CHAPTER 24

LOCKING THE DOOR

BY ALAN ADCOCK

In the late 1990's I needed to transfer some files from my work computer to my home PC. I opened a few ports, started up the FTP software and went to the office. Transferring the files was no problem, but when I arrived home several hours later I noticed a lot of drive activity. Turned out someone had discovered the FTP site I left open and was using it to distribute their counterfeit software. It only took a few hours for someone on the Internet to find the site I left open.

This occurred in the early days of the Internet. Today, the number of IP connected devices has increased rapidly and the number of probing attacks on IPs has increased even faster. As The Gartner Group points out, "All organizations should now assume they are in a state of continuous compromise."

A prospective medical practice client recently called my company for help. They had a similar firewall port issue. One of their IT staff had left some ports open and as a result a hacker leaked confidential patient information onto the Internet. This resulted in a Health and Human Services, Office for Civil Rights investigation—and required a breach notification be sent from the medical practice to all of its patients. Ouch!

YOUR FIRST LINE OF DEFENSE

Today's businesses rely heavily on Internet connectivity for email, web, and remote access to office information from mobile devices, laptops,

and PCs. Unfortunately, with the convenience of connectivity comes great risk of unauthorized users gaining access to your business data for theft, harm, or destruction. The speed at which an unprotected network or mobile computer can be compromised is staggering. Simply put, your business has no business connecting to the Internet without serious protection. With the "business network" now extending to mobile devices, home offices, and the "cloud," securing the perimeter is no longer restricted to the brick and mortar office.

Here are a few questions to consider:

1. How do you defend your business data from nefarious outsiders while allowing workers remote access to resources?
2. How do you guard against sensitive information, like Social Security or credit card numbers, leaking out of your network and leaving you, as the business owner, open to huge fines and possible prosecution?
3. How do you guard against employees using the Internet in inappropriate or illegal ways?
4. How do you protect your business from malicious software designed to either steal or destroy your corporate data?

The answer is...a modern business firewall, which addresses these and many other issues. A firewall is designed to keep out the traffic you don't want, while allowing the traffic you do want in. This is why IT professionals say **a hardware firewall is the first line of defense for the modern office.**

FIREWALLS 101

Before we continue, let's cover some basics. There are two types of firewalls: software and hardware.

A "software firewall" is an application installed on a single computer, often called a "personal firewall." Microsoft includes Windows Firewall in its popular desktop operating systems. While providing rudimentary protection, this software is often considered a nuisance and frequently disabled by users. Doing so leaves the user's laptop extremely vulnerable to compromise and infection, especially when connected to a public Wi-Fi hotspot. Software firewalls are also often bundled with anti-virus/

anti-malware software. The bottom line is software firewalls are chiefly for personal protection of a single device.

A "hardware firewall" is a dedicated device specifically designed for protecting a local network, such as your office PCs, servers, and printers from Internet threats. Hardware firewalls range from very simple, inexpensive, consumer-grade devices to complex machines that rapidly analyze information streaming to and from the networks of very large organizations. Fortunately, small and medium organizations are able to select from a variety of robust business-grade devices to protect their valuable data.

FIVE DANGEROUS MYTHS AND ASSUMPTIONS

Over the years, I have met with hundreds of business owners who believed—with good reason—that their networks were sufficiently protected. Here are a few of the unfortunately inaccurate statements and assumptions I've heard:

1. **"I already have a firewall from my Internet Service Provider."**
   Cable modems are not firewalls. Neither are DSL (or fiber, or T-1, etc.) converter boxes. While these boxes allow one or more computers to connect to the Internet, they provide little to no security for your network. They may "translate" your internal network addresses to a single "external" address to traverse the Internet, but a savvy hacker can easily retrace the steps back to your PC, like a burglar following his next victim home from the mall.

2. **"I've had a firewall for years."**
   Internet threats rapidly evolve. For instance, it used to be common practice for anti-virus software vendors to send out weekly updates. Today, "zero day exploits" make it necessary for anti-virus software to update several times daily. In the same manner, today's typical hacker isn't a maladjusted, geeky teenager looking for a thrill. Cybercrime is BIG business and is backed by organized crime and even nation-states. No one connected to the Internet is safe from these predators.

3. **"I am a small business. I don't have any information that anyone would want."**
   Wrong! Small businesses are even more likely to be attacked than the big guys. Why? Simply put, small businesses are easier prey. Security reports, such as those from Verizon and Symantec, show attacks on small businesses are increasing annually with thieves targeting data such as credit card numbers, customer information, and even locking up computers until a "ransom" is paid.

4. **"I already bought what I need from the office supply store."**
   Cheap, consumer grade broadband routers are not an option for anyone serious about their business. Low-cost routers lack the features necessary for strong perimeter defense, have minimal ability to be customized for specific business needs, provide little useful logging, and are unable to alert you of suspicious activity on your network.

5. **"So what if I get hacked? I have insurance that will cover it."**
   While cyber insurance is important, there's no way to insure against a damaged reputation once news of a data breach gets out, especially if it includes customers' personal or financial information. Few businesses recover from such a blow. If the hacker obtains bank account numbers and credentials, a business can be financially wiped out overnight. Even if insurance covers the loss, the ability to pay suppliers, meet payroll, or pay taxes may not occur quickly enough to avert disaster. Consider two things: How dependent is your business on the Internet for email, ordering, etc.? How long could your business survive if a cyber-attack closed you down for three days, a week, or longer? (Hint: most businesses don't survive.)

ACRONYMS AND DEFINITIONS TO HELP YOU WADE THROUGH THE MARKETING

It seems like all IT systems get buried in a sea of acronyms that mean different things to different vendors. To help you wade through the techno-speak and marketing hype as you try to find the right firewall solution to protect your business, here are some common terms and acronyms:

DMZ: Demilitarized Zone. In firewall terms, this is a network sectioned off from the main company network, usually containing Internet-facing servers, such as web servers. Security is handled differently for these servers than for the rest of the network.

DoS: Denial of Service, a type of attack used to overload a company's computer system.

IPS: Intrusion Prevention System, a key feature of NGFW (Next Generation Firewall) that evaluates traffic coming from the Internet and compares it to signatures, much like anti-virus software does for files on a PC.

NAT: Network Address Translation is a system which allows a company's internal IP address range to communicate out to the Internet IP range. A small company will typically have 5 to 14 public IP addresses assigned by their Internet Service Provider (ISP) and have 254 internal IP addresses for servers and desktops inside the company.

NGFW – Next Generation Firewall. (All vendors want their product to be the latest and greatest!) This term is used by many vendors and refers to the same feature set as a UTM (Unified Threat Management) appliance.

Port: A number from 1 to 65535 that serves as a specific "doorway" data uses to enter or leave a network. Some ports are assigned to a particular service (email commonly uses ports 25 or 110). Opening or blocking ports is an essential part of firewall security.

SMTP / POP: Two types of email systems.

TCP, UDP: Two ways information is "packaged" for transmission across networks.

VPN: Virtual Private Network, used to create a secure "tunnel" through the Internet for business communication.

WPA2 - A recommended type of security used in Wireless networking.

UTM - Unified Threat Management, a modern, advanced firewall. Exactly the same as NGFW.

BEYOND THE BASICS

We once visited a prospective client who, when asked about their firewall, pointed to "that small box with blinking lights" on a shelf. It was a router. I don't know if their former IT vendor called it a firewall, but the client certainly felt they were protected from the Internet by those blinking lights. We had to gently break the truth that their "firewall" was no better than a butler letting in anyone who came knocking at the door. (If you're not sure you have a firewall in place today, put down this book and talk to your IT staff/vendor immediately!)

Basic firewall technology has become a key part of many companies' security defense strategy. A traditional firewall will provide packet filtering, network-and-port-address Translation (NAT), thorough inspection of Internet traffic, and virtual private network (VPN) support.

Unfortunately, cyber-attacks have become more sophisticated and are targeting more than just "big business" these days. As a result, most small and medium-sized businesses are in need of more than just a basic firewall to protect their critical data and operations. As the pace of technological change continues to move quickly, firewall technology has become much more sophisticated. These newer, more advanced firewall solutions are known as **"NextGen Firewalls"** (NGFW).

NextGen Firewalls include the typical functions of traditional firewalls, but go deeper into the layers of Internet traffic to improve filtering of network traffic dependent on the packet contents. The key differentiators between traditional and next generation firewalls include:

Anti-virus / Anti-spyware: Protects against the latest content-level threats by detecting and removing malicious software.

Anti-spam: Significantly reduces spam volume at the perimeter for superior control of email attacks and infections. The firewall manufacturer develops and maintains accurate lists of spammers and spam content.

Application Control: By using "digital fingerprints" the NGFW can identify applications even if they are not running on their traditional port numbers. Once applications are identified, policies can be added to the firewall to control access to those applications in line with corporate policies.

External Data Inclusion: For a NGFW to function properly it needs to pull data from external systems. User information from Windows Active Directory, white/black lists for IP addresses and mail servers, and web filter categorization lists are examples of external data sources firewalls need to query in order to build successful security policies.

Intrusion Prevention Service: This integrated system protects against known and unknown network-level threats, including command and control traffic and botnet attacks, by examining network traffic for attack signatures.

Reporting: NGFW should be able to create reports based on included features to provide better visibility on firewall activity.

SSL Decryption: SSL refers to a type of encrypted traffic on the Internet. It is important for a NGFW to be able to look inside this SSL traffic to make sure it is not used to circumvent other firewall controls.

User Identification and User Based Policy: In networking systems it is difficult to identify individual users, so it is important to set policies in the firewall for users to move around the network and use different PCs and laptops.

FIVE (5) BEST PRACTICES OF FIREWALL OPERATION

In my experience, sometimes even with a NGFW firewall present, the business is not truly protected. In order for a firewall to properly protect your business, you must do the following:

1. Enable the Advanced Features

While it may seem obvious to fully utilize all the features that come with a firewall, all too often firewalls are installed with only a basic setup, not utilizing the feature set originally purchased. NGFW devices have a ton of options. It is often beyond the ability of an IT generalist to correctly implement these configurations, so a security provider may be needed to help lock down the network.

2. Review Configuration Regularly

It is very important to review firewall configurations to ensure changes which leave the network vulnerable do not occur. With any IT project, the initial setup of equipment is planned out and documented to be sure it will function as expected, but devices can become neglected over time. Adding a scheduled review of firewall configurations should be part of every company's security plan.

3. Configure Alerts

All NGFW devices have alerts and reports which can be generated from the system. There are even services that take this data and load it into databases for additional reporting and analysis. All companies should set up threat alerts to report directly to internal IT staff. It is also worth considering having a Managed Security Service Provider (MSSP) engaged in monitoring and responding to threats.

4. Keep Software / Signatures Up to Date

As the nature of threats on the Internet are ever-changing; you need to make sure your company's security response is also constantly updated. This is usually accomplished by having a current subscription with the firewall manufacturer and making sure the device is configured to receive updates.

5. Backup Configuration

Most companies have elaborate systems in place to backup data on servers and workstations. Unfortunately, this attention to backup does not typically extend to networking equipment like firewalls. As NGFW devices add more and more features, the configurations quickly become very complex. Manually rebuilding one of these device configurations would lead to significant downtime and lost productivity, so all businesses should manually or automatically back up configurations.

IN SUMMARY

The overall pace of technology advancement has enabled companies to do more with automation, while simultaneously introducing new risks. The struggle between hackers and security providers continues to escalate and requires continuous security improvement to overcome new types of threats. With all this in mind, it is vitally important for all companies to invest in firewall security as a fundamental part of their infrastructure.

About Alan

Alan C. Adcock has been "messing around" with technology for more than 30 years, and yet somehow never gets tired of this ever-changing industry. Alan is CEO of Automated Solutions Consulting Group (ASC Group) in Alpharetta, Georgia. Founded in 1999, ASC Group provides remote network monitoring and management, strategic technology consulting, lifecycle planning, Internet security, data storage and security, and cloud solutions. Many ASC Group clients have been clients for 15+ years.

Alan began his IT career at the age of 17 by working with a local systems integrator as a PC technician, eventually becoming the Senior Systems Engineer and Project Manager at that company. Later, he served as the Vice President of Information Technology for one of Atlanta's largest Real Estate Investment companies. In this role, Alan was responsible for all aspects of technology planning, including computer systems, telecommunications, office equipment, and project management, as well as coordinating technical support and managing a budget for over 155 users.

Alan co-founded Automated Solutions Consulting Group with Gary Smith in 1999 to serve small businesses that needed affordable CRM software solutions and dependable networks to automate their operations. Upon the death of Mr. Smith in 2007, Alan re-focused ASC Group exclusively on network engineering solutions for multi-server, multi-site organizations. ASC Group has since evolved into a full-service network services provider, and serves small-to-midsize businesses, medical practices, private schools and non-profit organizations in the greater Atlanta area.

While working with clients, Alan has seen first-hand the challenges posed by increasingly complex security and compliance demands. Today's smaller organizations have to be prepared to face the same (or greater) threats as large corporations, and ASC Group's goal is to bring big company technology solutions down to the small business level.

Alan grew up in Roswell, Georgia, and is a graduate of Georgia Tech. He currently resides in Woodstock, Georgia, with his wife and son.