SonicWALL Mobile Connect™ for Google Android

SECURE REMOTE ACCESS

Superior network-level access for Google® Android™ device users

- **Unified client app**
- **Data encryption**
- **End Point Control™**
- **SonicWALL Clean VPN™**
- **Application intelligence and control**
- **Unified policy-based controls**
- **Full network access**
- **Personalized web portal**

Smartphones and tablets that run Google® Android™ have emerged as a powerful and secure mobile computing platform for corporate, academic and government organizations. When used outside of the network perimeter to connect to external networks (including wireless hot spots, 3G/4G, etc.), these mobile devices must support VPN connectivity to ensure data privacy and security. When used inside corporate networks, mobile devices should be able to take advantage of all the protection and security offered by leading-edge Next-Generation Firewalls. Until now, no solution has addressed all these needs.

The SonicWALL® Mobile Connect™ unified client app for Android provides Android smartphone and tablet users with superior network-level access to corporate, academic and government resources over encrypted SSL VPN connections. SonicWALL is the only vendor to provide solutions for full malware scanning of the SSL encrypted traffic, and application control for Android devices.

Deployed with a SonicWALL Next-Generation Firewall solution (featuring Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service), Mobile Connect establishes a Clean VPN™ that decrypts and removes threats from Android device traffic tunneled over SSL VPN before they enter the network. Additionally, SonicWALL Application Intelligence and Control allows organizations to define and enforce how application and bandwidth assets are used.

SonicWALL Aventail® E-Class Secure Remote Access (SRA) solutions feature End Point Control™ (EPC). EPC allows administrators to define policies that identify specific attributes about the device, and ensure they are enforced before allowing access to the corporate network. As part of EPC enforcement via Mobile Connect, a policy can be set up to determine if an Android device has been rooted, so that connections from that device can be rejected or quarantined.

As smartphones and tablets are used inside the corporate network and connect over WiFi, traffic is scanned by a SonicWALL Next-Generation Firewall. This creates a Clean Wireless solution connection that ensures Android devices adhere to organizational security, app control and content filtering policies. SonicWALL offers the most comprehensive end-to-end secure remote access solution available today.

Features and Benefits

A **unified client app** available on the Android Market, Mobile Connect lets IT define and enable easy Android device access via SonicWALL SSL VPN and Next-Generation Firewall appliances through a single management interface.

Data encryption, enforced strong encryption, strong authentication and granular access policy provide security of transport.

End Point Control™, available only on the SonicWALL Aventail E-Class SRA Series, identifies specific attributes and enforces they are in place before allowing an Android system running Mobile Connect to connect to the network. These attributes include DeviceID, File, Process, Android OS version, and whether the Android device has been rooted.

SonicWALL Clean VPN™ provides the critical dual protection of high-performance Next-Generation Firewall and SSL VPN to secure VPN access and traffic, and decrypt and scan for malware on all authorized SSL VPN traffic before it enters the network.

Application intelligence and control enables IT to define and enforce how application and bandwidth assets are used.

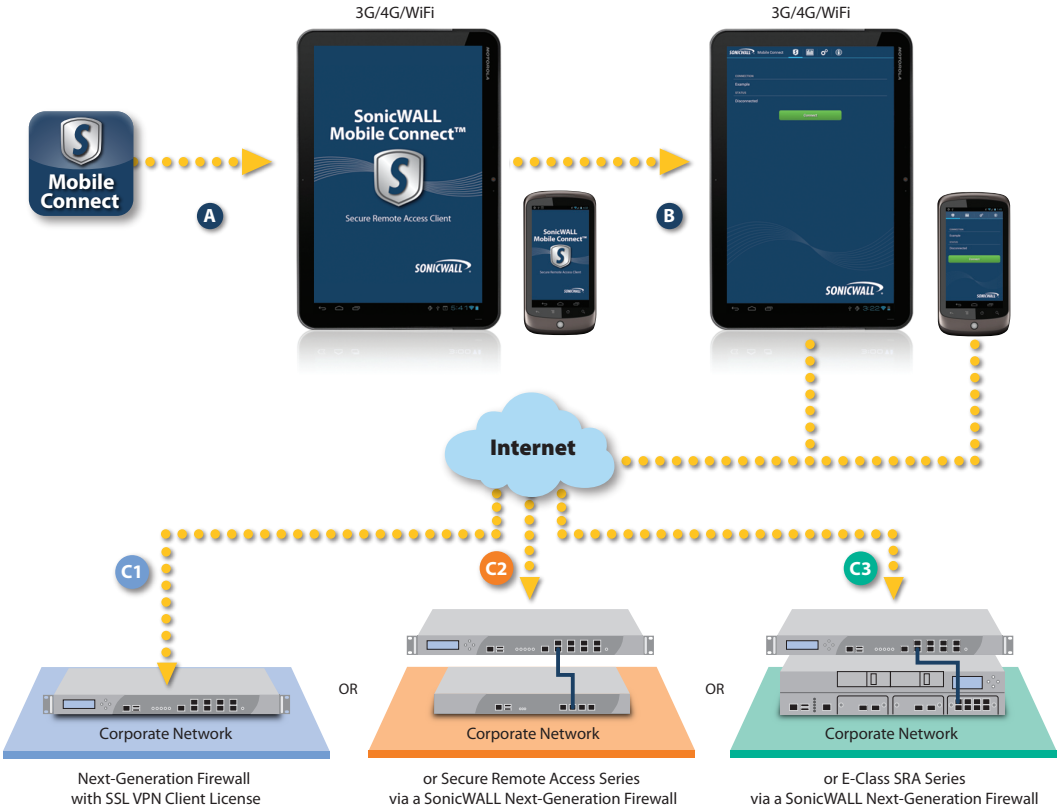
Unified policy-based controls display granular bookmarks and policies on one centralized page, thus streamlining configuration, troubleshooting and administrative overhead.

Full network access connects all Android devices to network resources, including web-based, client/server, server-based, host-based or back-connect applications.

Personalized web portal displays only the resources that are available to Google Android smartphone and tablet users based on policy.

SONICWALL®

DYNAMIC SECURITY FOR THE GLOBAL NETWORK™



A Download and install SonicWALL Mobile Connect from the Android Market on your Android-based smartphone or tablet. (Requires Android 4.0 or higher)

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

C1 Connect to a SonicWALL Next-Generation Firewall.
Benefits: Provides DPI scanning for malware as well as application intelligence and control.

C2 Connect to a SonicWALL SRA appliance via a SonicWALL Next-Generation Firewall.
Benefits: Provides DPI scanning for malware.

C3 Connect to a SonicWALL Aventail E-Class SRA via a SonicWALL Next-Generation Firewall.
Benefits: Provides DPI scanning for malware. End Point Control provides an option to quarantine or reject connections from rooted Android devices.

Specifications

SonicWALL SRA and Next-Generation Firewall Specifications

Compatibility
- C1 TZ, NSA or E-Class NSA appliance running SonicOS 5.8.1.0 or higher
- C2 SRA appliances running 5.5 or higher
- C3 E-Class SRA appliances running Aventail 10.5.4 or higher

SonicWALL Mobile Connect Specifications

Compatibility: Devices running Android 4.0 and higher

Software Access

Available for download from the Android Market

Available in Android Market

SonicWALL, Inc.
2001 Logic Drive, San Jose, CA 95124
T +1 408.745.9600 F +1 408.745.9300
www.sonicwall.com

SonicWALL's line-up of dynamic security solutions

NETWORK SECURITY | SECURE REMOTE ACCESS | WEB AND E-MAIL SECURITY | BACKUP AND RECOVERY | POLICY AND MANAGEMENT

SONICWALL®
DYNAMIC SECURITY FOR THE GLOBAL NETWORK™