The
**Broadcasters' Desktop Resource**
www.theBDR.net
... edited by Barry Mishkind – the Eclectic Engineer

# Doing IT Right

## Securing Gear On The Internet
## Part 2 – Why Firewalls Are the Answer

***By Bill Putney***

*[March 2017] The Internet is very convenient for program transmission as well as data. Still, there are potential potholes to avoid. Installing a proper firewall is essential to avoid bad guys getting into your system. Bill Putney continues the discussion on how to do this without spending thousands of dollars.*

In our first part of this discussion, we saw why many stations that think they have a firewall really do not, and noted the issues as to why a proper firewall is needed.

This time, we will show you how to build a firewall that will protect your station and its programs from bad guys and their hacks. The best part is it might be cheaper than the router you had thought was protecting your facility.

**HOW ATTACKS ORIGINATE**

To understand why a good firewall is necessary, it is helpful to understand how computer attacks arrive at your "door."

There are a couple general categories of network attacks.

For example, well-known in the public press are the Denial Of Service (DOS) attacks, the goal of which is just to stop any useful transfer of data or information to or from a site – in other words, to stall your system. Nothing can really stop a DOS attack on the public Internet. It does not have to even be an attack on you, it could be a general attack on some other service on the part of the Internet your data will be traveling on.

These attacks are usually of such a scale that your ISP will be working on isolating the offending sites from their network. Often the sites that do the damage in a DOS are ones where that site's computers have been taken over by an evildoer and used as proxies to attack other sites. Usually in such an attack, known as a Distributed Denial of Server (DDOS) attack, many zombie computers at many sites have been taken over to create an overwhelming attack.

Then there are actual network intrusions where, instead of merely swamping the victim, the attacker wants to take over control of devices on the target network to accomplish theft, modification or destruction of data, or turn the net-

work's devices against a third party sites. Protecting against this sort of attack is a little more complex and generally left to the site's administrators. That means the IT guys or if you are a small station, the broadcast engineer who gets to fix anything that does not have to do with sales or on air programming.

The recent attacks against some broadcasters that resulted in the stations broadcasting unauthorized program material can be generally thought of as an intrusion attack.

**DO NOT LEAVE YOUR DOOR OPEN**

Just before we launch off into the nuts and bolts of how to protect our networks, it is important to say that we want to be as sure as we can that the users on these networks do not invite the bad guys in.

Most broadcast gear is purpose-built stuff and, in general, does not lend itself to having a user bring malicious software to it.

That said, general purpose computers used for email and web browsing can be a real threat and should be protected using active anti-virus/anti-malware software. For the station owned computers this is easy to accomplish. For users that bring their own laptops and attach them to the station's networks such a policy is a little harder to enforce.

Certainly asking people to use a similar kind of protection software is the very least that should be done. It is a good start, but there is a long way to go yet.

**NETWORK TYPES**

If we think structurally, there are three classes of networks.

First the "Trusted" networks like Local Area Networks (LAN's) where we expect all the people and devices to be trustworthy and safe.
Second, are the "Untrusted" networks; where it is safest to assume that they are all out to get us. This is the public Internet and, in general, gets lumped into Wide Area Networks (WAN's) – Wi-Fi hot spots, for example, where experts caution users to be, well, very cautious.

The last class of network we will touch on are De-Militarized Zones (DMZ's). DMZ's are the networks where you need to risk public access but with a recognition that devices there might become compromised and cannot be fully trusted. These would include things like web and streaming servers or drop boxes for program contributors.

Usually DMZ's either have what we want to create or an iron clad way of connecting two "Trusted Networks," such as the LAN network at a transmitter site and the LAN network at a control point (which we will call the studio as a shorthand) together using the "Untrusted" Internet. We do not want to do this on a device-by-device basis because it quickly becomes cumbersome and, as we have discussed previously, security in most broadcast devices is superficial.

What we can do is make sure that your program material and your control commands – and only yours – make it to the transmitter site. We need to do this in a way that insures security. Not just a password but real cryptology.

**A RECOMMENDED FIREWALL**

At its core, a firewall is *a software application that prevents anything from coming into your server unless you ask for it* – sort of like the faucets on your sinks.

A firewall I have used for many things over the last 10 years or so is *pfSense*, an actively supported, Public Domain Open Source project.

Contrary to what you might think, having open source software as a security device is a good thing. No one could possibly hire enough people to spend the kind of time and attention one of these programs get.

Best of all, the program does not depend on secrecy to provide protection.
All of the protection necessary comes from well thought out and executed programming and, since everyone can look at it, anyone can find the holes in it, which gets them fixed in a hurry.

**COMMIT TO UPDATES**

Since this is security software you can expect that there will be frequent updates – and you do need to stay up with them.

These updates can be installed automatically but they may not come at the exact time you want your connections to be disrupted.

I tend to set my updates for "manual" mode and check in once a day. The good thing is that I run the same firewall software everywhere so when I see an update is available I know it is time to update it everywhere – I do not have to check at every site, every day.

**– AND UNIX**

*pfSense* runs as a program on the dread Unix operating system.

Now, hold on a second! In this case it is a very cut down version of Berkley Unix that has only the features needed to run the firewall software.

The idea is to keep the amount of software that needs to be tested for security as small as possible. Even a lot of consumer security devices use Unix (Linux or other variants) as a basis for firewalls because it has proven to be stable and trustworthy when pared down to its basics.

Therefore, most people never know they have a Unix based firewall and, once you get over the idea that it exists, there is almost never a reason to know it is Unix.

**BUILDING A REASONABLE FIREWALL**

First, let us put all your worry aside right away. *pfSense* comes as a complete package that you install on a common "PC."

Even better, the hardware requirements are very modest. I would say all you need is a computer with at least a 64-bit dual core 2 GHz Intel/ AMD processor or better, 2 to 4 GB of memory, a 20 GB or larger hard drive, two or more Ethernet ports, a garden variety video display port, and a few USB ports.

Often, I tell people we use "junk" computers for firewalls but what I mean is that we use computers that have outlived their usefulness in other applications.

**NO NEED FOR CUTTING EDGE GEAR**

In general, a firewall is an important device in the infrastructure, so you do not want it to be a maintenance headache, but it does not need to be blazing fast unless it is going to be doing a lot of simultaneous cryptographic sessions.



That said, if you are planning to do a lot of Virtual Private Network (VPN) links using a IP/SEC, which depends heavily on crypto-

graphy, you may well want to have a faster CPU and more cores or a card supported by *PFSense* that specifically does cryptography. We have never needed that here but you might, depending upon your circumstances.

At the same time, there is nothing wrong with buying a new computer for your firewall. But if you are cash-strapped like we are, we repurpose things a lot. What we will do is to replace the moving parts (fans and rotating disk drives) in an older computer. Usually, this is a lot less than buying a new computer for the purpose.

An outside source of used gear is eBay, where we have bought some really powerful firewall hardware that in its prime sold in the $20K ballpark. Those often are really just rack-mounted PCs with software but mostly the software licenses have expired or are not transferable. The hardware is usually first rate though.

One note of caution: sometimes these computers can be reloaded with *pfSense*. Other times, it can be nearly impossible to install new software on proprietary firewall hardware, so it is worth checking – it is a game left to those with a lot of time on their hands to attempt.

## IT REALLY IS SIMPLE

Again, for those of you worried about plunging into UNIX, *pfSense* comes as an all-in-one package.

You can download the file package from the *pfSense*.org website or one of their official mirror sites. Before getting the file, you will need to select the type of media you are going to boot from (CD or USB Drive).

Once you get the software file you need to "burn it" to the boot medium. How you make a bootable media is left to you, and it is dependent on the system you use to make it, but there is lots of info for that on the web.

You will only need a keyboard, mouse and display for the software installation. Once *pfSense* is installed, all of the configuration, management, and monitoring can be done with about any web browser on a computer on your LAN, so you do not have to learn UNIX at all to run it.

## A QUICK LOOK AT CONFIGURATION

While there are a lot of options for some of the configuration items, the defaults are designed to be the safest ones. (see below).

A simple shell menu allows for the setting of basic preferences.

When you are done, you can easily see how the firewall is configured with the browser. No obfuscation by programmer-ese configuration files with line after line of undecipherable yet critical instructions.

In use, the system can be controlled by a GUI that will work in any modern browser, like Firefox or Chrome. A "dashboard" rapidly display the status and key data of the system.


**pfSense Web Configurator**

Depending upon your particular situation, you may need/want to have a separate firewall at the transmitter site. Setup will be just as simple.

As noted, *pfSense* is open source, essentially free software that will run on virtually any computer you have handy. With a minimum of

muss and fuss, you will ensure that outsiders will not compromise your station's LAN and connected equipment – and you will never hear profane hip-hop instead of your programming.

- - -

*Bill Putney is the Chief Engineer for KPTZ, Port Townsend, WA. You can contact Bill at: billp@wwpc.com*

- - -

**After installation and interface assignment, pfSense has the following default configuration:**

- WAN is configured as an IPv4 DHCP client
- WAN is configured as an IPv6 DHCP client and will request a prefix delegation
- LAN is configured with a static IPv4 address of *192.168.1.1/24*
- LAN is configured to use a delegated IPv6 address/prefix obtained by WAN (Track IPv6) if one is available
- All incoming connections to WAN are *blocked*
- All outgoing connections from LAN are *allowed*
- NAT is performed on IPv4 traffic leaving WAN from the LAN subnet
- The firewall will act as an IPv4 DHCP Server
- The firewall will act as an IPv6 DHCPv6 Server if a prefix delegation was obtained on WAN, and also enables SLAAC
- The DNS Resolver is enabled so the firewall can accept and respond to DNS queries
- SSH is disabled.
- WebGUI is running on port *443* using *HTTPS*
- Default credentials are set to a username of *admin* with password *pfsense*

- - -

Would you like to know when other great ideas like this one are published?
It takes just 30 seconds to sign up – right here - for the one-time-a-week BDR Newsletter.

- - -

***Return to The BDR Menu***