NETGEAR®
Connect with Innovation™

Whitepaper

7 Ways IT Creates Security Breaches and How to Fix Them Right Now

Introduction

A Simpler Time

Fifteen years is a lifetime on the Internet. Back in the mid-'90's, DSL was still the Next Big Thing. Most people dialed up AOL from their homes. Workplace access was tightly regulated, and smart phones weren't even a dream. YouTube—never mind Netflix—would have brought the Web to a crawl. Social media like Facebook, Twitter, Google+, and LinkedIn were a decade in the future, and the day's online threats—Michelangelo, OneHalf, Concept—seem almost quaint in comparison to industrial-strength malware like Stuxnet, ZeuS, and Hydraq, "spear phishing" social-media exploits, and keylogging spyware. Yet in 1994, the year browser pioneer Netscape was founded, basic firewall technology was already mature.

From their position at the network's edge, firewalls examine traffic passing through packet by packet, and block anything their rules say looks suspicious. Those rules were, and still are, pretty simple—block traffic using risky protocols like Telnet (used for remote login) or traveling to or from ports (logical data connections) that are rarely used for email, web browsing, file transfer, or other legitimate business. The most advanced, "stateful" firewalls add a few rules about the state of the data connection (starting, ongoing, invalid), but still follow the same basic principles.

The idea was to keep hackers and malware from exploiting any of the thousands of protocols and ports available on any typical computer or business network. And firewalls worked well—so well, in fact, that even as late as 2004, a business conversation might go:

"What are you doing about IT security?"

"We have a firewall."

"Oh."

Fast forward

No more. Today's threats are more complex, move faster, and exploit more vulnerabilities than 1994-era technologies ever anticipated, including:

- **Customized threats**—hackers now target individual small businesses[1] using Zeus and other malware attack "kits" sold online to create custom-crafted code that packet-based firewalls and signature-based antivirus software can't detect, much less stop.
- **Social-media "scareware" and phishing attacks**—"social engineering" attacks now harvest information from sites like Facebook or LinkedIn, then use it to trick employees into installing fake antivirus software or visiting malicious websites masquerading as YouTube videos, and hidden behind "bit.ly" shortened URLs
- **Mobility**—perimeter-based firewall defenses can't protect the exploding number of mobile devices, whose users may connect through your WiFi networks to avoid their providers' data limits. "Sniffing" attacks at locations you can't control can reveal passwords that put your network at risk.

New technologies called Unified Threat Management (UTM) firewalls combine traditional firewall technologies with new, cloud-based services that address these threats and even combat more sophisticated exploits of application vulnerabilities. But habits established over long years of relying on simple firewalls can create a false sense of security, and obscure the need for an upgrade.

Bad habits

These seven "bad habits" are holdovers from those early days. They persisted because of firewall limitations you had to either accept or work around using stopgap measures. But in today's threat environment, habits like these can actually make your small-business network less secure.

1. **One size fits all**—Simple firewalls can't align protection to the requirements of different job roles, departments, hours, days, or seasons. So small businesses needed to apply a single set of rules—often the default rules that came with the firewall—to everybody. But while blocking all traffic to and from Twitter may keep production personnel from installing "scareware", for example, it also cuts Marketing off from a valuable way to promote products and services. UTM firewalls allow policy flexibility, so you can protect critical areas like HR/payroll, R&D, or Legal, defend vulnerable areas like call centers, all without throttling back productivity of Sales, Marketing, and IT, or frustrating them into risky security evasions and workarounds.

2. **Special exceptions**—The opposite of "one size fits all" is just as bad. Faced with the "one size" limitations of simple firewall security, businesses create a patchwork of favors and exemptions to avoid short-term conflicts and productivity bottlenecks. These include separate, "privileged" devices, applications, and networks, in a never-ending parade of special cases and one-off workarounds. Accumulated over years, this habit creates an unmanageable rat's nest of ad hoc policies and exceptions, until inevitably something nasty slips in, or something valuable slips out. UTM firewalls let businesses develop coherent access policies tied to their Active Directory databases, and then apply them systematically across all individuals and departments.

[1] Geoffrey A. Fowler and Ben Worthen. "Hackers Shift Attacks to Small Firms." The Wall Street Journal. (New York: News Corporation, July 21, 2011). http://online.wsj.com/article/SB10001424052702304567604576454173706460768.html

3. **"Do it yourself" and point solutions**—Creative problem-solvers relish a challenge, so often their first reaction to firewall gaps and limitations is a little generic hardware, some script magic, and a late night or two. Custom solutions work well in the environment for which they were designed, but may not adapt or scale well. When your company networks change or grow, those solutions may add more burden than value, and don't stay secure very long. UTM firewalls offer a gap-free manageable alternative at far lower cost than maintaining a brittle patchwork of ad hoc solutions.

4. **Social-media blind spots**—Having grown up with computers, younger employees have an intuitive understanding of how technology works and a casual acceptance of technology as an integral part of their lives. Blind to the business risks of opening your workplace to Facebook, Twitter, and nonstop IM traffic, their at-work social networking—using workplace computers and WiFi networks to avoid racking up smart-phone data charges—creates security risks for your business. UTM firewalls help you establish and communicate reasonable boundaries and exceptions that work for both your employees and your business, without forcing you into a police role that compromises employee morale.

5. **Focus on technology**—Firewalls and other technical solutions are essential for security, but they're not enough. After all, human error, not technology, is responsible for most security breaches. Employee IT security training often gets neglected under the pressure of other obligations and false confidence that a firewall will take care of everything. But that lack of training and awareness has consequences when end-users don't understand how to avoid IT risks. UTM firewalls bridge the gap between technology and training by applying the same set of policies to filter traffic at the network edge that you use to educate employees in training sessions and employee manuals.

6. **Focus on what's new**—It's human nature to focus on the latest and greatest, and that includes online threats. But the vast majority of malware directed against your business consists of old, well-recognized threats, still effective against out-of-date operating systems, browsers, and applications. Even a single old vulnerability can put your network at risk, but nobody has the time or motivation to patch, upgrade, or replace that old Windows NT print server that seems to work just fine. UTM firewalls aren't a substitute for good endpoint defenses, but by keeping both new and old malware off your network, they add an extra layer of protection.

7. **Focus on headquarters**—Security is a global imperative, but small-business people work with what's in front of them. A firewall at your headquarters network perimeter doesn't protect branch offices, work-from-home employees, or field sales staff. With integrated Virtual Private Network (VPN) technology, a modern UTM firewall protects employee communications that originate outside your network perimeter, even when the first link is an insecure coffee-shop or airport network. And UTM firewalls are inexpensive enough to deploy even at smaller branch offices.

Break the habits

Don't let old habits from the days of simple firewall security keep your business from the protection it deserves. Upgrade your defenses now with a UTM firewall solution that starts with all the features you expect from a traditional stateful firewall, and then adds comprehensive up-to-date protection, including:

- Advanced virus, malware, and scareware detection with automated updates based on millions, not thousands of signatures
- Stream-Scanning technology that keeps network latency low, even when scanning those millions of signatures
- Anti-Spam with fast local+cloud hybrid scanning that needs no "tuning" to work
- Flexible, automated Web, Peer-to-Peer, and IM usage policy enforcement
- Zero-Hour Threat Protection that stops even new and custom threats in real time
- Secure Remote Access using IPsec and SSL protocol Virtual Private Networks

And UTM firewalls do more than protect. In a companion paper, *Tame the Productivity Paradox—how to keep the Web and social media productive for your small business*, we outline the productivity gains available when you implement thoughtful policies for employee use of time- and bandwidth-hogging social-media, gaming, and entertainment sites.

NETGEAR® ProSecure® UTM Firewalls come in a full range of prices and capabilities to meet the requirements of any small or mid-size business. See how businesses like yours have upgraded their protection in NETGEAR case studies at: http://prosecure.netgear.com/customers/case-studies/index.php.

For more information, please review the full line of NETGEAR solutions at http://prosecure.netgear.com. Low basic hardware costs, simple subscription options, and no per-user licensing make even the best protection surprisingly affordable.

About NETGEAR

NETGEAR designs innovative technology solutions to address the networking, storage, and security needs of small- and mid-sized businesses. NETGEAR offerings include an end-to-end portfolio of networking products for sharing Internet access, peripherals, files, multimedia content, and applications among multiple computers and other Internet-enabled devices. Products are built on a variety of proven technologies such as wireless, Ethernet and powerline, with a focus on reliability and ease of use. NETGEAR products are sold in approximately 28,000 retail locations around the globe, and through more than 37,000 value-added resellers.