Mobility, Security and the Enterprise: 10 Best Practices for Controlling Smartphone and Tablet Access to Corporate Networks
## Table of Contents

The Consumerization of IT .......................... 1  
A Moving Target ...................................... 2  
Risk/Reward: A Complex Equation ................. 3  
Smartphones are Outside of IT Control ............. 4  
Data Leakage and Loss ................................ 5  
Malware Threats ...................................... 6  
Bandwidth Overconsumption ......................... 7  
Making Smarter Mobile Access Decisions .......... 8  
Establishing a Best-practice Defense ............... 9  
Best Practice #1: Establish SSL VPN Access to Corporate Resources 10  
Best Practice #2: Establish Reverse Web Proxy ........ 11  
Best Practice #3: Require a Lost or Stolen Phone or Tablet be Reported Immediately 12  
Best Practice #4: Comprehensively Scan All Mobile Device Traffic 13  
Best Practice #5: Control Data-in-flight .......... 14  
Best Practice #6: Maximize Firewall Throughput to Eliminate Latency 15  
Best Practice #7: Establish Controls Over Mobile Device Application Traffic 16  
Best Practice #8: Establish Mobile Device Wireless Access Security 17  
Best Practice #9: Manage Mobile Device Traffic Bandwidth 18  
Best Practice #10: Visualize Bandwidth Activity 19  
Deploy SonicWALL Solutions for Smartphone and Tablet Security 20  
SonicWALL Mobility Solution ....................... 21  
Conclusions ........................................... 22
Many technologies that enterprises adopt for their information systems often have roots in consumer applications. More employees are extending their workday and increasing office efficiency by leveraging the same technology they use to enhance their personal lives—in particular, smartphone and tablet devices.

Many corporate end users do not allow IT to dictate which smartphone or tablet platform they can use. A growing number will use whatever application, device or technology they want, regardless of corporate IT policies. IT has effectively lost its ability to completely mandate the choice of smartphone or tablet access in a corporate setting.

The power of users now rules the day.
Face the facts: there will be many rapid changes in smartphone/tablet platforms beyond the control of corporate IT. Administrators must deal with multiple operating system platforms, including iOS, Google® Android, Nokia® Symbian and Microsoft® Windows Mobile and Windows Phone 7.

**Juggling support for multiple smartphone platforms can burden IT.**

IT administrators must have an agnostic approach to support multiple smartphone/tablet platforms for its users, as well as provide contingencies for access continuity. For example, BlackBerry users in certain countries faced threatened service outages that could have required them to switch to a different platform.
Risk/Reward: A Complex Equation

Perhaps the biggest threat is from users themselves, who are increasingly utilizing their mobile devices with scant regard for IT policies (e.g., playing games or checking personal Gmail while connected to corporate networks). Increasingly, mobile device usage is placing great pressure on corporate network resources, too, especially when users consume high-bandwidth content such as video.

According to a study by IDC, people downloaded 10.9 billion mobile apps in 2010 (a figure IDC expects will increase to nearly 76.9 billion by 2014), many a potential threat to corporate security.

The combination of these factors presents IT departments with a serious dilemma. On one hand, smartphones and tablets are simply too powerful and useful for businesses to ignore, empowering users in completely new ways and enabling them to work far more flexibly and productively. Security must be seen to be enabling the business, rather than holding it back from the rewards many of these new devices offer.
Smartphones are Outside of IT Control

Smartphones operate in two worlds: they can connect to the corporate network over wireless, or bypass the network entirely using mobile cellular connections. That means they might download malware from the web over 3G/4G, and then disseminate it over the corporate WiFi network.

Transferring data in and out of the corporate network, smartphones and tablets are beyond IT control

It is harder for IT to control what users do with their smartphone devices, and how these devices expose business data to security threats. Even if IT-issued, any endpoint device that can bypass security measures is insecure.
Data Leakage and Loss

Smartphones and tablets may also retain sensitive or proprietary data while connected to the corporate wireless network, and then leak it over unsecured cellular to the web—and IT has no recourse. Whether unintentionally, maliciously or driven by profit, employees are leaking a growing amount of data over smartphones/tablets.

*Users more frequently lose smartphones than computers.*

Smartphone content is more vulnerable to loss or theft, as network access codes, usernames and passwords are often unsecured or set for automatic log-on. Consumers who “jailbreak” phones to customize carriers or features often leave themselves open to root password hacks.
As their numbers increase, smartphones and tablets become a more lucrative target for criminal attacks. The same threats that plague traditional computer operating systems can affect smartphones and tablets, disseminated in emails, social media sites, games, screen savers, instant messages, slide shows, or in some cases by shady URL-shortening services that make bogus, redirecting links more difficult to identify.

**Smartphones and tablets can magnify malware distribution by spam, phishing, pharming and pretexting.**

Because smartphones and tablets are a more intimate communications channel than a computer, users are more likely to interact with files masquerading as personal communications. Likewise, users cannot as easily detect cues that a website is a false front on a handset with a small screen. Again, the infection may not be apparent even after perpetration, and can propagate via smartphone across corporate IP networks.
Bandwidth Overconsumption

The sheer volume of interactive Web 2.0 and streaming media traffic over smartphones and tablets can affect corporate wireless network throughput. Some of these applications, such as streaming video, constantly evolve to avoid control. In addition, like any web-facing endpoint device running applications over the network, smartphones present a potential channel for forced denial-of-service attacks.
Choosing and/or encouraging a mobile device platform that is safe, easy to configure and manage, and that is flexible enough to meet the needs of employees and senior executives sounds easy on paper. In practice, however, it is one of the biggest challenges ahead for IT managers.

To be certain that devices are safe, IT departments must design security policies that are invariably a complex blend of technology and policy.

Most analysts agree that enterprises should be able to enforce several basic security features on any mobile device, including mandatory passwords, over-the-air device wiping capabilities and data encryption.

In practice, the choice of the platform itself will determine the effectiveness of the overall policy.
Establishing a Best-practice Defense

The consumerization of IT as well as best practices demand that IT enforce sound smartphone and tablet policy with proven technology. IT should define, document and communicate smartphone and tablet use policy, and combine that policy with the deployment of corresponding enforcement solutions. Examples of documented IT policies include requiring users to set strong passwords on their smartphones and tablets (valuable in cases of a lost device, etc.) and report lost or stolen mobile devices to IT immediately. Examples of enforcement solutions include security technologies that can recognize when solicited connections are originating from mobile devices and provide differentiated access policies based on type of device and user authentication. The following critical best practices include approaches for both policy and technology.
Agent-based Secure Sockets Layer Virtual Private Networking (SSL VPN) tunnels add easy “in-office” network-level access to critical client-server resources from laptops, smartphones and tablets, thereby minimizing demand on IT support. Administrators should select SSL VPN gateway solutions that have certified smartphone/tablet clients from the same vendors. This provides a single point of management and similar user experience for both laptops and smartphones, rather than trying to cobble together and support one solution for laptops and a different solution for smartphones and tablets.

Best Practice #1: Establish SSL VPN Access to Corporate Resources
By providing standard web browser access to web resources, reverse proxies can authenticate and encrypt web-based access to network resources. Reverse proxy adds the benefit of delivering access agnostically to laptop, smartphone and tablet platforms, thus making it easier to deploy and manage mobility solutions and minimizing administrative overhead. Both SSL VPN and reverse web proxy should integrate seamlessly with standard authentication methods such as two-factor authentication or one-time passwords.
Best Practice #3:
**Require a Lost or Stolen Phone or Tablet be Reported Immediately**

Smartphones and tablets can get lost, stolen or compromised. Device identification technology uses serial number information to allow organizations to chain a specific mobile device to a specific user. This effectively provides a watermark for the device, thus enabling IT to block access to corporate resources. Also, smartphone and tablet OS vendors typically offer a “remote wipe” feature for when the devices are lost or stolen.
Best Practice #4: Comprehensively Scan All Mobile Device Traffic

Smartphones and tablets can act as conduits to enable malware to cross the network perimeter, even over WiFi or 3G/4G connections. Integrated deployment with a Next-Generation Firewall (NGFW) establishes a Clean VPN™ that decrypts then scans all the content. NGFW gateway security measures (Anti-Virus/Anti-Spyware, Intrusion Prevention Service) decontaminate threats before they enter the network.
Best Practice #5: Control Data-in-flight

Data leakage protection can scan outbound traffic for watermarked content, even if that traffic is encrypted. At the same time, IT should scan all data-in-flight for malware, and prevent internally launched outbound botnet attacks that can damage corporate reputation and get business-critical email servers blacklisted. Full-featured Next-Generation Firewalls can provide those protections.
Best Practice #6: Maximize Firewall Throughput to Eliminate Latency

When smartphones and tablets are connected to the corporate network, in order to minimize impact upon latency-sensitive applications such as video conferencing and voice over IP (VoIP), the Next-Generation Firewall platform must be able to comprehensively optimize business-relevant mobile device traffic in real time. IT can obtain such performance capability in solutions that integrate deep packet inspection methods with a high-speed multi-core processor architecture.
As primarily a web-enabled device, smartphones and tablets can access applications such as social media and streaming video. IT should establish control over these applications, just like with other devices when connected directly to the corporate network. Application intelligence and control technology can extend firewall functionality to identify, categorize, control and report upon application usage over the corporate network from these devices.
Analysts expect ninety percent of smartphones to have WiFi functionality by 2014. Security for wireless networks has to be at least on par with wired networks running deep packet inspection. IT should apply both WPA2 and deep packet inspection to traffic connected to the corporate network over WiFi. To be as secure as wired networks, WLANs also need other security features such as deep packet inspection, to scrub traffic using an array of intrusion prevention, anti-virus and anti-spyware technology.
Organizations need to control converged voice-and-data communications enabled by smartphones directly connected to the corporate network. At the same time, they need to optimize quality of service and bandwidth management, as well as prioritize traffic on a per-application and per-user basis. Application-intelligent bandwidth management can dedicate both throughput to latency-sensitive smartphone and tablet applications (e.g., VoIP), as well as limit bandwidth-consuming traffic.
Best Practice #10: Visualize Bandwidth Activity

To control the proper use of mobile networks, administrators need tools to provide them with the ability to view traffic and adjust network policy based on critical observations. This enables administrators to ensure bandwidth for mobile device traffic, while adjusting policy to restrict or block bandwidth-consuming traffic based upon a real-time view of bandwidth utilization, application and user traffic, and other user activity.
Deploy SonicWALL Solutions for Smartphone and Tablet Security

SonicWALL® Aventail® E-Class Secure Remote Access (SRA) delivers full-featured, easy-to-manage, clientless or thin-client “in-office” connectivity for up to 20,000 concurrent mobile-enterprise users from a single appliance. E-Class SRA enhances productivity and business continuity with policy-enforced remote access to network resources from Windows®, Windows Mobile, Apple® Mac OS®, iOS, Linux®, and Google Android® devices. Built on the powerful SonicWALL Aventail SSL VPN platform, E-Class SRA connects only authorized users to only authorized resources. When combined with SonicWALL Next-Generation Firewall as a Clean VPN™, that decrypts and removes threats from traffic tunneled over SSL VPN before they enter the network.
SonicWALL Mobility Solution

SonicWALL is the only provider that solves the challenges of access, security and control with one integrated SonicWALL Clean VPN™ solution that combines Clean VPN and application intelligence and control. When SonicWALL Secure Remote Access solutions are deployed with a SonicWALL Next-Generation Firewall, SonicWALL Clean VPN scans tunneled traffic to block malware from exploiting mobile devices as a conduit into the network. SonicWALL Application Intelligence and Control can allow increased bandwidth for critical iOS and Android applications, while limiting bandwidth for unimportant or unacceptable traffic.

- **SonicWALL Clean VPN™** delivers the critical dual protection of SSL VPN and high-performance Next-Generation Firewall necessary to secure both VPN access and traffic. The multi-layered protection of Clean VPN enables organizations to decrypt and scan for malware on all authorized SSL VPN traffic before it enters the network environment.

- **SonicWALL Clean Wireless** delivers secure, simple and cost-effective distributed wireless networking by integrating universal 802.11a/b/g/n wireless features with an enterprise-class firewall/VPN gateway.

- **SonicWALL Application Intelligence and Control** can maintain granular control over applications, prioritize or throttle bandwidth, and manage website access. Its comprehensive policy capabilities include restricting transfer of specific files and documents, blocking email attachments using user-configurable criteria, customizing application control, and denying internal and external web access based on various user-configurable options.
Conclusions

Personal smartphone and tablet use in corporate environments has reached its tipping point. More than ever end users are increasingly demanding access to network resources from their personal consumer mobile devices. While riding this tide does offer potential business benefits, it comes with inherent risks.

*Personal smartphones and tablets pose a risk—*  
*SonicWALL has the solution*

SonicWALL solutions, including Secure Remote Access, Next-Generation Firewall, Clean VPN, and Application Intelligence and Control, can help organizations easily implement best practices to secure smartphone and tablet use in corporate network environments.
How Can I Learn More?

- Download the whitepaper “Controlling Laptop and Smartphone Access to Corporate Networks”
- Opt-in to receive SonicWALL Newsletters

For feedback on this e-book or other SonicWALL e-books or whitepapers, please send an e-mail to feedback@sonicwall.com.

About SonicWALL

Guided by its vision of Dynamic Security for the Global Network, SonicWALL® develops advanced intelligent network security and data protection solutions that adapt as organizations evolve and as threats evolve. Trusted by small and large enterprises worldwide, SonicWALL solutions are designed to detect and control applications and protect networks from intrusions and malware attacks through award-winning hardware, software and virtual appliance-based solutions. For more information, visit the company web site at www.sonicwall.com.

1 “Gartner Says Consumerization Will Be Most Significant Trend Affecting IT During Next 10 Years,” Gartner Inc., October 20, 2005
2 “Millennial Workforce: IT Risk or Benefit?,” Symantec, March 2008
5 Gartner: Mobile To Outpace Desktop Web By 2013,” Media Post Communications, January 13, 2010
6 “Worldwide Smartphone Sales Forecast to 2015,” Coda Research Consultancy, May 2010
7 “Survey: Wi-Fi becoming smartphone must-have,” CNET News, April 1, 2009

© 2012 SonicWALL, Inc. All rights reserved. SonicWALL® is a registered trademark of SonicWALL, Inc. and all other SonicWALL product and service names and slogans are trademarks or registered trademarks of SonicWALL, Inc. Other product and company names mentioned herein may be trademarks and/or registered trademarks of their respective owners. 01/12 SW 1442