Realtime publishers

Using Cloud Services to Improve Web Security

The Essentials Series

Using Web Security Services to Protect Portable Devices

sponsored by webroot®

Mike Danseglio

Copyright Statement

Using Web Security Services to Protect Portable Devices

Today's workforce is a security challenge. Employees no longer follow strict guidelines from the IT department regarding computer use at work, computer security measures, personal computing devices used for work, and so on. In fact, many CxO's find that the stricter the rules, the less employees pay attention, leading to even less IT control of the computer infrastructure.

One particularly difficult area to secure is the multiple-location workforce. This type of employee works at home one or two days a week, and perhaps travels out of town on business a couple of times a month. She cannot be disconnected from the office during all of those times, so she has a laptop to do her work and a couple of USB drives to move data around when switching computers.

This type of work flexibility is quickly becoming common. To get an idea of how widespread this situation has become, Forrester Research reported earlier this year that 64% of US-based employees telecommute at least one day per week. And these numbers are expected to continue to grow over time.

Understanding the Security Challenge of Portable Users and Devices

You've seen that many employees regularly work outside the traditional workplace. Another interesting data point is that this kind of work flexibility can lead to an increase in incoming attacks. For example, the following graph (see Figure 1) shows that the likelihood of a network being attacked consistently increases as the number of remote workers increases (Source: Webroot Research, May 2010).

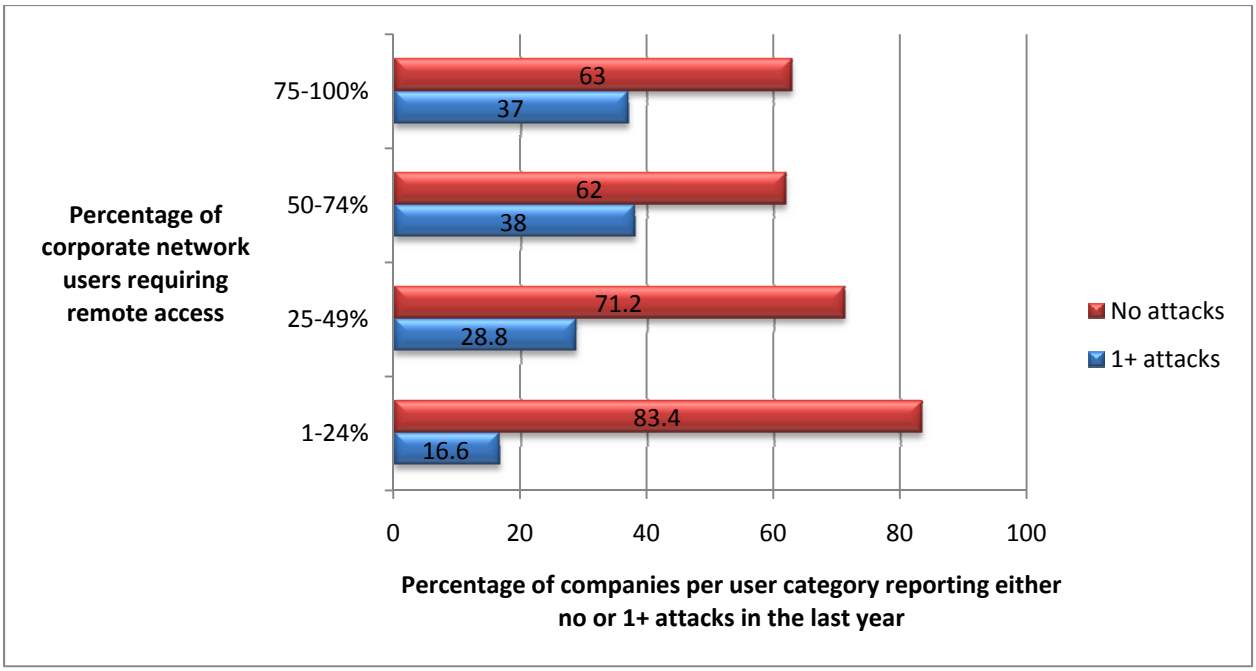

Figure 1: Telecommuting can lead to an increase in incoming attacks.

These statistics should alarm you. Not only are a large number of employees working outside the traditional office, they are doing so frequently and without formal documentation. In many cases, IT decision makers and technologists are unaware that it is happening. Planning a security strategy against an unknown workplace behavior is, at best, a difficult challenge.

Let's take a look at a common small business network. For simplicity, the components shown in Figure 2 are limited to the components that impact Web security.

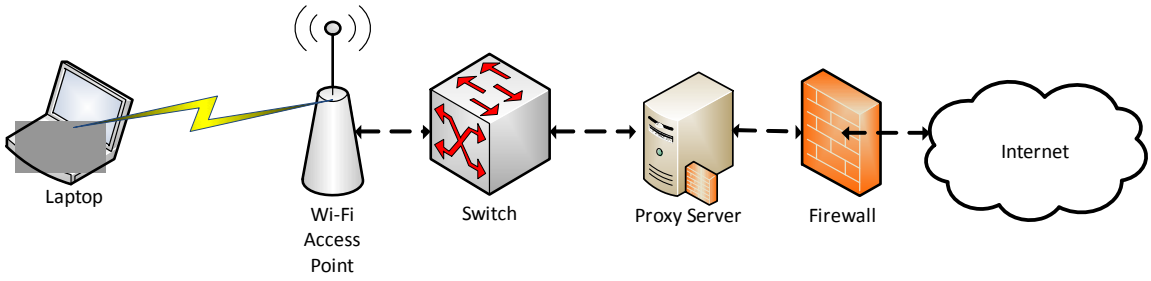

Figure 2: A laptop connecting through a corporate network to a Web site.

You can see that the corporate network is well protected. We have encrypted data between the laptop and the wireless access point, often using advanced encryption such as Wi-Fi Protected Access (WPA) and mutual authentication. The proxy server does a great job of applying corporate rules around data use, filtering some types of content, and so on. We also have a dedicated firewall to block all types of attacks including Web-based threats. This setup compares unfavorably to the typical home network that an employee uses at least one day a week (see Figure 3).

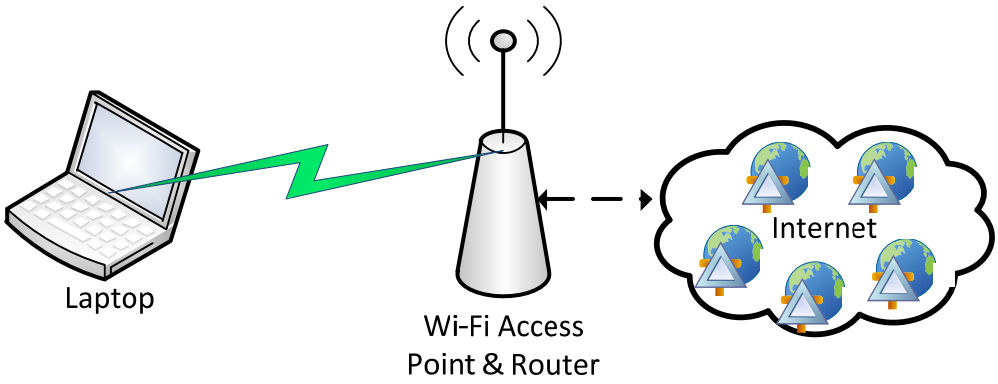

Figure 3: Much less security in the work-at-home flow.

Figure 3 shows a lot less complexity. Although simplicity can mean improved security, in this case, it is not a benefit. The wireless connection to the access point is typically either unencrypted or uses weak Wired Equivalent Privacy (WEP) cryptography. And the typical combination router and access point device supplied by an Internet Service Provider (ISP) does not offer significant defense against Web-based attackers.

> **Note**
> Figure 3 shows a work-at-home flow; the same diagram accurately represents most public wireless access such as coffee shops, airports, and libraries.

A core problem lies in the fact that the same laptop (or any other portable device) will be used at multiple locations. Each of those locations has its own security protecting it against Web threats. But, as you can see from these two figures, security between networks varies drastically.

Addressing Security on Portable Devices

The historic approach to dealing with portable users and devices connecting to dubious networks has been to implement client-centric security—putting very stringent security measures on the client computer (in this case, the laptop). But this method introduces numerous drawbacks and challenges to the IT professional:

- Computers that do not update security or operating system (OS) software
- Computers that fail to apply current security policy from the office network
- Computers that remain compromised over time
- Users that subvert security measures, intentionally or unintentionally
- Users that employ corporate resources at home and violate corporate policy, such as browsing illegal or inappropriate Web sites
- Users that unintentionally transport malware between home and work networks, circumventing corporate security measures

This is not to say that local security measures do not have value. On the contrary, malware scanners and firewalls prevent numerous attacks on roaming client computers every day. But they cannot be relied upon for complete protection in an unmanaged workflow or in risky environments.

Cloud-Based Web Security

Cloud-based security has recently evolved as a strong solution to address the challenges of portable device security. It complements other security measures by providing an extra layer of security against Web threats. Typically, cloud-based Web security solutions are managed by the cloud provider, which means the security follows the device and works equally well from home, work, and the coffee shop.

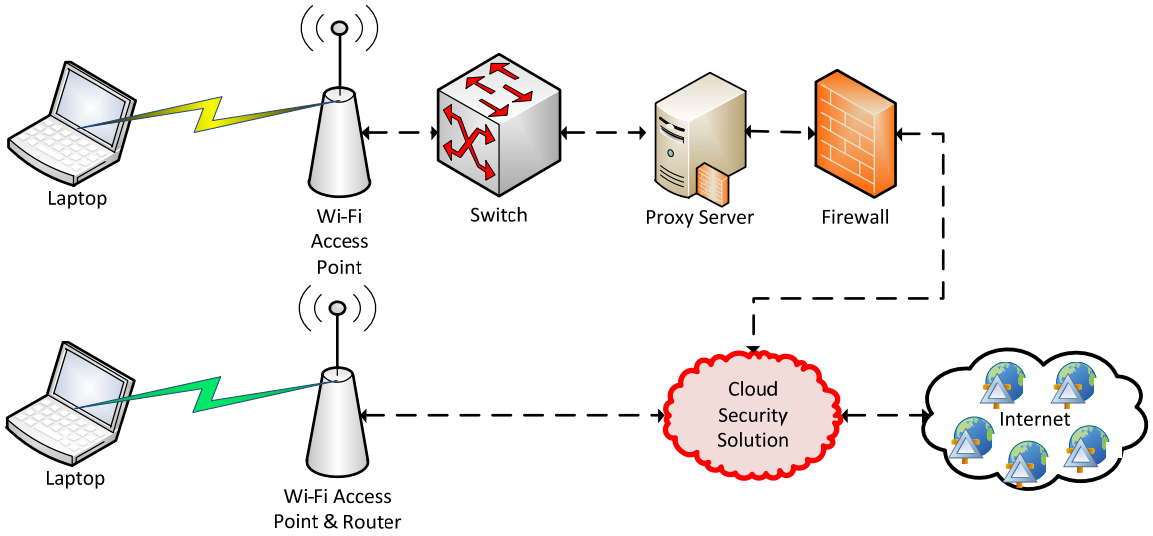

Figure 4: Using a common cloud-based security solution from any location.

Figure 4 illustrates how the cloud-based Web security approach it integrates into both the corporate and home network environments. There are numerous benefits to this type of security approach:

- Continue to receive security benefits from existing security solutions
- Consistent security policy applied at all locations
- Dedicated third-party management of security solutions, often with guaranteed service levels
- Simple integration into existing networks and devices
- Reduced security workload for corporate IT personnel
- Centralized accounting and reporting of Web activities for compliance reporting
- Layered security controls provide complementary security benefits

One indirect benefit that is difficult to quantify is the knowledge that both corporate and remote users have a constantly managed security layer between them and attackers. Many of the worldwide computer security threats over the past several years would have no impact on systems that use this type of security.

Summary

All IT resources need to be protected. Whether they're used in the home or workplace, devices that are compromised will cost the company time and money. And as more employees take their work home regularly, solutions must be in place that help protect users and keep their systems in compliance with policy. An excellent solution to this challenge is the recent advancement of cloud-based security solutions, which complement existing security and work virtually anywhere to filter Web-based threats and policy violations.