Secure Mobile Access (SMA) or next-generation firewall appliances. Mobile workers simply install and launch the Mobile Connect application on their mobile device to establish a secure connection to an SMA or next-generation firewall appliance. The encrypted SSL VPN connection will protect traffic from being intercepted and keep in-flight data secure. Context-aware authentication ensures only authorized trusted users and devices are granted access.

Behind the scenes, IT can easily provision and manage access policies via SonicWall appliances through a single management interface, including restricting VPN access to a set of trusted mobile apps allowed by the administrator. Plus, the SonicWall solution integrates easily with most back-end authentication systems, including most popular identity providers and multi-factor services authentication, so you can efficiently extend your preferred authentication practices to your mobile remote and work-from-home (WFH) workers.

Features and benefits

Ease of use

iOS, OS X, Windows 10, Android, Chrome OS and Kindle users can easily download and install the Mobile Connect app via the App Store™, Google Play, Chrome Web Store, Amazon App Store, or Windows Store.

Centralized policy management

IT can provision and manage user and device accessing via SonicWall appliances — including control of data, resources and applications hosted on-prem or in the cloud — through a single management interface. Unlike other VPN solutions, the SonicWall solution allows you to quickly set role-based policy for mobile and laptop devices and users with a single rule across all objects; as a result, policy management can take only minutes instead of hours.

Verification of both user and device

A Mobile Connect user is granted access to the corporate network only after establishing user and device identity, location and trust. End Point Control can determine whether an iOS device has been jailbroken or an Android device has been rooted, as well as whether a certificate is present or the OS version is current, and then reject or quarantine the connection as appropriate.

Easy access to appropriate resources

Mobile devices can connect to all allowed network resources, including web-based, client/server, server-based, host-based

Benefits:

- Ease of use
- Centralized policy management
- Verification of both user and device
- Easy access to appropriate resources
- Malware protection
- Mobile device registration and authorization management
- Per-application VPN
- One-click secure intranet file browsing and on-device data protection
- Auto-launch VPN
- Easy integration
- Application intelligence and control

Provide fast, secure mobile access through an intuitive, easy-to-use app that is simple to install and launch on both smartphones and tablets.

Specifications compatibility

SonicWall SMA and Next-Generation Firewall
TZ, NSA, E-Class NSA or Super Massive 9000 Series appliances running Sonic OS 5.9 or higher
SMA 100 Series/SRA appliances running 8.5 or higher
SMA 1000 Series/E-Class SRA appliances running 11.4 or higher
SonicWall Mobile Connect
Devices running iOS version 7.0 or higher
Devices running OS X 10.9 or higher
Devices running Android 4.1 or higher
Kindle Fire devices based on Android 4.1 or higher
Devices running ChromeOS 45 or higher
Devices running Windows 10

Partner Enabled Services

Need help to plan, deploy or optimize your SonicWall solution? SonicWall Advanced Services Partners are trained to provide you with world class professional services. Learn more at www.sonicwall.com/PES.

and back-connect applications. Once a user and device are verified, Mobile Connect offers pre-configured bookmarks for one-click access to corporate applications and resources for which the user and device has privileges.

Malware protection

When deployed with a SonicWall next-generation firewall, Mobile Connect establishes a Clean VPN™, an extra layer of protection that decrypts and scans all SSL VPN traffic for malware before it enters the network. All files uploaded by trusted user to corporate networks are inspected by our cloud based multi-engine Capture ATP service to protect from advanced threats such as ransomware and zero-day threats.

Mobile device registration and authorization policy management

With Mobile Connect and seamless integration with SMA solutions, if a mobile device has not previously registered with the SMA appliance, the user is presented with a device authorization policy for acceptance. The user must accept the terms of the policy to register the device and passed all device trust and integrity checks before given permissible access to allowed corporate resources and data. The terms of the policy are customizable by the administrator.

Per-application VPN

Mobile Connect in combination with SMA, enables administrators to establish and enforce policies to designate which apps on a mobile device can be granted VPN access to the network. This ensures that only authorized mobile business apps utilize VPN access. Mobile Connect is the only solution that requires no modification of mobile apps for per app VPN access. Any mobile app or secure container can be supported with no modifications, app wrapping or SDK development.

One-click Secure Intranet File Browse and On-Device Data Protection

Protect company data at rest on mobile devices. Authenticated users can securely browse and view allowed intranet file shares and files from within the Mobile Connect app. Administrators can establish and enforce mobile application management policy for the Mobile Connect app to control whether files viewed can be opened in other apps, copied to the clipboard, printed or cached securely within the Mobile Connect app. For iOS devices, this allows administrators to isolate business data from personal data stored on the device and reduces the risk of data loss. In addition, if the user's credentials are revoked, content stored in the Mobile Connect app is locked and can no longer be accessed or viewed.

Auto-launch VPN

URL control allows apps that require a VPN connection for business (including Safari) to create a VPN profile and automatically initiate or disconnect Mobile Connect on launch (requires compatible server firmware). In addition, for iOS or OS X devices, to simplify use when a secure connection is required, VPN on Demand automatically initiates a secure SSL VPN session when a user requests internal data, applications, websites or hosts.

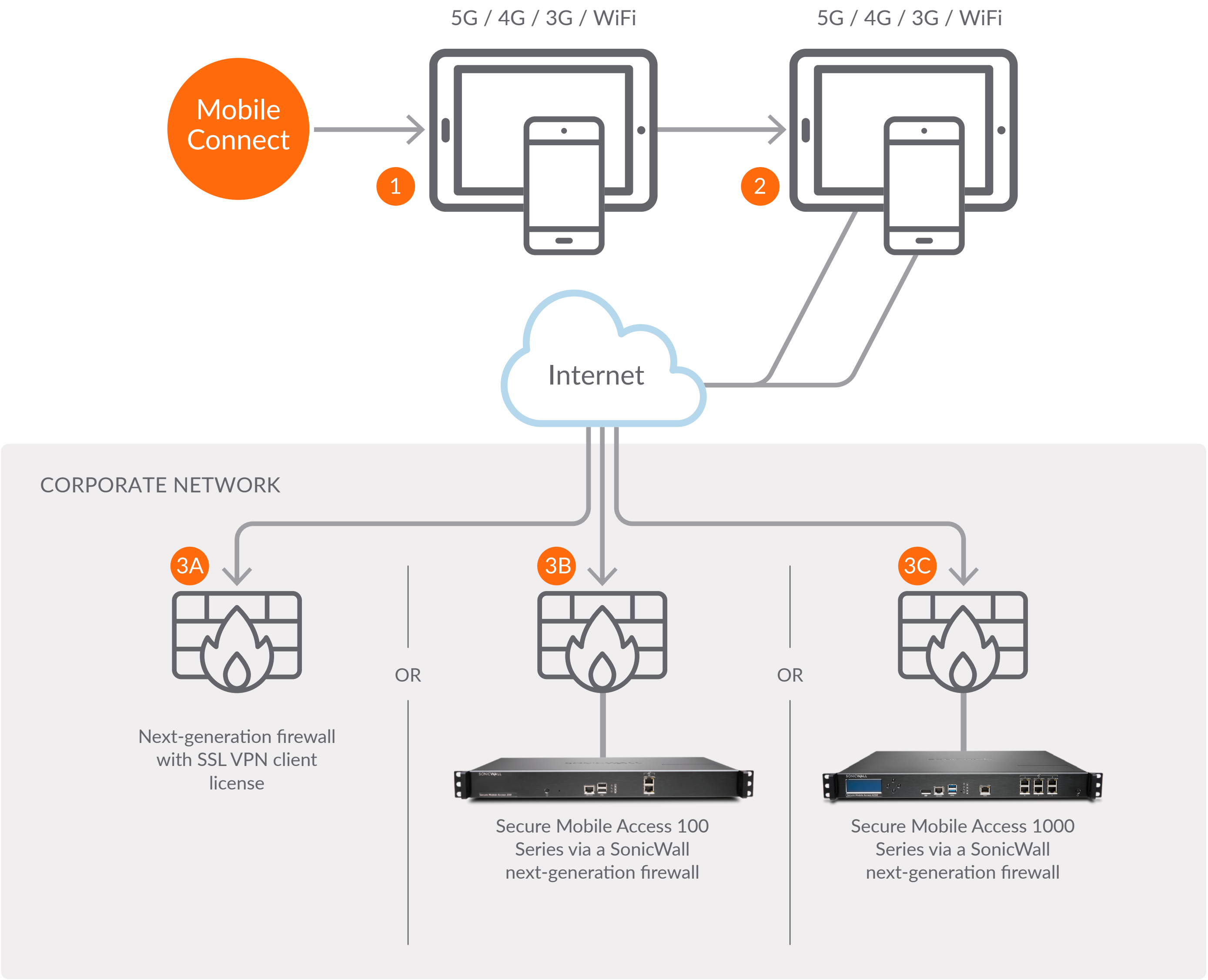
Integration with existing authentication solutions

The SonicWall solution supports easy integration with most back-end authentication systems, such as LDAP, Active Directory and Radius, so you can efficiently extend your preferred authentication practices to your mobile workers. For optimal security, you can apply your choice of identity-based authentication using Ping Identity, okta or onelogin in conjunction with SAML single sign-on (SSO) service with enforced two-factor authentication (2FA) technologies.

Application intelligence and control

When deployed with a next-generation firewall, IT can easily define and enforce how application and bandwidth assets are used.

Software Access


5G / 4G / 3G / WiFi
5G / 4G / 3G / WiFi
Mobile Connect
1
2
Internet
CORPORATE NETWORK
3A
3B
3C
OR
OR
Next-generation firewall with SSL VPN client license
Secure Mobile Access 100 Series via a SonicWall next-generation firewall
Secure Mobile Access 1000 Series via a SonicWall next-generation firewall

1 Download and install SonicWall Mobile Connect onto mobile device.

2 Create a connection profile to connect to your corporate network.

3A Connect to a SonicWall next-generation firewall.

Benefits: Provides DPI scanning for malware as well as application intelligence and control.

3B Connect to a SonicWall Secure Mobile Access 100 Series appliance via a SonicWall next-generation firewall.

Benefits: Provides zero-trust, least privilege access policies, DPI scanning for malware plus end point control to quarantine or reject connections from unregistered, vulnerable, unprotected, and jailbroken or rooted mobile devices.

3C Connect to a SonicWall Secure Mobile Access 1000 Series appliance via a SonicWall next-generation firewall.

Benefits: Provides zero-trust, least privilege access policies, DPI scanning for malware, end point control to quarantine or reject connections from unregistered, vulnerable, unprotected, jailbroken or rooted mobile devices. Also, enables administrators to restrict VPN access to an allowed set of trusted mobile apps, and manage enforced BYOD security policy terms.

Features	iOS	OS X/ Mac	Android	Kindle Fire	Windows 10	Chrome OS
Layer-3 VPN connectivity (SSL VPN)	Yes	Yes	Yes	Yes	Yes	Yes
App distribution	App Store	Mac App Store	Google Play	Amazon App Store	Windows Store	Chrome Web Store
Connect on demand	Yes[3]	Yes[3]	—	—	MDM/ PowerShell	Yes
Configurable trusted networks	Yes[1]	Yes[1]	—	—	Yes	—
Network awareness	Yes[1]	Yes[1]	Yes[1]	Yes[1]	—	—
Credential caching	Yes	Yes	Yes	Yes	Yes	Yes
Touch ID/Fingerprint support	Yes[2]	—	Yes[2]	—	—	—
Face ID support	Yes	—	—	—	—	—
URL control	Yes	Yes	Yes	Yes	—	—
Basic authentication (Username\Password)	Yes	Yes	Yes	Yes	Yes	Yes
Two-Factor Authentication (Dell Defender\TOTP\RADIUS)	Yes	Yes	Yes	Yes	Yes	Yes
Client certificate authentication	Yes[3]	Yes[3]	Yes[3]	Yes[3]	Yes	—
Password change	Yes	Yes	Yes	Yes	Yes	Yes
Always On VPN	Yes	Yes	Yes	Yes	Yes	Yes
SAML 2.0 SSO Support	Yes	Yes	Yes	Yes	Yes	Yes
IdP integration	Ping Identity, okta, onelogin	Ping Identity, okta, onelogin	Ping Identity, okta, onelogin	Ping Identity, okta, onelogin	Ping Identity, okta, onelogin	Ping Identity, okta, onelogin
TLS 1.3 connection	Yes	Yes	Yes	Yes	Yes	Yes
Time-based OTP	Yes	Yes	Yes	Yes	Yes	Yes
SMS Gateway	Yes	Yes	Yes	Yes	Yes	Yes
Windows domain SSO for VPN	—	—	—	—	Yes	—
Split-tunnel\Tunnel-all routing	Yes	Yes	Yes	Yes	Yes	Yes
IPv6 support	Yes[4]	Yes[4]	Yes[4]	Yes[4]	Yes[4]	—
Compression of data over VPN	Yes[3]	Yes[3]	Yes[3]	Yes[3]	Yes[1]	Yes[3]
ESP Mode (UDP transport)	Yes[1]	Yes[1]	Yes[1]	Yes[1]	—	—
Network conflict resolution	Yes[1]	Yes[1]	Yes[1]	Yes[1]	Yes[1]	Yes[1]
End Point Control	Jailbreak, Certificate, OS version, DeviceID[3]	DeviceID, OS version, Client certificate, Anti-Virus software[1]	Root, Certificate, OS version, DeviceID, Anti-Virus software[3]	Root, Certificate, OS version, DeviceID, Anti-Virus software	DeviceID, OS version[1]	DeviceID, Chrome OS version[1]
File Reader/ Bookmarks	Yes[2]	—	Yes[2]	Yes[2]	—	—
RDP bookmarks	2X RDP, Microsoft Remote Desktop for RDP	—	2X RDP, Remote RDP Lite/ Enterprise, Microsoft Remote Desktop for RDP	2X RDP, Microsoft Remote Desktop for RDP	—	—
Citrix receiver bookmarks	Yes[2]	—	Yes[2]	Yes[2]	—	—
VNC bookmarks	Remoter VNC	—	android-vnc-viewer	—	—	—
Web bookmarks	Safari, Chrome	—	Any browser—configured in Android system settings	Silk Browser	—	—
Terminal bookmarks	iSSH, Server Auditor for SSH	—	ConnectBot, JuideSSH	JuideSSH	—	—
Native HTML5 Bookmarks	RDP, VNC, SSH, Telnet[2]	—	RDP, VNC, SSH, Telnet[2]	—	—	—
MDM management of VPN connection profiles	Yes	—	—	—	Yes	Google Mgmt Console

[1] *This feature is supported on the E-Class SRA/SMA 1000 series appliances only. Please refer to the product release notes for the specific software version required to support this feature.*

[2] *This feature is supported on the SRA/SMA 100 series appliances only.*

[3] *This feature is supported on the SRA/SMA 100 series and E-Class SRA/SMA 1000 series appliances only. Please refer to the product release notes for the specific software version required to support this feature.*

[4] *This feature is supported on the SRA/SMA 100 series, E-Class SRA/SMA 1000 series and Next-Generation Firewall appliances. Please refer to the product release notes for the software specific version required to support this feature.*

About SonicWall

SonicWall has been fighting the cybercriminal industry for over 27 years defending small and medium businesses, enterprises and government agencies worldwide. Backed by research from SonicWall Capture Labs, our award- winning, real-time breach detection and prevention solutions secure more than a million networks, and their emails, applications and data, in over 215 countries and territories. These organizations run more effectively and fear less about security. For more information, visit www.sonicwall.com or follow us on Twitter, LinkedIn, Facebook and Instagram.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Refer to our website for additional information.
www.sonicwall.com