

## Re: [fw-wiz] Defense in Depth to the Desktop

**Source:** <http://www.derkeiler.com/Mailing-Lists/Firewall-Wizards/2004-12/0117.html>

---

**From:** Paul D. Robertson (*paul\_at\_compuwar.net*)

**Date:** 12/13/04

To: Chris Pugrud <cpugrud@yahoo.com>

Date: Mon, 13 Dec 2004 16:30:23 -0500 (EST)

On Mon, 13 Dec 2004, Chris Pugrud wrote:

> > *This*  
> > > *is the classic "eggshell" weakness of network security, hard and crunchy on*  
> > *the*  
> > > *outside, soft and chewy on the inside. The Strong Internal Network Defense*  
> >  
> > *I don't think I'd use eggshell to denote hard ;)*  
> >  
> *But I would. It's relatively hard compared to what's inside, but, as you note*  
> *above, it's not actively reinforced, tested, or updated, so it's probably*  
> *pretty weak on an absolute scale. I recently performed an assessment for a*  
> *customer that began with them bragging about how tight their firewall ruleset*  
> *was. After the assessment I complimented the "tightness" of the ruleset but*  
> *noted that all of their "DMZ" servers were dual-homed. One interface on the*  
> *Internet, one on the inside, completely bypassing the firewall.*

I'm dealing with one of those right now too, severely over-done hardware, over-complex network and multi-homed everything (Windows boxes too, WINS doesn't like that!)

> > *I've only ever seen internal firewalls implemented at extremely large*  
> > *organizations. Making it a routed network helps some with the MS stuff,*  
> > *but it's so uncommon to see internal routing in small companies who don't*  
> > *have the admin resources to not be totally killed by a big malware event.*  
> >  
> *I prefer to work with organizations in the 100-300 size. They usually have*  
> *limited internal routing and some decent hardware (depending on position in*  
> *Hype/Budget/Funding scale). I was just searching for something that is a bit*  
> *easier to explain and apply to the people that write the checks and is more*  
> *effective than sacrificing rubber chickens at dawn (err, I mean nifty do*  
> *buzzword compliant gimmick of the week).*  
>

Sure, but I really guess I'm not seeing this as a solution for a firewall more than it's a solution for an internal network architecture...

## Firewall-Wizards: Re: [fw-wiz] Defense in Depth to the Desktop

> > *Unless, for instance your administrators are remote, and they need to have*  
> > *access to the client's registry from a server they remote into...*  
>  
> *There are accomodations for this scenario when you get to the analysis. I on;y*  
> *presented the 2 cell compartment model for illustrative purposes. I guess you*  
> *still get what you pay for.*

Indeed, I've just been doing some consulting at some small sized companies recently and all the stuff that I'd never do on a network I designed seem to be in place and common (\*sigh\*.)

> > > *In addition to the firewall, the client systems are fully isolated from*  
> > *each*  
> > > *other by layer 2 controls (private vlans). The servers may be similarly*  
> > > *isolated, but doing so is minimally effective and damaging to server to*  
> > *server*  
> > > *communications.*  
> >  
> > *Why not just turn off automatic ARP on the clients and statically ARP them*  
> > *to the router? (Hmmm, can you do that in Windows?)*  
> >  
> > *You can do something "security" usefull in Windows? It is much easier, direct,*  
> > *and simple to do it in the switch where I can do it once and I know it will*  
> > *continue to work as programmed despite MS patch o' the day.*

But configuration things, especially those which fit in a .reg file that can go into a login profile are much more likely to be adopted than "buy another firewall" things, no?

> > > *Consider the introduction of a zero day worm virus [\*2] into such a network*  
> > *by*  
> > > *an infected client. The client can attack all of the servers, and all of*  
> > *the*  
> > > *servers may become infected. The infected client can not attack any of the*  
> > > *other clients because of the layer 2 isolation. The infected servers can*  
> > *not*  
> > > *attack any of the clients because of the firewall. The end result is that*  
> > *one*  
> > > *client and the servers, a small subset of the organization, are infected.*  
> > *This*  
> > > *is much less devastating, and much easier to clean up, than if the entire*  
> > > *network was infected.*  
> >  
> > *Not if the worm is especially destructive, infect the servers and you've*  
> > *killed the business if the critical business resources are on the servers.*  
> >  
> > *Sure, the business is down, but only the servers have to be cleaned up, not X*  
> > *thousand client systems. I've seen (ok, heard it) it happen too many times*  
> > *where organizations had to send the entire workforce home so they could*  
> > *methodically work through the building disinfecting and patching every single*  
> > *end user system in the entire organization. I'd much rather have limited*

## Firewall-Wizards: Re: [fw-wiz] Defense in Depth to the Desktop

> *functionality and only have to clean up 20-120 servers.*

Again, if the data's on the server, and the data's at risk, I'd rather not see it happen.

>  
> > > [\*2] *The infamous "zero day worm virus" is invoked as a worse case analysis because it invalidates anti-virus and patch defense mechanisms. Since worms are increasingly targeting necessary network ports, personal firewalls are also equally invalidated as a defense mechanism. Marcus can gleefully dance on their graves.*  
> >  
> > *I'm not sure this assumption carries fully- personal firewalls generally allow per-process outbound traffic blessing- so the worm would have to hook a service that's allowed to communication outbound- while that's been done, it's certainly still true that personal firewalls are useful in limiting the damage from most "downloaded and clicked" stuff, which is where a good chunk of the risk exists. The rest of the risk is the laptop that just walked in hibernated and infected, and the VPN user- heck, quarantining the laptops for 90 mins when they first come in would probably do about as well as anything...*  
>  
> *How many hundred times a day is a user going to "click" to access the organizational file server, email server, and porn (err proxy) server before they just enable some dangerously broad default allows? I recognize some value for personal firewalls, but I think that using personal firewalls, especially on deskbound organizational systems, puts us on the wrong side the tail chasing treadmill. You are talking about a lot of money and management and application management and helpdesk headaches that could be much more easily and cheaply and sanely managed at the core router/firewall/rubber chicken substitute.*

Hmm, the user can't enable it in the "enterprise" versions, it's a company or group-wide policy thing. I'm not sure it's a lot of support costs, and given the amount of spyware and Trojans I've found recently- I'd say it's almost a necessity. Firewalls don't stop this stuff without content inspection and knowing what's bad- or disabling active content, and these days, that's a difficult to win battle :(

PFWs seem to me to be a pretty good stop-gap. The ability to get back some control over the desktop is worth its weight in gold- losing that ground is what made the war swing against us!

> > > *Analysis*  
> > >  
> > > *The primary design of the model is to focus security resources on the servers.*  
> > > *No organization can reasonably maintain strict control over client systems, but they do have absolute control over making sure that servers are currently*

## Firewall-Wizards: Re: [fw-wiz] Defense in Depth to the Desktop

- > >
- > > *Were it that easy– I've seen plenty of "we can't update that server*
- > > *because \$critical application will fail."*
- >
- > *Sure, that a risk that's easier to accept, to know that one system will be*
- > *vulnerable and you can focus your energy on getting that one system updated and*
- > *protected. That's a bit more difficult to do if your attention is "focused" on*
- > *a few thousand desktops in various states of patch/AV/user disfigurement.*

You're still going to have to deal with the desktops, because the users are going to have to work and have critical files there. I think that I'm probably more worried about spyware Trojans than worms right now– worm events get lots of press, but the infestations are really ugly.

- > > *You could probably get about the same level of protection by assigning /32*
- > > *addresses to the clients and only giving them a route to the router– no*
- > > *need to tax the switches with newfangled–VPN–foo at all. You still get*
- > > *some broadcast stuff, and you don't want gratuitous ARP on, but I bet*
- > > *it'd have about the same effect. You could then add interface routes to*
- > > *the local host for those you wanted to interconnect at the local admin*
- > > *level.*
- >
- > *Because this newfangled–VPN–foo (well, it's only a few years old (supported in*
- > *Cisco switches at a minimum)) does that much easier and less messily than*
- > *hyper–subnetting (/30 clients with router) or anything else I've seen. I'm in*
- > *process of prepping a post about layer 2 isolation (aka private vlans) that*
- > *does a much better job of articulating their virtues and uses than my previous*
- > *attempt.*

But then you've got a single point of failure, and just using a 255.255.255.255 subnet mask and a static route seems to be not that messy to me. Plus it works no matter what vendor's gear you happen to hit– that's always a bonus to me because the "switch just went down and we need to put in whatever we can" scenario with little sleep needs to not carry a bunch of administrative overhead.

- > > > *Application protocols that are broken are peer to peer systems and any kind*
- > > > *of*
- > > > *desktop file sharing. This is strongly viewed as a good thing in most*
- > > > *organizations. If I was an attacker going after juicy data the first place*
- > > > *I*
- > >
- > > *Shared stuff is becoming popular inside, like Netmeeting– I'm not sure*
- > > *this is a good long–term strategy (I'm not sure it's not a great one too.)*
- >
- > *Better to just cut it off at the knees before the lusers get used to it.*
- > *Seriously. The only way I maintain my sanity is the regular howls of laughter*
- > *administered by user "requests" to do some thing assinine that is clearly not*
- > *an actual business objective. Now when legitimized (not necessarily*
- > *legitimate) business objectives elicit howls it is clearly time to polish the*
- > *resume.*

Firewall-Wizards: Re: [fw-wiz] Defense in Depth to the Desktop

My normal perspective is exactly that, but it's way different when you're going in somewhere that's already wrapped around it as process.

Paul

---

Paul D. Robertson "My statements in this message are personal opinions paul@compuwar.net which may have no basis whatsoever in fact."

---

firewall-wizards mailing list  
firewall-wizards@honor.icsalabs.com  
<http://honor.icsalabs.com/mailman/listinfo/firewall-wizards>