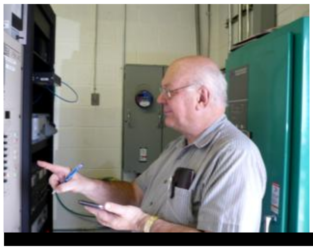


The

Broadcasters' Desktop Resource

www.theBDR.net ... edited by Barry Mishkind – the Eclectic Engineer

Bits and Bytes

Intrusion Prevention 101: Get Thee a Router

By Steve Lewis

[February 2013] The Feb 11th launching of a Zombie Alert through CAP/EAS boxes at six radio and television stations brings digital security to the fore. How secure are your stations' computer systems?

After the rash of unauthorized access to EAS boxes that occurred this past week, it seems like a fitting time to review basic network security.

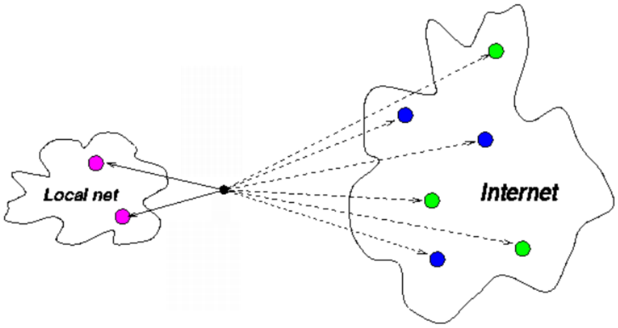
Of course, the situation at each station – or business - is different. Especially at large clusters or chain stations, network security may be in the hands of a highly competent IT Department. Or it might be left to a part-time contract engineer to handle.

This particular article is targeted at smaller stations that operate without a highly-trained IT staff at its disposal, nor the money required for exotic pieces of new IT gear.

IN HERE AND OUT THERE

A network is any collection of computers which can talk to one another.

The Internet is the world's largest *external* network for this purpose. The dozen to a few hundred computers at your station most likely belong to their own *internal* – or Local Area Network (LAN) – so the station staff can share documents and print, among other things.



The Internet brings the whole world together

Connecting these networks safely, so your company's computers, data, and operations are secure, is the goal.

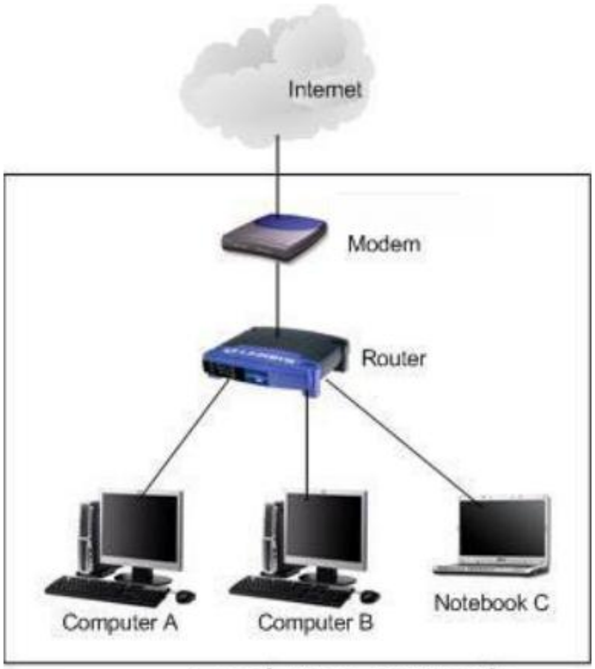
KEEP THE OUTSIDE OUTSIDE

Most of us know that the Internet, while really cool, is a dangerous place.

If you did not already know this, take my word for it. The problem is that there are people with nothing better to do than to try to be destructive in one way or another.

You absolutely must take careful measures to keep these people out of your internal network.

One of the simplest ways to keep the bad guys out is an inexpensive router/firewall available at places as convenient as Walmart for well under $100. What these devices do is to take the single Internet address assigned to you by your Internet service provider and translate it to your internal network addressing scheme.



Local Area Network

This is called Network Address Translation (NAT), and it is this process that isolates your internal network from the external Internet. For example, if your Internet address is 65.92.15.78 NAT will translate this address to, something like 192.168.1.xxx, where xxx is a number that represents each internal computer's address, such as 192.168.1.67.

LOCKOUT

Any attack by a nefarious criminal has to be made to your external address but, in most cases, the attack cannot traverse the NAT translation to reach your internal network because there is no easy way to attack a specific computer without a path to its internal address.

The effect is very simple: The address translation makes the computers on the internal network invisible.

The effect is magic, really. If your internal computer wishes to communicate to an address on the external network – perhaps a website – the NAT sees the request, remembers what computer on the inside made the request, translates the address of the request to that of the external internet address, and sends the request off to the website.

When the data returns from the website, the NAT translates it back to the internal address and your computer views the website page that it requested.

This behavior is pretty much the default behaveior on all cheap routers. There are usually additional configuration options which modify the default behavior for special cases. These options are not required for maximum protection.

DECONSTRUCTING THE ZOMBIE ALERT

Let us take a moment and examine the Zombie Attack debacle.

The key aspects of the situation were formed by:

- Amazingly, EAS boxes sitting out, unprotected, on a network with an address that was available directly to the Internet. This is, of course, bad.
- Worse yet, the EAS boxes were still configured with the default password left unchanged.

To me, this appears to have been a crime of opportunity. It is no different than if you left for work in the morning with your front door wide open.

Now, just what do you think will happen?

Digital Alert Systems
Digital Alert Systems DASDEC™-II
http://www.digitalalertsystems.com

DO NOT BE FOOLISH

An EAS box – or any important gear – should never be allowed to be exposed directly to the Internet.

As we have seen, if the stations just used a simple NAT router/firewall, the perpetrators would have not had access to the EAS boxes in the first place. Furthermore, as demonstrated by some other stations, where the intruders did manage to enter the LAN, the bad guys were stopped in their tracks by a password that replaced the default.

While the NAT in a sub-$100 router is not completely foolproof, the unchanged password was an open invitation to intruders wanting to create havoc.

SETTING UP YOUR ROUTER/FIREWALL

A word or two of caution is in order regarding the configuration of any router being used for NAT and firewall protection.

These are general purpose devices that support a variety of configurations to satisfy as many different users' needs as are practical in a small, inexpensive device. For instance, most incoming connections from the external network are refused, but a feature called "port forwarding" actually enables communications to pass *into the LAN* from outside.

Normally, this is enabled on an IP-by-IP address and port-by-port basis. But you also can see how some these settings will defeat the NAT technology if misapplied.

Another caution: although usually not enabled by default, most NAT routers allow remote administration. Be sure and turn this off or you soon will allow outside hackers to reconfigure the router, possibly defeating all the security it once provided.

Similarly, while it may seem tempting to allow wireless access to your network, doing so will require another set of configurations to be set and adjusted carefully to provide the necessary security you seek. If the router has Wi-Fi enabled by default, you should disable it. And please do not forget to set the router's administrative password to something other than the default (which is, incredibly, often set to "password" by the manufacturer). If the router allows you to set the administrative account name, change that as well.

A HEAVIER DUTY FIREWALL

Some companies will prefer a more sophisticated software and/or hardware firewall – but that takes solid IT people to operate properly, and is more or less beyond the scope of this article.

Specially designed firewalls are a good addition to any front line protection setup. Nevertheless, a truly secure firewall can easily become costly and require experienced technicians to configure and maintain. The proper way to deal with the issue is to do a cost/benefit analysis, taking into account the value of the information contained within your network, your mission critical applications like the program automation, the embarrassment of having aired a fake EAS alert, and other factors.

Simply put: an NAT will generally fend off the casual hacker while a firewall (configured correctly) will generally keep every criminal out.

Doing nothing is not an alternative.

- - -

*Steve Lewis has experience in computer programming, IT, and broadcast engineering. Contact Steve at:*steve@theengineeringbureau.com

- - -

Return to The BDR Menu