

## Eye of the Storm

**Hurricane**  
LABS, LLC.

### IN THIS ISSUE

#### How Technology Saved My Life

#### \*buntu as a Desktop OS - Or the Start of a Friendly "Distro War"

#### Not Good Networks - Answers

#### n00b notes

## How Technology Saved My Life

By: Bill Mathews

*Editor's Note: This originally appeared on my personal blog. Despite the fact that it's not directly security related, I hope it reminds us that though our jobs are to secure information, we have to let good technology shine.*

I'm not one given to fits of emotional fancy or professing my gratitude for things in an overly dramatic way, but here I go. First, let me give you some background. For the last few years I've suffered from a couple of wrenching and debilitating diseases and we don't need to go any further about what they are. Let's just say they make it very difficult to lead a "normal" life. Yeah I know, wah wah poor me, but this story isn't about how sick I am. It's about how technology has let me lead a fairly productive life despite my health issues.

Now 90% of the time I am able to go into the office and work away with no problems. However when I have an episode, it usually keeps me at home for an extended period - this week has been one of them. In no particular order, here's a list of the technology I use to keep my work going even when my body isn't.

**The Blackberry:**<sup>1</sup> I suspect it's pretty obvious why this is on the list. I can make my doctor appointments, get prescriptions, lay in bed when necessary, still keep up with my daily email routines, and answer any questions, tickets, etc that need immediate attention. My loyalty to the Blackberry is being challenged though by the Apple iPhone<sup>2</sup> especially since the new Blackberries have lost their scroll wheel. Very upsetting.

**Asterisk<sup>3</sup> and various add-ons:** Recently we added softphones (basically a software phone) to our Asterisk system, which extends my desk phone to my home office via VPN. Basically without call forwarding, I can take/make calls abstaining from any extra effort or

running up the cell phone minutes - truly a great technology.

**Instant Messaging(IM):**<sup>4</sup> We use instant messaging religiously for our internal communications. Most of the guys sit right next to each other and use IM to talk back and forth. It's great when you're on a call and need some advice. It provides almost instant escalation when needed. We use an internal Jabber server for our IM stuff so we can do TLS encryption for privacy and control - who can and cannot be on the service. Given the nature of what we do, it's pretty important. More relevant to this list, it allows me to be "there" even when I'm not.

**Virtual Machines:** Vmware<sup>5</sup>, Xen<sup>6</sup> (being bought by Citrix might change my attitude towards them), and the rest. This technology allows me to quickly build up servers and test out new ideas quickly and efficiently. More importantly, I can do this without tons of hardware that I have to interchange and climb around the floors to wire up. We were late to this game I admit, but it really has changed the way we think about things. Off topic for this list, but to save money, power, and space all of our failover systems will run on VMWare virtual machines.

**Email, Websites, VPNs, etc:** These "old" technologies enable the remote aspect of business. You can send email from pretty much anywhere and VPNs allow you to do that in a private (and if done properly) authenticated environment. Both technologies have been around for many moons and really need no further description.

These are the so-called disruptive technologies that have saved my life. They have enabled me to start and run a company in spite of my physical limitations and prosper at doing so. The moral, I hope, is that technology isn't always "bad" or "scary." If used properly, it can be powerful and life altering. That's why I love technology and my job.

1: <http://www.rim.com/>

2: <http://www.apple.com/>

3: <http://www.asterisk.org/>

4: <http://www.jabber.org/>

5: <http://www.vmware.com/>

6: <http://www.citrixserver.com/>

## \*buntu as a Desktop OS Or, the Start of a Friendly "Distro War"

By: Steve McMaster

There are countless flavors of Linux out there called "distributions" or "distros". Popular examples are Red Hat Enterprise Linux (including the community supported edition, Fedora, and the rebranded edition of RHEL, CentOS), SuSE Linux Enterprise, Ubuntu, Debian, and Mandriva. Each distribution is run by people with different sets of ideas about what makes a distribution good. Debian, for example, is known for trying to be stable while sacrificing the bleeding-edge of software. Red Hat is known for its Enterprise-level support. Ubuntu is known for its large community base and more current software. There are also distributions targeted at niche situations. For example, DamnSmallLinux is a distribution that runs from a Mini-CD and is designed to run on very old hardware without a huge performance hit.

When it comes to running Linux on a server, your choice of distribution is not always your own. Sometimes (or even quite often), the software you want to use requires a specific distribution or comes as a prepackaged distro all its own. Red Hat or a variant is quite commonly used for this, such as with VMware's ESX platform. However, when choosing a distribution for your desktop, the choice is almost always your own. I'd be hard pressed to think of a situation where it's not your own, except in perhaps a corporate environment. My choice in this case is Kubuntu and now I'm going to tell you why.

Ubuntu comes in three official versions itself - the standard version, Ubuntu, which uses the GNOME desktop environment; Kubuntu, a version using the K Desktop Environment "KDE"; and Xubuntu, a version using the lightweight XFCE. I have used all three, and my personal favorite (this is where the "Distro War" comes into play) is Kubuntu.

Out of all of the desktop Linux distros I have used, the \*buntu distros come with the most usable vanilla installation. A default installation comes with all of the tools you'll need to get started using it right away. First off, it comes with the popular Mozilla Firefox web browser for browsing to all of your favorite websites. It also comes with the OpenOffice.org office suite, which is fully compatible with the Microsoft Office file formats, including the new Office 2007 formats. For those dull and quiet moments at work, each flavor of Ubuntu comes with its own audio and video players, and there are decoders available for any media format you can think of, although they are not included by default. Lastly, Ubuntu saves you time upon your first boot by including most, if not all, of the drivers you'll need to make your hardware work.

Speaking of drivers, Ubuntu takes a very middle-of-the-road stance on so-called "non-free"<sup>7</sup> drivers (mostly on drivers for

7: non-free (adj): software that may or may not be "free as in beer" (requires no payment), but is never "free as in freedom" (you are not free to use it however you wish). This is usually software that you can't modify or redistribute.

video cards and wireless network adapters). By default, open source video drivers will be installed and you will be told that proprietary drivers are available. If you need drivers to use a wireless card, and there are no open source drivers available, these will be enabled automatically. However, if you choose not to use them, they can be disabled through a friendly interface. A very important difference between \*buntu and other Linux distros is it allows you to choose whether you want to enable this extra functionality at the cost of using proprietary software, instead of making the choice for you.

Ubuntu tries to keep its packages up to date, without risking stability by running bleeding-edge, unstable, untested software. Packages are how you install software in Ubuntu and other Debian-based distros - they are generally standard and easy to maintain and update. Within a day or two of a security vulnerability being discovered, it is fixed and available for an update in the Ubuntu repositories.

There are dozens of reasons why so many people (including half of our office) choose an Ubuntu-based distribution to run on their desktop (or laptop - Ubuntu runs great on laptops, too!). If you'd like to try one of the Ubuntu-based distros, you can download CD images for free at their respective websites:

Ubuntu (GNOME): <http://www.ubuntu.com/>

Kubuntu (KDE): <http://www.kubuntu.org/>

Xubuntu (XFCE): <http://www.xubuntu.org/>

## Not Good Networks - The Answers

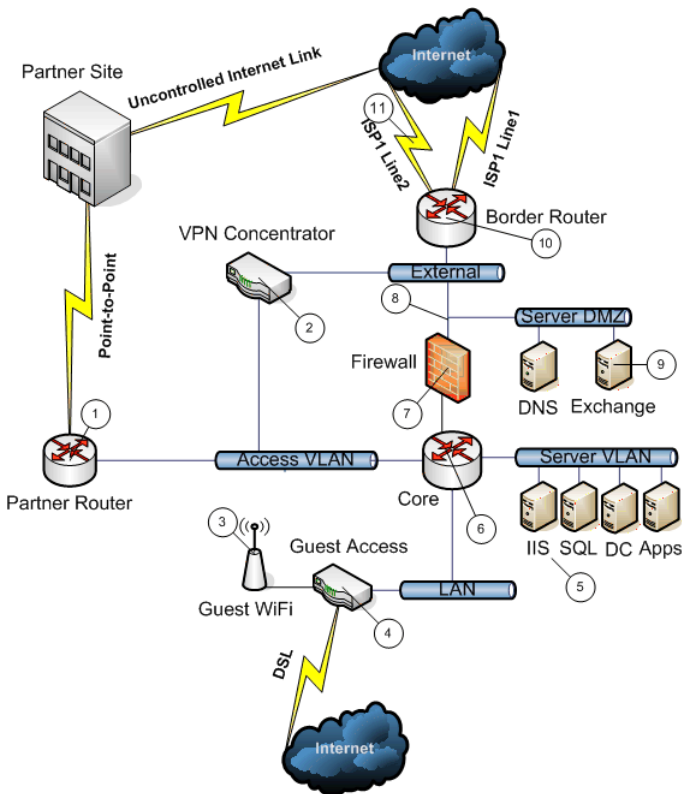
By: Nick Stockhaus

I would like to thank those of you who participated in the "Not Good Networks" contest we had last month. This month I have attached the topology which identifies the problem-spots that I had designed, as well as an updated version of a more correct network design. Congratulations to Ray Pesek from Third Federal Savings and Loan for taking the prize! Thanks again for playing.

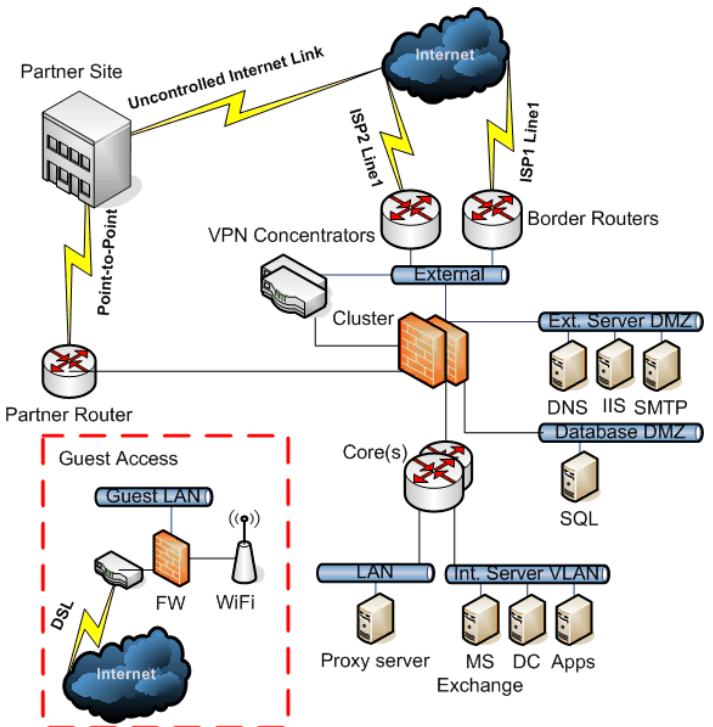
1) **The partner router:** This has bad news written all over it and MUST be separated from everything else by the firewall. We assume that the router and everything behind it is hostile, no matter what.

2) **VPN Concentrator:** Dumping VPN clients directly onto the LAN is just begging for trouble. Sure it might make accessing Exchange easier (if it weren't in a fake DMZ anyhow), but there is absolutely no control over the users. Any remote user should be considered hostile and contaminated, since you have little control over it.

Not Good Networks - The Answers: Continued from Page 2



Bad Network - Explained



Corrected Version

3) **Guest WiFi:** While that is very kind to offer wireless access to your guests, this should not be touching your LAN. Routing it though the firewall could be OK, if in its own DMZ, but best practice would be to have it completely isolated.

4) **Guest Internet:** The same as above, I would isolate this completely. It could also make a great way to test things externally (for your IT support), just make sure that your LAN users cannot accidentally bridge the gap with a laptop!

5) **Two servers - ISS and SQL:** The points to note here are that IIS is accessed by the outside world, which means it should not live near other internal application servers or near the LAN. Put it in a DMZ specifically for externally accessed servers. The SQL server, being used in conjunction with the ISS server, should not live on the same segment as the web server itself. The best practice is to run the database server on its own DMZ to control access via the firewall.

6) **Redundancy in your core routing/switching infrastructure:** When everything else in the path to the Internet is redundant, the core becomes a fine place for catastrophic failure. EVERYTHING touches the core...remember that.

7) **Redundancy of the firewalls:** Running a cluster will help to assure uptime along with seamless failover. It will also help to keep downtime at a minimum during upgrades.

8) **“DMZ” placement:** Let me say that we are not big fans of anything sitting outside of the firewall. Unless it is a router of sorts that will not allow traffic to bypass the firewall in any way, it belongs behind the firewall. This “DMZ” is not being properly protected, and even if the servers are running firewalls they should still have that extra layer of stateful inspection. You pay for it so use it!

9) **Email infrastructure:** Bottom line is that an Exchange server has little business being on the outside of a firewall, and arguably even at the border in a DMZ. The pictured setup allows external access directly to the server, relies on only that server for spam/virus filtering, and requires users on the LAN to access a server in a hostile environment. It just screams “BAD”! The best method for this is to setup an SMTP relay in a true DMZ, that is protected by the firewall, and sit the exchange box on the internal Server VLAN.

10) **Redundancy of the border routers:** With proper ISP redundancy and a firewall cluster (assuming redundant switching as well), using a single router will be your ultimate point of failure. In an environment where downtime is not easy to obtain, how are you ever going to run your IOS upgrades?

11) **ISP Redundancy:** Having two lines is great, but if they are both coming from ISP1 and something happens to them (routing issues, circuit failure, “scheduled” upgrades...) then your redundant routers and firewall cluster start to seem less than helpful.

## n00b notes

By: Matt Yonchak

**Hurricane**  
LABS, LLC.

Before you go any further, read the article at this URL:

<http://tech.msn.com/howto/articlewsj.aspx?cp-documentid=5983122&icid=tg5983122&GT1=10840>

In case you don't have Internet handy the article is entitled "10 Things Your IT Department Won't Tell You." It was written by someone at the Wall Street Journal with the help of several "experts" and posted on msn.com. The article basically gives you ways of getting around your company's security policies to do whatever you want while on your computer at work. I'm not sure where to begin describing the issues I see with this article.

I won't start ranting about how ridiculous it is that Microsoft put this article on their site or how I find some of the opinions offered by their security experts laughable. What I do find funny are the ways they say you can do these things without getting caught. For example, I think three of the tricks listed would be seen by a properly placed IDS and then blocked using a good firewall with application based protections (Check Point). You don't even need to spend money on the IDS - Snort has rules for web-based IM clients, web proxies, and Google docs. This should encourage you to use all the tools at your disposal to do your job. A wise man once told me there really isn't any excuse for having to say "I didn't know". The last thing any of us want is to have our boss at our desk asking how sensitive data was lost because someone was using Google docs. I don't know about your boss, but if that happened to me, saying "I didn't know it was going on" wouldn't fly with mine. Trust me none us want that happening to me, especially me.

My other major issue with the article is the hypocrisy shown by Microsoft. They claim to be helping your business run smoother/more efficiently with their software. Then they turn around and allow an article to be put on their site telling your employees how to waste company time. Heck, next they should write an article about why you should have your Windows firewall disabled all the time or how it's a good idea to put unpatched servers on the bare Internet; both of which they preach against. Time to teach what you preach, guys.

Now I don't claim to be smarter than the people involved in writing the article, but I think a little common sense would go a long way in deciding what to write their article about. Maybe I'm old school, but if you put out a product that companies depend so heavily on, you have a \*wait for it\* RESPONSIBILITY to those customers and writing an article like this is just irresponsible. I'm sure some of you (and you know who you are) think I'm hating on Microsoft because I dislike using their OS and that's not the reason. It was just truly surprising to me that I would see this on their site. It's not like this article is the end of IT security as we know it or anything. Just see it as a friendly reminder from everyone at Microsoft to watch your back because they're certainly not doing it for you.

### Upcoming Events and Training

**March 14:** Check Point User Group of Pittsburgh Meeting, Radison Hotel - Green Tree, Pittsburgh, PA.

**March 25-27:** Check Point Essentials Class, Hurricane Labs, Independence, OH.

Register for these events at [www.hurricanelabs.com](http://www.hurricanelabs.com)