Controlling Laptop and Smartphone Access to Corporate Networks

Understanding the similarities and differences of securing mobile laptops and smartphones

SONICWALL®

DYNAMIC SECURITY FOR THE GLOBAL NETWORK™

Table of Contents

SONICWALL®
DYNAMIC SECURITY FOR THE GLOBAL NETWORK™

The Consumerization of IT

With company-issued, IT-controlled laptops, IT has traditionally had the option to lock down the operating system to prevent the installation of potentially insecure or non-approved applications.

Today, employees demand the same freedom-of-technology at work as they have in their personal lives.[1]

This consumerization of IT[2] (as well as the budgetary incentive of offsetting inventory costs) has led companies to establish "bring your own device" (BYOD) policies that enable employees to select their own personal mobile devices for use at work.

Issues Pertaining Specifically to Laptops

For laptops using applications running on standard Windows®, Macintosh® and Linux® operating systems, consumerization and BYOD has resulted in an open, uncontrolled "wild west" application environment. In effect, end users can install any applications they like, even those that are potentially insecure or dangerous and not sanctioned for corporate use, without any additional layer of security screening or review.

Because of their open application environment, laptops require device interrogation.

Device interrogation for Windows, Mac and Linux enables IT to see if the proper security applications are running on the device, and enforce security policy to allow, quarantine or deny access to the device based on the defined security policy of the company. For these unmanaged laptops, security demands using reverse-proxy portal access or a virtual private network (VPN) tunnel with endpoint control.

Issues Pertaining Specifically to Smartphones

In contrast, apps designed to run on smartphone (as well as tablet) operating systems typically undergo stringent review and are white-listed before becoming available for download. (This does not apply, of course, to smartphones that have been jailbroken).

Because of this distinction, device interrogation is more critical for a laptop than for a smartphone.

For example, iOS users have rarely downloaded a rogue app from the App Store℠. Google Android®, while somewhat less stringent (and overcoming some rogue application issues early on), has been largely successful in maintaining a closed, white-listed app environment.

Administrative Distinctions between Laptops and Smartphones

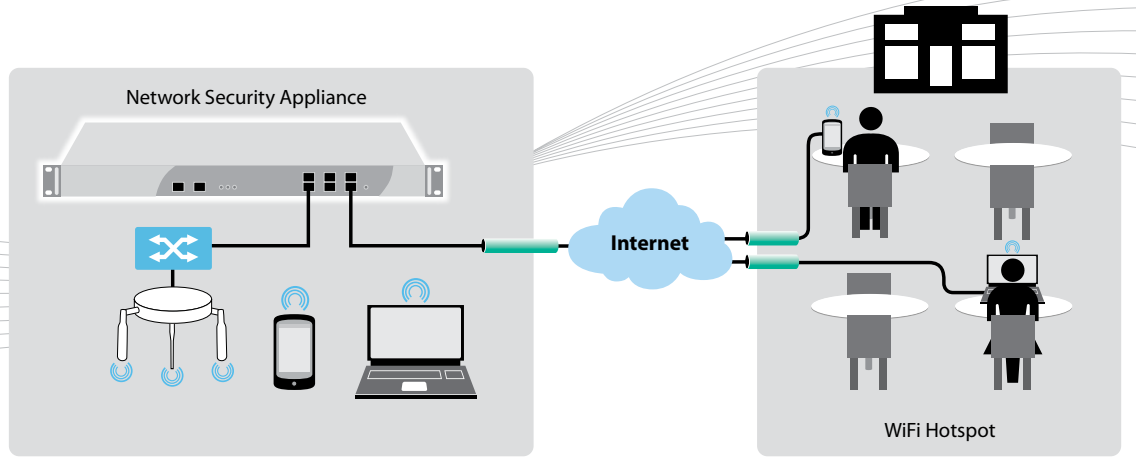
Administrators deploying laptops can select from a wide variety of IPSec and SSL VPN clients. IT administrators will often select a secure gateway and utilize that vendor's secure client for connectivity. However, most secure clients are not supported by smartphone operating systems like iOS. Only a select group of security vendors have been provided low-level access to iOS.

Laptops and smartphones differ in ease-of-use, deployment and administration, as well as unified clients and security policy.

Security vendors who are not trusted by the smartphone are often forced to "tap" into various third-party clients to try to achieve a makeshift solution. As problems arise, administrators are forced to decipher the vendor "blame game" to determine where problems really exist. Administrators can more easily deploy and maintain gateway solutions from vendors that also have approved VPN access with the smartphone operating systems.

A Comprehensive Approach to Best Practices

Both laptops and smartphones may connect to the network remotely over WiFi, and so are subject to man-in-the-middle attacks. As a result, both laptops and smartphones require encrypted access through a VPN to ensure the confidentiality of communications outside the network. Companies that rely strictly on Remote Desktop Protocol (RDP) solutions would be more susceptible to this type of snooping attack because the communication is unencrypted or may only support very weak encryption standards.



Securing mobile access for laptops and smartphones is in many ways similar.

IT must also have the ability to scan all traffic to ensure network integrity and security. Organizations are grappling with the reality that mobile devices are not only conduits of information flow but, unfortunately, also a delivery vehicle for malware into networks, either inadvertently or intentionally. Different security practices apply depending upon whether the mobile devices are connecting from outside or inside the network perimeter.

Best Practices for Both Laptops and Smartphones Connecting from Outside the Perimeter

The following best practices address security issues of both laptops and smartphones that connect to the network from outside the perimeter:

- Establish Reverse Web Proxy
- Establish SSL VPN Tunnels
- Scan VPN Traffic Through a Next-Gen Firewall
- Add Strong Authentication

These practices are detailed further in the following pages.

Best Practice #1: For Both Laptops and Smartphones Connecting from Outside the Perimeter

Establish Reverse Web Proxy

By providing standard browser access to web resources, reverse proxies can authenticate and encrypt web-based access to network resources from outside the perimeter. Reverse proxy delivers access agnostically to both laptop and smartphone platforms, thus minimizing deployment overhead.

Best Practice #2: For Both Laptops and Smartphones Connecting from Outside the Perimeter

Establish SSL VPN Tunnels

Agent-based encrypted SSL VPN tunnels add easy "in-office" network-level access to critical client-server resources for both laptops and smartphones connecting from outside the perimeter. Administrators should select SSL VPN gateway solutions that have certified smartphone 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.

Best Practice #3: For Both Laptops and Smartphones Connecting from Outside the Perimeter

Scan VPN Traffic Through a Next-Gen Firewall

Both laptops and smartphones can act as conduits to enable malware to cross the network perimeter, 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 (e.g., Anti-Virus, Anti-Spyware, Intrusion Prevention Service) can decontaminate threats before they enter the network.

Best Practice #4: For Both Laptops and Smartphones Connecting from Outside the Perimeter

Add Strong Authentication

A secure solution for laptops, smartphones and tablets should integrate seamlessly with standard authentication methods such as two-factor authentication and integrated one-time passwords.

Best Practices Specifically for Laptops Connecting from Outside the Perimeter

The following best practices address security issues with laptops (because they do not have a white-listed app environment like smartphones) that connect to the network from outside the perimeter:

- Deploy Endpoint Control
- Create a Secure Virtual Desktop
- Enforce Cache Cleaner

These practices are detailed further in the following pages.

Best Practice #5: Specifically for Laptops Connecting from Outside the Perimeter

Deploy Endpoint Control for Laptops

To help determine and enforce acceptable security policy compliance for managed and unmanaged Windows, Macintosh and Linux laptops outside the perimeter, endpoint control can determine the presence of security applications and allow, quarantine or deny access based on security policy and user identity. As addressed above, this is very important for laptops, but less important for smartphones due to their white-listed app distribution environment.

Best Practice #6: Specifically for Laptops Connecting from Outside the Perimeter

Create a Secure Virtual Desktop for Laptops

Secure virtual desktop environments can prevent users from leaving sensitive data behind on unmanaged Windows laptops. They accomplish this by removing all files and links generated during the VPN session upon disconnection.

Best Practice #7: Specifically for Laptops Connecting from Outside the Perimeter

Enforce Cache Cleaner Technology for Laptops

A cache cleaner can remove all browser-based tracking information from a Windows and Mac laptop once the user logs off or closes the browser.

Best Practices for Both Laptops and Smartphones Connecting from Inside the Perimeter

The following best practices address security issues of both laptops and smartphones that connect to the network from inside the perimeter:

- Scan WiFi Traffic through a Next-Gen Firewall
- Control Application Traffic
- Prevent Data Leakage
- Block Inappropriate Web Access
- Block Outbound Botnet Attacks

These practices are detailed further in the following pages.

Best Practice #8: For Both Laptops and Smartphones Connecting from Inside the Perimeter

Scan WiFi Traffic through a Next-Gen Firewall

Integrating NGFW with 802.11a/b/g/n wireless connectivity creates a Clean Wireless™ network when the laptop or smartphone user is inside the perimeter.

Best Practice #9: For Both Laptops and Smartphones Connecting from Inside the Perimeter

Control Application Traffic

In general, mobile device apps are either critical business solutions or personal time-wasters. An Application Intelligence and Control solution can enable IT to define and enforce how application and bandwidth assets are used.

Best Practice #10: For Both Laptops and Smartphones Connecting from Inside the Perimeter

Prevent Data Leakage

Data leakage protection technology applied to laptops and smartphones inside the perimeter can scan inbound and outbound traffic and take policy-driven action to block or allow file transmission based upon watermarked content. It can also forward non-compliant watermarked files to IT, HR or management for further remediation.

Block Inappropriate Web Access

Content filtering for both laptops and smartphones (and even corporate desktops) used inside the perimeter can enforce company browsing policies for mobile users and help them comply with regulatory mandates by ensuring a non-hostile network environment.

Block Outbound Botnet Attacks

Anti-malware scanning can identify and block outbound botnet attacks launched from laptops and smartphones connected from inside the perimeter.

Mobile Device Management

To deal with issues of mobile security even further, some organizations consider implementing Mobile Device Management (MDM) gateways. Among other things, MDM may restrict access based on phone number, identify jailbroken devices, and isolate business data into encrypted MDM-managed virtual desktop containers that IT can remotely wipe based upon policy criteria.

However, taking on an MDM solution typically involves significant investment and additional infrastructure complexity, which can sometimes counter its benefits.

Before taking on the added expense, an organization should consider why it needs MDM. If MDM does not offer distinct benefits for specific use cases, the organization should reallocate budget to uses that are more productive.

SonicWALL Mobility Solutions

To implement these best practices, IT requires solutions with the capability to enforce them.

SonicWALL® Aventail® E-Class Secure Remote Access (SRA) Series, SRA Series for Small- to Medium-Sized Businesses (SMB), and **SonicWALL Next-Generation Firewalls** deliver easy, policy-driven SSL VPN access to critical network resources from an extensive range of mobile device platforms, including Windows, Macintosh and Linux-based laptops, Windows Mobile, iOS, Google Android and Nokia Symbian smartphones.

SonicWALL Aventail Advanced End Point Control™ (EPC™) (available for Windows, Macintosh and Linux-based devices) integrates unmanaged endpoint protection, encrypted virtual **Secure Desktop** and comprehensive cache control. EPC offers advanced endpoint detection and data protection for enterprises by interrogating endpoint devices to confirm the presence of all supported anti-virus, personal firewall and anti-spyware solutions from leading vendors such as McAfee®, Symantec®, Computer Associates®, Sophos®, Kaspersky Lab® and many more.

SonicWALL Mobility Solutions (continued)

The **SonicWALL Mobile Connect™** unified client app for iOS provides Apple iPad, iPhone, and iPod touch users full access to network-level resources over encrypted SSL VPN connections to ensure confidentiality and data integrity for users outside the network perimeter. Deployed on or with a SonicWALL Next-Generation Firewall, it enables Clean VPN to remove malware from communications relayed through iOS devices. SonicWALL Application Intelligence and Control enables IT to define and enforce how application and bandwidth assets are used whether the user is inside or outside the network. Users can download and install the app easily via the App Store, providing secure SSL VPN connections to SonicWALL Aventail E-Class SRA, SRA for SMB or SonicWALL Next-Generation Firewall appliances.

Additionally, **SonicWALL Aventail Connect Mobile™**, in combination with SonicWALL Aventail E-Class SRA appliances, provides a remote access solution for Windows Mobile smartphones and Google Android smartphones and tablets. Both Mobile Connect and Connect Mobile clients provide "in-office" access optimized for the device, combining a seamless network experience for users, along with a single, centrally managed gateway for mobile access control.

SonicWALL Aventail SSL VPN solutions provide **Secure ActiveSync® Support** for access to Microsoft Exchange email, contact and calendar services from iOS, Android, Symbian, Windows Mobile and Windows Phone 7 smartphone and tablet devices. SonicWALL Device Identification lets administrators chain a specific smartphone or tablet to a specific user so, in the event that phone is lost or stolen, they can quickly revoke corporate access.

SonicWALL Mobility Solutions (continued)

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. Clean VPN protects the integrity of VPN access by establishing trust for remote users and their endpoint devices, using enforced authentication, data encryption, and granular access policy. Simultaneously, Clean VPN secures the integrity of VPN traffic by authorizing this traffic, cleaning inbound traffic for malware, and verifying all outbound VPN traffic in real time.

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

The differences between laptops and smartphones affect how IT should approach security, particularly in the areas of device interrogation and VPN client provisioning. Still, corporations, academic institutions and government entities must require both laptops and smartphones to support strong VPN or remote proxy connectivity when used outside of the corporate network to ensure data confidentiality and security while taking advantage of external wireless connectivity, hot spots, etc.

When used inside the corporate network, laptops and smartphones should be able to take advantage of all the protection and security offered from leading-edge Next-Generation Firewall technology

IT must be able to guarantee vital bandwidth to critical applications, while limiting the negative impact of undesired traffic. SonicWALL solutions, including Mobile Connect, SSL VPN, Clean VPN, and Next-Generation Firewalls with application intelligence, control and visualization, can help organizations easily implement best practices to secure laptop and smartphone use in corporate network environments.

SONICWALL®

DYNAMIC SECURITY FOR THE GLOBAL NETWORK™

How Can I Learn More?

- Download the Whitepaper "Controlling Smartphone and Laptop 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 email to **feedback@sonicwall.com.**

Forward to a Friend

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] "The State of Workforce Technology Adoption: US Benchmark 2009," Forrester Research, Inc., November 11, 2009
[2] "Gartner Says Consumerization Will Be Most Significant Trend Affecting IT During Next 10 Years," Gartner Inc., October 20, 2005

SonicWALL's line-up of dynamic security solutions

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