13 ways through a firewall: What you don’t know can hurt you

How secure are firewalls?

Fast Forward:
- Firewalls are a staple of industrial cybersecurity programs, but how secure are they?
- Any time a firewall deployment is considered, relevant firewall vulnerabilities should be identified, and both compensating measures and alternatives should be evaluated.
- Unidirectional security gateways are a comparatively new alternative that all security practitioners should become familiar with.

By Andrew Ginter

Firewalls are seen as pillars of both business-focused and industrial, control-system-focused cybersecurity programs. But how secure are firewalls really? Firewalls have been with us for 25 years. While firewall limitations are well known to both black-hat and white-hat experts, those limitations are not as well known to everyday security practitioners.

This article catalogs 13 classes of attacks, which target firewalls, or target the systems that firewalls are supposed to protect. Each attack description is written as if the objective was to penetrate only one layer of firewalls. In practice, firewalls are deployed in many layers separating the Internet from industrial control and safety networks. The descriptions, though, generally describe only an attack through one layer each, the thinking being that if one layer of firewalls can be breached, then new attacks can be mounted on the next layer of firewalls in the layered defensive architecture.

Rather than simply sow fear, uncertainty, and doubt, we also evaluate a handful of alternatives and compensating measures. A “green” grade means the measure blocks nearly all attacks in the class. “Yellow” means only some of the attacks can be blocked. “Red” means the measure is largely ineffective for this class of attack. For intrusion detection technologies, the green/yellow/red grades mean the technology can detect nearly all, some, or none of the attacks in the class.

The alternatives and compensating measures are:

**2-FACT:** 2-factor authentication is the use of biometrics, smart cards, or some other measure in addition to a password to identify and authenticate individuals seeking to access protected equipment. 2-factor authentication is used regularly on remote access mechanisms for industrial networks but is used much less commonly inside industrial networks, in part because of concerns about slowing down emergency response in safety emergencies.

**ENC:** Encryption is the use of cryptosystems to protect either the confidentiality or authenticity of data communications mechanisms. Encryption is starting to be used fairly routinely in client/server interfaces for modern control systems, and these are the communications most likely to pass through a firewall. Encryption is
occasionally used when data must pass across wireless networks or wide-area networks. Encryption tends not to be used when communicating between distributed control system (DCS) software and programmable logic controllers (PLCs) or other devices.

RULES: Firewalls themselves can protect against some attacks if their configurations and rules are improved or made more specific.

HIDS: Host intrusion detection and intrusion prevention systems can detect and/or prevent certain classes of suspicious activities. Anti-virus systems, application control/whitelisting systems, removable device controls, and file-change monitoring all fit here. These are all technologies intended to harden the typically “soft interior” of control networks.

NIDS: Network intrusion detection and intrusion prevention systems can detect and/or prevent certain classes of suspicious communications. These systems may be separate appliances, or they may be built into firewalls. These systems may be signature-based systems or may be learning-based or anomaly-based systems as well.

PATCH: Security update programs or “patch” programs regularly test and install updated versions of software and operating systems to repair the software defects, which are security vulnerabilities. Patch programs are particularly challenging for change-controlled networks because of the risks to safety and to reliability that are inherent in any changes to executable code.

UGW: Unidirectional security gateways allow information to flow out of a protected industrial network but are physically unable to send any attack or communication at all back into the industrial network. The gateways replicate industrial servers to business networks. Business applications and business users access only the replica servers.

<table>
<thead>
<tr>
<th>Table of mitigations</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
<tr>
<td>Phishing</td>
</tr>
<tr>
<td>Social engineering</td>
</tr>
<tr>
<td>Compromise a domain controller</td>
</tr>
<tr>
<td>Attack exposed servers</td>
</tr>
<tr>
<td>Attack exposed clients</td>
</tr>
<tr>
<td>Session hijacking</td>
</tr>
<tr>
<td>Piggy-back on VPN connections</td>
</tr>
<tr>
<td>Firewall vulnerabilities</td>
</tr>
<tr>
<td>Errors and omissions</td>
</tr>
<tr>
<td>Forge an IP address</td>
</tr>
<tr>
<td>Bypass a network security perimeter</td>
</tr>
<tr>
<td>Physical access</td>
</tr>
<tr>
<td>Sneakernet</td>
</tr>
<tr>
<td>Totals:</td>
</tr>
</tbody>
</table>
With that introduction, let’s look at the 13 ways through a firewall – and how well the alternatives and compensating measures address each type of attack.

#1 Phishing: Phishing attacks send email through a firewall to persuade recipients to either reveal passwords or to download and run malware. “Spear phishing” is the method of choice for advanced, targeted attacks. Spear-phishers produce extremely convincing emails, based on public information about specific target individuals’ interests, associates, and activities. Best mitigations: plant firewalls should not allow email and other Internet-originated content into industrial networks. Unidirectional gateways do not permit any communications or attacks into plant networks. Encryption and two-factor authentication really do not help with phishing attacks – the victims of the attack are already logged in using their credentials and frequently pull the attacks on to their computers using encrypted connections.

#2 Social engineering: Password theft is most easily accomplished by social engineering – look under a victim’s keyboard, or look for a sticky note on their monitor, or shoulder-surf while they type their password. Sometimes simply calling the systems administrator and weaving a convincing tale of woe is enough to persuade this person reveal a password or even create an account for the attacker. More exotic password theft is accomplished by tricking people into installing keystroke loggers. Best mitigations: two-factor authentication means a stolen password alone is not enough to grant access. With unidirectional gateways, even with a stolen password, the gateways are unable to communicate any attack back into a protected network.

#3 Compromise a domain controller: Or more generally, compromise a trusted external asset. Historically, control systems were designed so that they did not rely on any external system for correct, safe, and reliable operation. In recent years, this has changed in many organizations. Control systems now often rely on IT domain controllers, domain name servers (DNS), or enterprise resource planning (ERP) servers for example, even though those external servers are not managed as safety-critical or reliability-critical assets. Take domain controllers for example: in many businesses, when an employee leaves the company, one mouse-click disables that employee’s accounts company-wide, including accounts on industrial control systems. This turns the central domain-controller into a single point of failure for all industrial systems in the business. When attackers compromise a domain controller, they no longer need to attack other systems – they can simply change existing passwords or create their own accounts and passwords. Best mitigation: do not allow industrial systems to trust a corporate domain controller. Firewall rules and unidirectional gateways can prevent such trust relationships by blocking all communications from corporate domain controllers.

#4 Attack exposed servers: Industrial servers are notoriously vulnerable to buffer-overflow, SQL-injection, cross-site scripting, denial-of-service, and a host of other kinds of attacks. Signature-based network and host intrusion detection and prevention systems can detect/prevent well-known attacks but cannot detect never-before-seen “zero-day” attacks. Industrial security researchers routinely report finding a dozen or more zero-day vulnerabilities in every industrial software system or device they look at, after only a handful of hours of
investigation. For the foreseeable future, it appears that it will continue to be very simple to find industrial zero-day vulnerabilities. Anomaly-based detection and prevention systems can detect some zero-day attacks. Application control/whitelisting systems can catch many zero-day attacks. Best mitigation: replicate industrial servers to business networks via unidirectional gateways rather than accessing those servers directly through firewalls.

#5 Attack exposed clients: Industrial client software is just as vulnerable as industrial servers. A compromised server on an external network, such as the business network, can propagate attacks back into industrial clients. For example: pull a file from a virus-infected file server, and now there is a virus on the industrial network. Pull a web page from a compromised web server, and drive-by malware can wind up on the industrial network. Anti-virus systems, and both host and network intrusion detection/prevention systems, are as ineffective for these attacks as they are for attacks on industrial servers. Best mitigation: do not allow industrial clients to access servers on less-trusted networks, either by changing firewall rules or by deploying unidirectional gateways. Deploy application control/whitelisting systems.

#6 Session hijacking: Taking over existing communications sessions via man-in-the-middle attacks allows attackers to insert their own commands into existing, authenticated communications streams. This attack is most easily accomplished with freely downloadable software tools, either on a local area network (LAN) segment or by impersonating a wireless hotspot. Best mitigation: Encrypt communications sessions carrying commands, and train people not to ignore or "click through" encryption error messages and warnings, or deploy unidirectional gateways to prevent the receipt of any commands from less-trusted networks.

#7 Piggyback on VPN connections: When a trusted insider is provided with a VPN account and password, most people assume they are providing that person with remote access to a trusted network. In fact, those credentials provide the trusted individual’s computer with access to the trusted network. Malware in control of a computer can jump across VPN connections terminating in that computer, and a compromised computer coupled with split tunneling enabled allows distant attackers to launch interactive remote control attacks on industrial assets across VPN connections. Best mitigation: Do not allow VPN connections to industrial network, either by reconfiguring firewalls or by deploying unidirectional gateways.

#8 Firewall vulnerabilities: Firewalls are software. All modern software has defects, some of which are security vulnerabilities. In recent years, disturbingly simple vulnerabilities have been discovered in firewalls widely used in industrial settings – vulnerabilities as simple as hard-coded passwords and encryption keys. Surprisingly, some firewall vulnerabilities, such as cross-site scripting vulnerabilities in HTTP-based “VPN” proxy servers, are so-called “design vulnerabilities.” Design vulnerabilities are security issues in software that may never be corrected because the vulnerabilities are essential to the designed and desired operation of the software. Best mitigation: use hardware-enforced unidirectional gateways rather than software-based firewalls for security.
#9 Errors and omissions: Modern firewalls are complex. It is not unusual to require at least eight weeks of full-time training to become familiar with most of the features of one firewall. Small configuration errors can expose protected equipment to attack, and the hundreds of screens in the configuration tools for modern firewalls make tracking down these errors very difficult. Best mitigation: deploy unidirectional gateways where the gateway hardware protects the safety and security of industrial networks, no matter how the gateway software is configured.

#10 Forge an IP address: Most firewall rules are expressed in terms of IP addresses or ranges of IP addresses. Forging an IP address is often enough to persuade a firewall to accept at least some communications from an attacker. Forging an IP address can be extremely simple – just bring up the user interface on a computer and change the address to the address of the computer that a more-trusted user logs into. This works best if the attacking computer is on the same LAN segment as the more-trusted computer, and the more-trusted computer is a laptop that is currently absent from the LAN segment. Best mitigation: unidirectional gateways block all attacks from untrusted networks, no matter their IP address.

#11 Bypass a network security perimeter: Complex networks may have non-obvious, unprotected paths from business networks to industrial networks. Well-meaning insiders may set up rogue wireless access points on critical networks. Industrial networks might physically extend beyond physical security perimeters and so expose those networks to unauthorized connections. All of these conditions result in electronic communications being accessible to attackers without traversing the firewall. Best mitigation: Strict network monitoring can help detect new wireless connections and foreign IP addresses. Regular scrutiny and/or simplification of networks is necessary to keep network perimeters defined and secure.

#12 Physical access: With many firewalls, if an attacker can touch the device, they can compromise it. Some firewalls have administrative ports that permit unauthenticated access to change configurations. Most firewalls can be physically reset to factory defaults and reprogrammed, or the firewall can simply be physically replaced with a router. Other tampering is possible for sophisticated attackers. Best mitigation: physical security programs protect the physical integrity of the network perimeter. Some equipment has a degree of tamper-proofing built in, but a physical security program is the best mitigation here.

#13 Sneakernet: Carrying CDs, USB sticks, or even entire laptops past physical and cyber security perimeters can expose industrial networks to malicious code. These attacks might be by disgruntled insiders or by poorly-trained or deceived insiders. Best mitigation: end-users must be trained to know that movable media is dangerous. Device/media control software can limit the ability of malware to execute while on the physical media. Application control/whitelisting systems can catch many kinds of movable media and zero-day threats.

The bottom line
In a sense, it is not surprising that there are many kinds of attacks possible on firewalls. The ISA-99 series of standards, NERC-CIP, API 1164, and many other industrial security standards and guidance have a great deal to say about how any one firewall must be managed in order for it to remain somewhat secure. This makes firewalls a difficult technology to manage. To keep firewalled connections even reasonably secure takes a great deal of effort in the form of processes, procedures, testing, reviews, audits, documentation, and other recommended activities.

If we assign weights of 2/1/0 to the green/yellow/red grades, we can get an idea of how effective is each of the alternatives and compensating measures. By this metric, firewalls themselves do reasonably well as mitigation against firewall-based attacks: simply manage the rule set very cautiously, and do not enable all of the tempting features of modern firewall appliances.

By the 2/1/0 metric, though, the single most effective alternative is the hardware-based unidirectional gateways. This alternative to firewalls is comparatively new. The gateways only came into widespread use in industrial settings within the last few years. Advice from a variety of experts is that unidirectional technology is something that all industrial security practitioners should become familiar with, and it is something that practitioners should consider deploying any time they consider deploying a firewall.

That said, looking at the table of mitigations shows that no single technology can mitigate all firewall/network threats. There are no silver bullets. No one technology fits in all circumstances or meets all needs. Industrial security practitioners must understand the limitations of each of the security technologies they deploy and must evaluate those limitations against business needs and safety and reliability requirements. A defense-in-depth security posture is still the right way forward in the vast majority of cases, and a layered approach to security includes not only firewalls but also a variety of security measures and technologies. Practitioners are encouraged to deploy the strongest applicable, practical security technologies in every layer of their defense-in-depth postures.

ABOUT THE AUTHOR

Andrew Ginter (andrew.ginter@waterfall-security.com) is the director of industrial security at Waterfall Security Solutions. Andrew spent 25 years developing – and leading the development of – control system software products, control system to ERP middleware products, and industrial cybersecurity products. Andrew represents Waterfall to ISA99, NERC-CIP, and other cybersecurity standards bodies and writes and speaks frequently on industrial cybersecurity topics.

Source:

http://www.isa.org/InTechTemplate.cfm?Section=Archives4&template=/ContentManagement/ContentDisplay.cfm&ContentID=92916