Why Firewalls Fail to Protect Web Sites

A White Paper by

Karl Forster
Lockstep Systems, Inc.
+1-480-596-9432
1-877-WEB-FIXR

info@lockstep.com

www.lockstep.com

Why Firewalls Fail To Protect Web Sites

The purpose of this document is to outline how a firewall works and how hackers get through your firewall and alter the web site content on your web server.

The Purpose of a Firewall

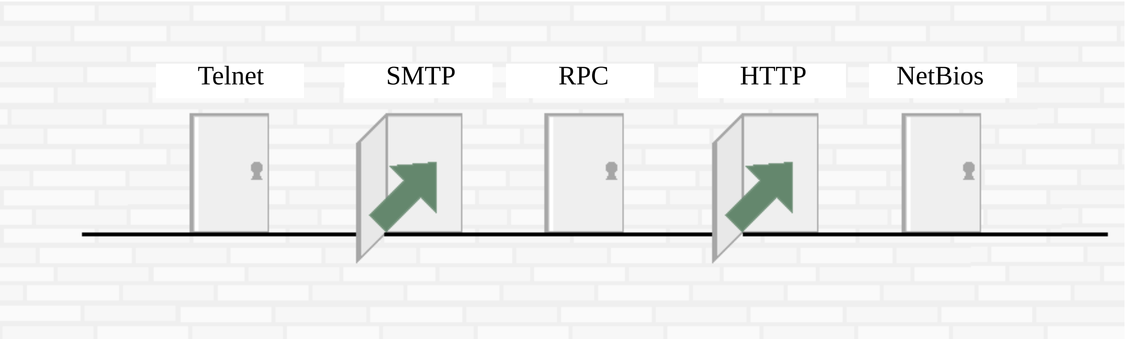
The firewall was designed as a gateway to allow or deny access to network resources. The firewall makes its decisions based on what the user wants to connect to, not what their intent is. When you have a web server, the firewall must grant access to the web site to allow people on the Internet to be able to give Internet visitors access to the web site content. Therefore, when a hacker requests to access the web server, the firewall has essentially been designed to grant access to the hacker.

A Brief History of Firewalls

The firewall was invented about a decade prior to the invention of the web server, and the original goal of a firewall was to prevent users on the Internet from accessing selective network resources.

Initial firewalls were designed as simple packet filters - they simply looked at what the user wanted to connect to and compared that to a list of allowed and disallowed resources. If the user requested a connection to an allowed resource, the firewall allowed access to the user. If the user requested a connection to a disallowed resource, the firewall did not allow the user access.

When the firewall is installed, the administrator gives the firewall a list of the resources they want to allow access to, and a list of resources to which access should be denied. Typically, the administrator allows access to resources such as e-mail servers and web servers. Each resource available on a network is assigned a "port" number, the number that corresponds to the type of resource. When the user wants to connect to a server resource, it specifies a port to connect to. For example: if the user wants to talk to an SMTP e-mail server, then they would connect to the port assigned to the SMTP protocol, which is usually port number 25.



Firewall vendors have concentrated on improving the manner in which the firewall handles different connections from users. The resulting new breed of "state full firewalls" has improved the way a firewall processes a user connection, but has not advanced the firewall beyond the original idea of either allowing or disallowing a communication to occur between a user and a server.

Why Firewalls Fail to Protect Web Sites

Over time, a company's network resources have grown to include the web server that hosts their web site. In order to view web site content in an Internet browser, users must be granted access to it, and this means that the firewall must be configured to grant users access to the web server. If the firewall blocks the web server, web site visitors would not be able to view the web content.

Access is Granted to Hackers

Once the firewall is configured to allow access to the web server, it will automatically allow all traffic to flow between the user and the web server. The firewall cannot differentiate between a nice user and a hacker, and as a result both are granted the same, authorized access to your web server.

Hackers Take Advantage of Known Errors

The most common way a hacker will take over the server is to take advantage of known errors in web server applications. Almost all web server software contains faulty code of some sort, and a hacker will use these glitches to his advantage. Examples include:

- In response to a form that asks for user information, a hacker types in commands that get executed by the web server.
- Many web servers offer debugging information to anyone who requests it through a standard web browser - including a hacker.
- A hacker can utilize an overflow capacity limitation on a web server by sending more information than the web server is expecting.

Buffer Overflow Error - CodeRed and CodeRed II virus

The most common error that hackers exploit is buffer overflow, which occurs when the hacker sends more information to the web server than it expects, and the server cannot correctly handle the overflow data. Extra data that does not fit in the allocated memory space can be used to alter the normal operation of the web server. When the overflow includes an executable file, the web server will run the program.

Buffer overflow errors have been widely reported in almost every brand of web server, running on every operating system. CodeRed and CodeRed II are examples of two of the largest mass hacks that utilized a buffer overflow error on the Windows IIS Server from Microsoft. The CodeRed viruses sent extra data to the web server that contained a program that the web server executed. In both of these attacks, the firewalls in front of the web servers sent the data right through.

The reason the firewalls did nothing to prevent the hacks is because the firewall is designed to pass "allowed" data straight through without alteration.

The hackers simply acted like any normal web user, and the only thing the hacker did was communicate extra information to the web server beyond its expectations.

Buffer overflow is not limited to Windows web servers. Recently a flaw in the PHP scripting language was discovered to allow a buffer overflow attack to occur. (PHP is most commonly used by Apache servers running on Linux and UNIX.) The estimated number of servers running PHP is 8.4 million with 1.0 million web sites actually using PHP content. All of the 1.0 million web sites with PHP content are vulnerable to this attack, and any firewall used in front of these web servers is designed to pass the attack on to the web site.

Failure to Protect Servers is Nothing New

The failure of a firewall to protect the web server is nothing new. Firewalls have failed to protect several other network servers, the most notable of which is the e-mail server. If someone has an e-mail server behind a firewall, then the firewall must be configured to grant users access to the e-mail server from the Internet. When a virus is sent in an e-mail message, the firewall is designed to pass the virus on to the e-mail server "as is" and without alteration. The end user receives the e-mail message with the virus, opens it and then infects their machine, and it is the firewall that allowed that virus enter the company in the first place.

False Sense of Security

Many network administrators believe that when they have a firewall in place, they have security.

Just as the firewall grants an e-mail virus creator access to the e-mail server to transfer the illicit content, the firewall also grants access to the web server for a hacker to carry out a hack. However, when a web site is hacked, most people look at the firewall as a means of barring all destructive access to their web server. A firewall does not have the capability to determine if the content on your web server is good content or bad content, it only sees it as content, regardless if you posted it or if a hacker posted it.

Firewalls only look at connections, not at the intent of the users attempting to connect or at the content the users may bring into a network environment. As long as firewalls contain openings for users to access resources, a hacker will continually have a method of gaining access and altering web servers - including web site content.

The Lockstep Solution

In conclusion, firewalls are designed to provide only a limited amount of security, and any company with a web server needs to implement additional measures to protect the web site content on that server. A complete web site security solution should include a firewall, a routine installation of web server software updates, and an automated response to a breach in firewall security as it occurs.

1. **Install a firewall**
   Installing a firewall is an excellent first step, but additional measures must be added to create a total web site security solution.
2. **Install software updates**
   Install software updates and patches to web servers, but keep in mind that patches are "after the fact". The whole reason the patch was created is in response to a vulnerability that has already been exploited, and hackers find these vulnerabilities faster than the patches are created.
3. **Have an automated response to detect and repair corrupted web site content**
   The best solution is to have a plan in place that will allow you to automatically and quickly recover after a hacker changes your web site.

Take the steps needed to complete your web site security solution and install WebAgain to automatically protect your web site content from corruption.

LOCKSTEP®