InterPath Financial Institution: Network Security Implementation

By Allan Feid

4/30/2008

Table of Contents

Executive Summary

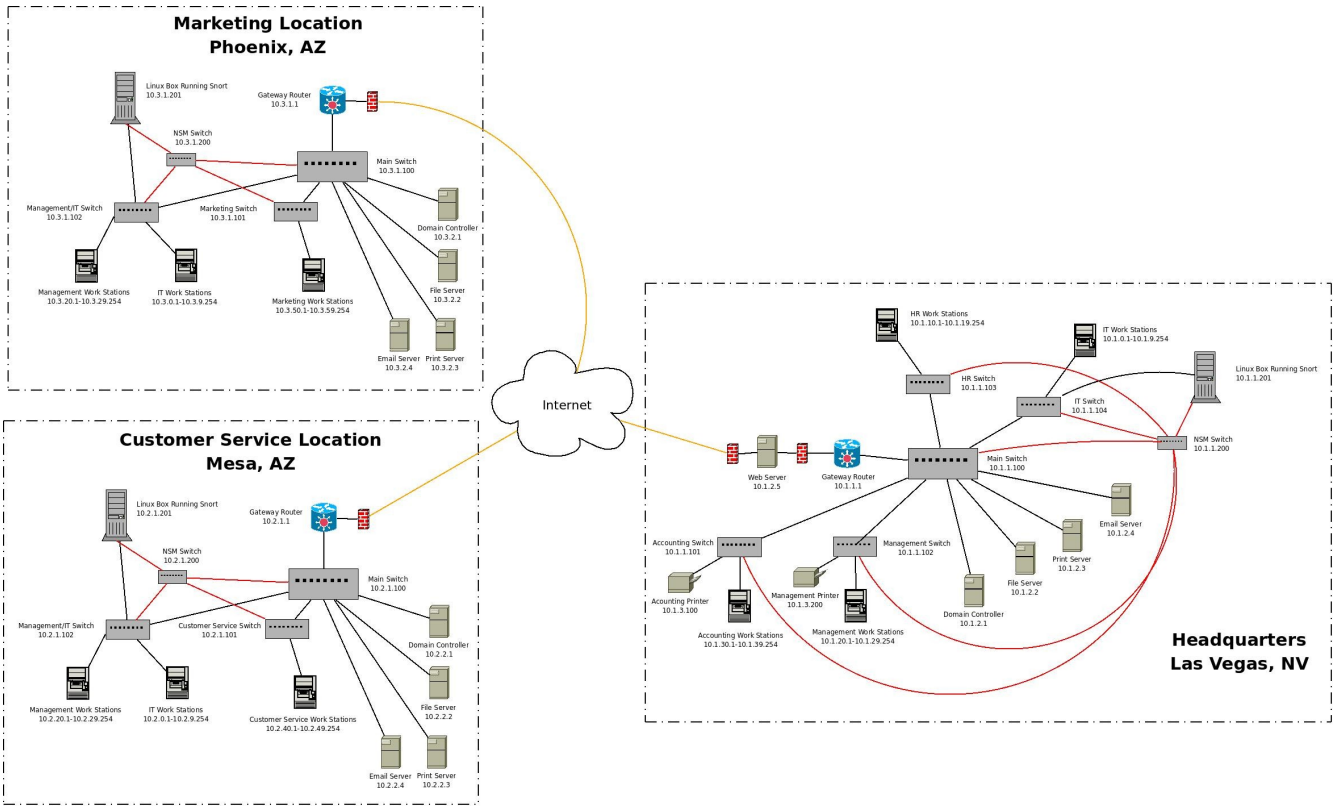
This document was created to outline a new network infrastructure for InterPath Financial Institution. There are technical diagrams of what the network will look like, and various security measures we want to take to ensure proper security for our customers' data. This document also contains information about why we should spend the money to implement the plan.

On April 11th, 2008 InterPath Financial Institution (IFI) was broken into by hackers. They breached into our main headquarters where we maintain all of our customers personal information. We are unsure of what they took, changed, or if they still have access to our computer systems. We have informed all of our customers who's data was stored at the main headquarters. We have about 25,000 customers 15,000 of which are stored at our main headquarters. This is unacceptable and we don't know the damage that's been done. We're currently searching the network for recently modified files and blasting the computers with a fresh install of Windows XP.

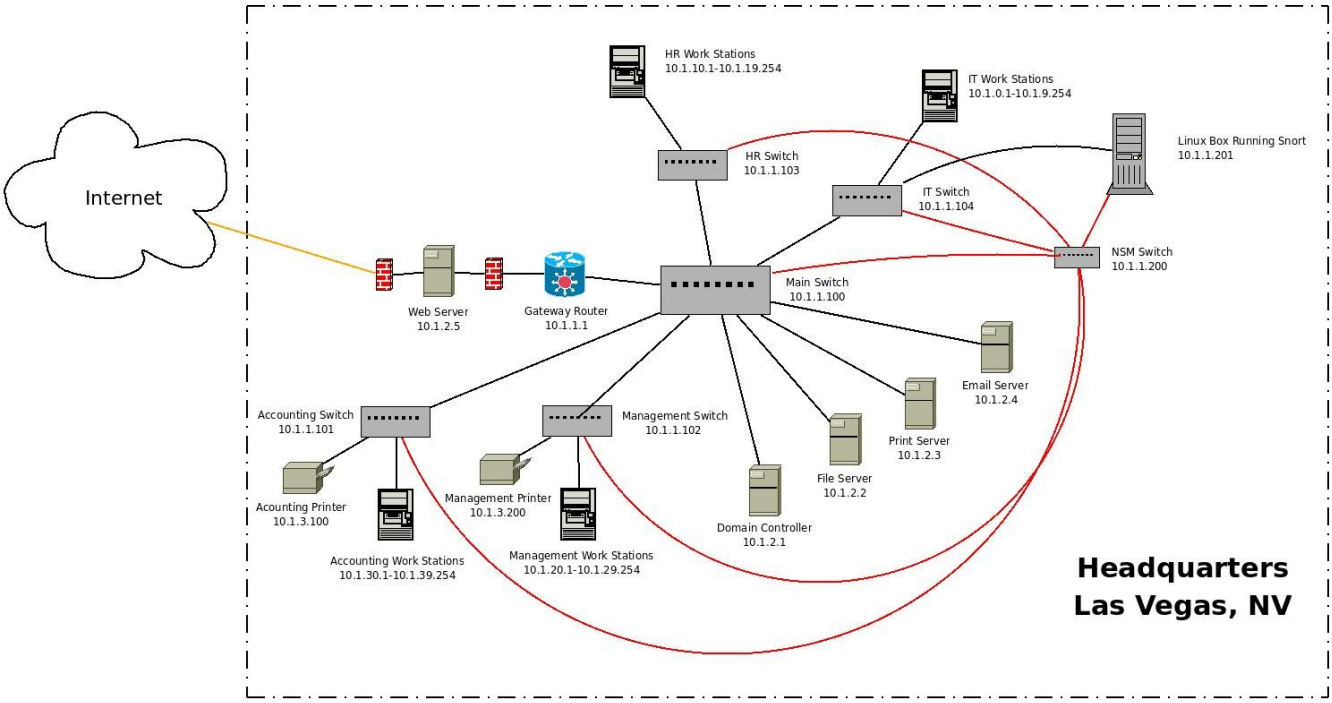
It has come to my attention, that the network does not have any Intrusion Detection Systems (IDS) in place nor does it have means of monitoring the entire network. With such a large company, in three different locations, I'm not sure why we haven't implemented either of these yet. Without these, keeping track of what is happening on our network becomes a very difficult task. We have somewhere around 1,000 hosts connected to the network. We need to implement a security monitoring system and intrusion detection system in order to prevent attacks like this from happening in the furture.

The New Infrastructure

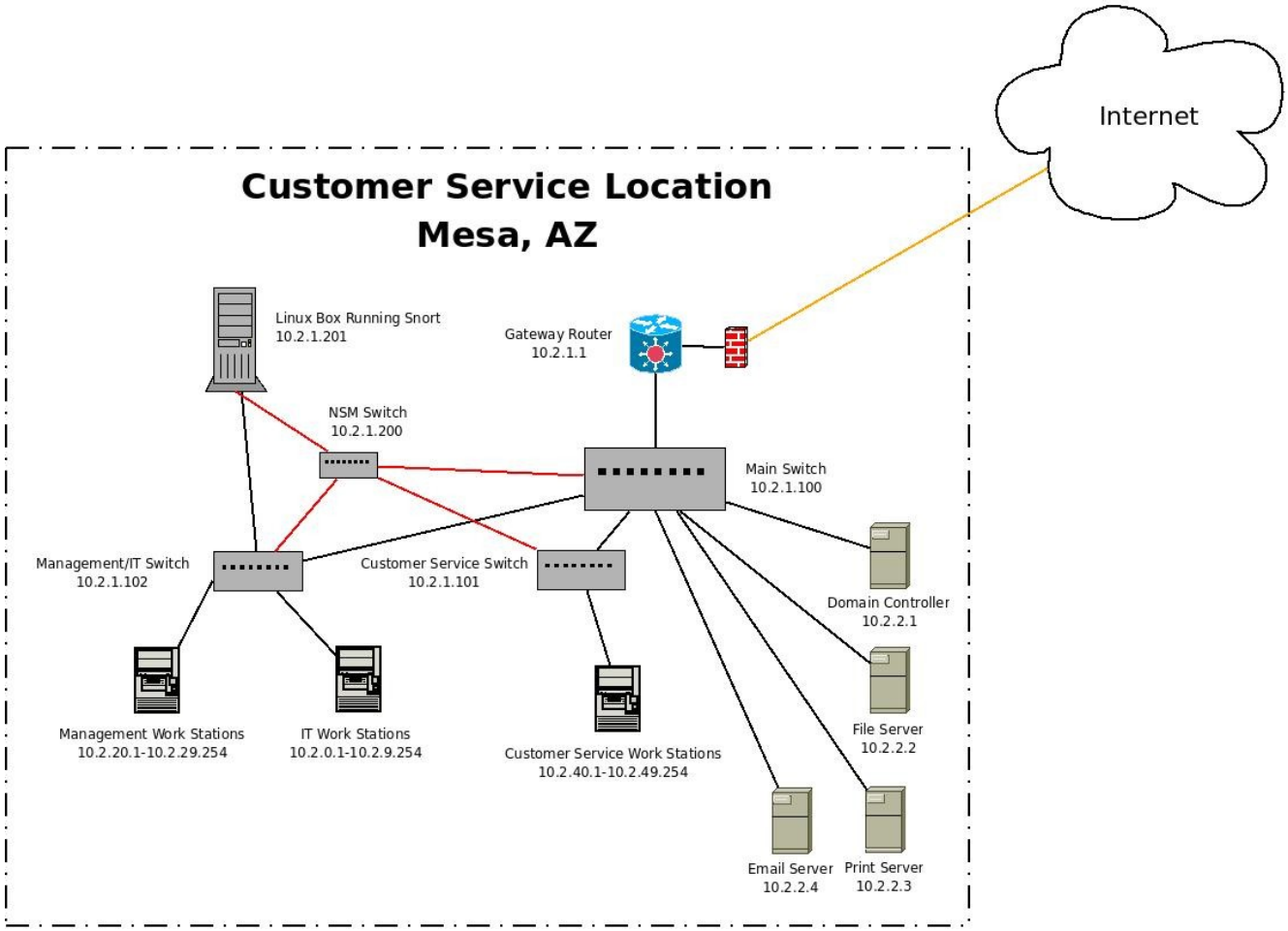
Over the passed week, I've been working on a new infrastructure for our network. This new infrastructure will include a one-way network designed to replicate all traffic on our network through an IDS. Here's an overview of the design I've come up with:



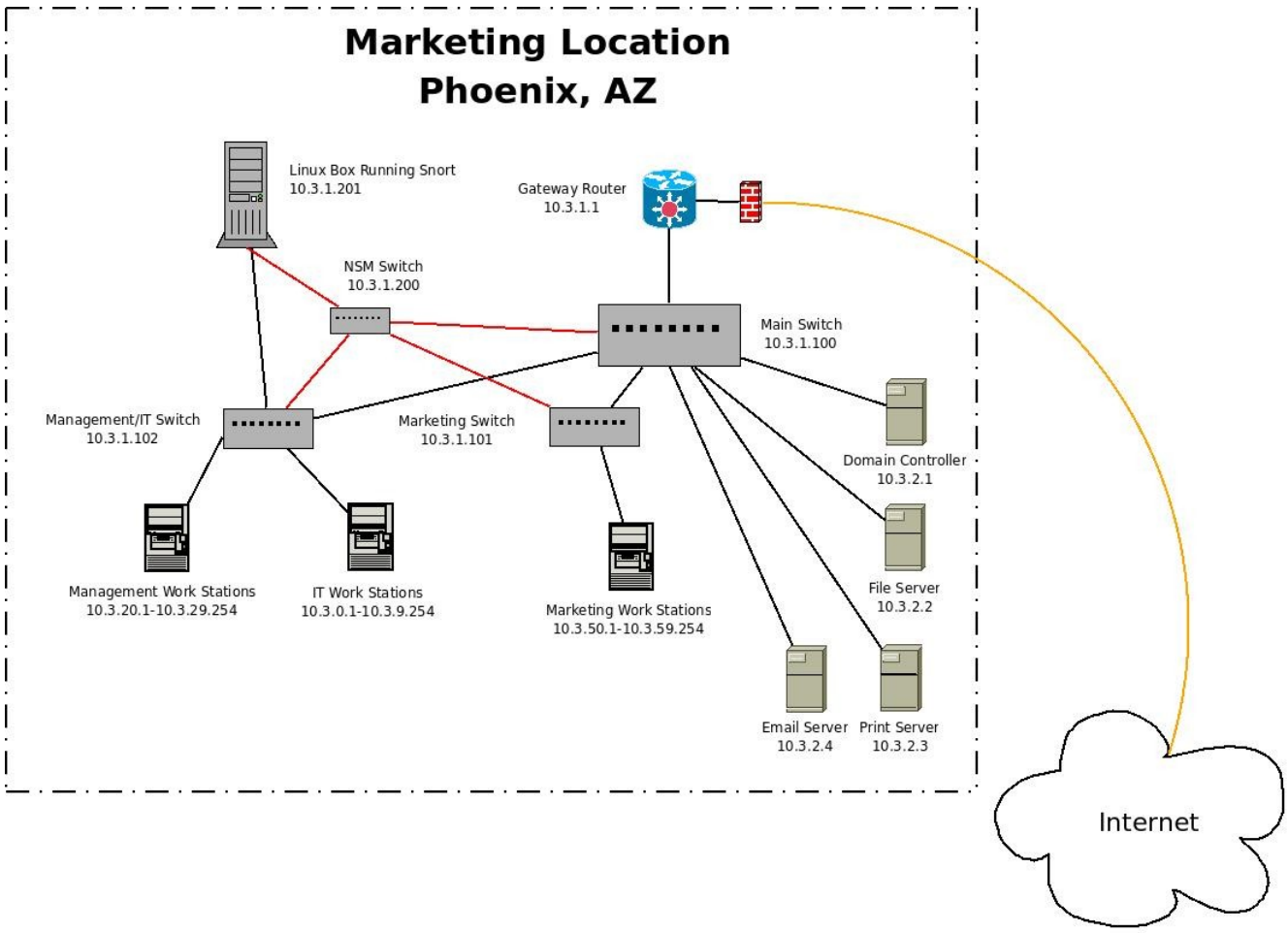
Main Headquarters, Las Vegas, NV



Customer Service Call Center, Mesa, AZ



Marketing Center, Phoenix, AZ



IP Scheme

In the new design, as you can see we will be using a TCP/IPv4 environment. To make management of the network easier on the administrators, I've come up with an IP scheme that will be easy to identify various different servers, workstations, switches, printers, and location based on the IP address of the various hosts. In the new network layout, we will be using a 16-bit subnet mask (255.255.0.0) and the Class A private addresses (10.x.x.x). We will use the second octet to determine the location of a host. In the above diagrams, 1 will be used for our headquarters, 2 for the call center, and 3 for our marketing location. The third octet will determine what type of host it is inside of the location. The IT department will use 0-9 for their workstations, HR will use 10-19, management will be

on 20-29, accounting will use 30-39, customer service representatives will be using 40-49, and our marketing team will use 50-59. All routers, servers, printers, and switches will be included in the IT department range of 0-9. Routers and switches will be using 1, servers will use 2, and printers will use 3. Routers and switches will be distinguishable by the fourth octet. All routers will use everything under 100, and switches will be over 100.

With this setup in use, we will quickly and easily be able to determine where traffic is coming and going to without trying to track down what IP addresses belong to which computers. The old system was not very organized and IT always had trouble figuring out what computers were having issues by IP address. This was a huge priority for me when redesigning our network so all of us in IT will know what IP addresses should be going to which departments and devices.

Workstation Security

Turn off unnecessary services

To harden our host workstations, we first want to disable any unnecessary services. After looking at one of our current workstations, we have way to many services turned on that are not needed. The following services will be turned off on our systems once we blast out fresh installs to every workstation:

- Alerter
  - used to send administrative alerts to computers
- Application Layer Gateway Service
  - used to allow third-party plug-ins for Internet Connection Sharing
- ClipBook
  - used for sharing your clip book with remote computers
- Error Reporting Service
  - used for sending error reports to Microsoft when something crashes or goes wrong
- Help and Support
  - lets users see help and support on a local machine, not necessary on our machines

- Internet Connection Firewall (ICF) / Internet Connection Sharing (ICS)
  - we will have our own firewall software, and hardware routers
- Messenger
  - used to send messages to remote computers using the net send command
- System Restore Service
  - used to make restore points, this is not useful at all in our environment, and personally I've never used system restore successfully
- Themes
  - used to enable various graphic effects for the end users' desktop

These services are all completely useless in our network environment, and the more services running the better chance of an exploit being available on that machine. By turning these off, the machines will run faster and be less exploitable. Through the use of GPOs, we will make sure that only the services required to run on our network will be enabled and nothing more.

Internet Access

Certain user groups may need more access than others, but when it comes to an internet connection we will disable internet access from our customer service representatives. They will only need access to local Intranet web pages to check various things about a customers account. There's no need for them to have internet access. The other departments will be granted internet access, but through a central proxy server that will filter out inappropriate content defined by our management department. We will not allow access to any instant messaging protocols that send information through the internet, instead we will use email and Network Communicator. This will keep all chatter on our local network and avoid the possibility of company information being sniffed from the internet.

Anti-Virus

I've done a lot of research on which anti-virus suite to use on our systems. After doing some research I have found that the most popular anti-virus programs do not work 80% of the time (Kotadia,

2006). Virus programmers are getting smarter and have found ways to completely disable the popular scanners or work around them. With this knowledge, I've found a lesser known lightweight scanner called NOD32. I've been using it on my own machine for some time now and it works amazingly fast, and takes almost no resources. The interface is not all bloated and filled with “pretty colors” like the popular scanners like. Yes, it may be less user friendly, but we're worried about protecting our systems and the IT department will be trained on how to use the scanner efficiently and effectively. The version they have for small to medium sized businesses is called ESET Smart Security. With this version, we can install to both client and server machines and set up a local mirror server that will save us bandwidth from having all clients access the internet to update virus definitions.

Intrusion Detection / Prevention

Since our new network design had network monitoring in mind when being created, we have a system setup that allows all traffic on our network to go through a single Linux machine at each location. Each switch will be setup to with a monitoring port that all traffic will be replicated to. The monitoring port will then be connected to another switch setup with a monitoring port. Finally, from that second monitoring port we will have a Linux machine setup to read all information on the network. The way it's setup, all traffic will hit the second switch, which I call our Network Security Monitoring switch (or NSM switch), and then on the monitoring port will be pushing out all the traffic from that locations network. The Linux machine will have two network cards, one connected to the NSM switch and the other will be connected into the regular network to provide alerts to administrators. The NSM switch won't be accessible from anywhere but the Linux machine, and these boxes will be running Snort to provide us with a solid IDS and IPS.

The Linux machine, will be running a lightweight *nix distro and have a good sized hard drive and a SQL database. The database will house all of our network traffic and give us a good place to start in case of another attack. Since Snort by itself doesn't have a very user friendly interface, we will use

the Sguil, which is an add-on that provides a nice GUI to look at everything. Snort can be setup to send email alerts, and that is something we will definitely be using. We will setup an email account specifically for alerts from Snort. Most of our IT guys have blackberries or other phones that can receive email, so we want to make sure they have access to this account from where ever they may be. It is important to know what is happening on the network at all times, and this will give them a heads up and ability to respond to an attack before it's been complete. Attacks take very little time these days, so keeping up with Snort alerts is a must.

ARPwatch

To give us that extra bit of protection, we want to use ARPwatch on our networks. This will also be installed on the Linux machine and it too will send out email alerts. What this program does is monitor all ARP packets and notify you if someone is trying to poison your networks ARP cache. This will help prevent attacks from the inside, and if an attacker has managed to get passed our security, then this will notify us as soon as they try to ARP poison our network in order to sniff traffic.

Firewall Settings

We will be using hardware based firewalls for all of our main traffic. For starters, none of our local programs use UDP connections, so we will block all incoming UDP packets. The only TCP ports we need to leave open are for VPN access from our IT staff and certain managers that require the ability to access network resources from home. For our VPN access, we will be using IPSec through L2TP on port 50 and 51. This will leave the least amount of ports open on our network and still allow IT to VPN in and then use RDP to administer our servers.

The DMZ

For our web server, we will use a software based firewall. The firewall we have chosen is Sygate. This is a nice firewall that gives pretty advanced features. Since this server will need web

access, we will leave port 80 open and this server will maintain it's on VPN access. There will be no way to access this server from the local network so we must VPN in to make any changes to the web server. We want to keep the public stuff completely separate from our private network. To ensure this, we will have router rules in place to drop all packets to and from the web server trying to get into the local network.

Why do we need all this security?

Upgrading and redesigning our network layout will most certainly be costly. The reason we need to maintain this much security is to ensure the privacy of our customers. If our customers data can easily be obtained by determined hackers, for one we won't be a very reputable financial institution and it's just irresponsible on our part that we did get breached and still have no idea what was taken.

The money spent on security, is definitely worth it in our case. We want to uphold our reputation as a company that provides our customers with peace of mind that their private data will not be taken and given to others. In today's age, computer security is becoming more and more of a household word. If we do not have any security in place, we will surely be attacked time and time again and our customers will leave us for other companies that do not have these security issues.

The information we maintain on our network is very important to customers. We have all of our customers social security numbers, bank account information, how much money is in the account, passwords, users names, street addresses, phone numbers, and insurance information just to name a few things. Attackers are looking to steal this kind of information to sell. A hacker can sell someone's identity for about $20 a person. With our 25,000 customers, that's easily $50,000 worth of information on our network. To secure $50,000 worth of information, we should be ready to spend the same amount, but in this case we certainly won't need that much. A lot of our security monitoring software mentioned here is open source and freely available this will save us a ton of money. The actual hardware used to run this software can be older machines that we will be replacing, once again saving

us money. The real expense is our anti-virus program. That will roughly cost us $3,000 to have a license for each machine on our network. The only other expense would be the time needed to upgrade and redesign the network.

The redesign can take place over a 6 month period where we will test and configure everything while making this switch as transparent as possible to employees doing their job. Employees, however, will notice more restrictions on what they can do and will probably need meetings to explain why we're taking away their privileges. This won't effect their ability to do their job, but instead just restrict the things they can do on the computers.

Once this new infrastructure and security measures are in place, there won't be much more cost to maintain the network and this will, again, ensure our customers privacy and keep their business with us. All we have to do once the infrastructure is up, is maintain the network as usual. We will monitor firewall logs closely along with our Snort system to make sure everything is working the way it should. To sum it all up, our current security measures are almost non-existent. We have some anti-virus and firewalls, but without an IDS we will almost never find out when attack has occurred with such a large network. Our customer's data should be important to us, so why not spend the money to keep them safe.

Resources

Anonymous, (2008, April 30). University Of Massachusetts Amherst's health services network breached by hackers. Retrieved April 30, 2008, from Cyber Insecure Web site: http://cyberinsecure.com/university-of-massachusetts-amhersts-health-services-network-breached-by-hackers/

Kotadia, Munir (2006, July 6). Why popular antivirus apps 'do not work'. Retrieved April 30, 2008, from ZDNet Australia Web site: http://www.zdnet.com.au/blogs/securifythis/soa/Why-popular-antivirus-apps-do-not-work-/0,139033343,139264249,00.htm

Cheswick, W, Bellovin, S, & Rubin, A (2007). *Firewalls and internet security second edition*. Boston: Addison-Wesley.