

## Re: Draft I: Selling Internet Whitelisting

**Source:**

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2004-11/6792.html>

---

**From:** Les Connor [SBS Community Member] (*les.connor\_at\_DEL.cfive.ca*)

**Date:** 11/28/04

Date: Sun, 28 Nov 2004 00:10:53 -0600

Hmmm.

I think this approach might have it's place, but perhaps not in any small business that relies on entrepreneurial instincts to thrive. It's too heavy handed and stifling for my liking, and in fact I'd suggest that a company that censors their employees view of the world in this way is going down fast.

--

Les Connor [SBS Community Member]

-----  
SBS Rocks !

"Andrew M. Saucchi, Jr." <spam-only@2000computer.com> wrote in message news:OjvZ%23MP1EHA.3452@TK2MSFTNGP14.phx.gbl...

As promised. The title is a bit pompous, but it was the first one that came to mind.

Internet Whitelisting: Salvation for the Business Owner

Prepared by 2000 Computer Solutions, Inc.

Until now, most businesses have allowed employees full access to Internet, simply because it was never given a thought. The Internet company activated the connection, the network consultant plugged the network hub or switch into the Internet connection, everyone shouted, "Hooray! Down with dial-up!" and everyone was online. The time has come to rethink this attitude, and in this document we will attempt to explain why your company should adopt a locked-down Internet policy.

We now have several years' experience with the policy of open Internet access. It has been more of a failure than a success. Employees with unlimited Internet access are faced with a bewildering barrage of temptations, succumbing to any of which can cause their computers to become damaged. Looking at a seemingly harmless web site can allow the workstation to become infiltrated with programs designed to convert the workstation into an advertising kiosk. Eventually, the workstation becomes unusable, and we need to spend considerable time attempting to remove the offending programs, usually at considerable expense to the client.

Even experienced professionals sometimes have trouble differentiating between a legitimate web site and a dangerous threat, and your employees-- lacking the skill required to make what sometimes is a difficult call-- most likely will get caught in some sort of trap sooner or later. Scam operators can make a fake bank site that looks identical to a real bank's site in an attempt to steal user ID's and passwords-- simply by downloading the graphics from the real site!

Some employees develop bad work habits as a result of having unlimited access-- spending the day looking at pornography, shopping sites, or offshore casino gambling sites. We know-- we've reviewed the logs on the

servers that had that feature. The logs record every web site access. It often isn't a pretty sight.

The vast majority of web sites have nothing to do with your employees' work. Given the risk, allowing unrestricted access to Internet is not well-advised. The workstation should be seen as a tool for completing work-related tasks, not an entertainment device. How many of you have a TV set in the office for your employees' use? If someone even attempted to bring one from home, you'd probably ask politely but firmly that it be removed at once. Unlimited Internet falls in the same category.

Fortunately, work-related tasks can usually be isolated to a fairly short list of sites. What is even more fortunate is that we can sell you a tool that will allow employees to access the sites they need to get their work done while blocking the rest. It's called ISA Server, and if you have Small Business Server installed, you may even have this tool running on your server already! All you need to do is make us a list of sites you need and allow us to reconfigure ISA Server not to allow unlimited access.

Every employee can have his own "whitelist" of approved sites. One employee may need access to your bank's web site for wire transfers. Another employee may need to access the IRS site to download tax forms or instructions. Some employees may need no access at all. The rare, trustworthy employee may need full access (though we would recommend against it). You get to decide; you remain in control; you help us to maintain control over your network and keep it running smoothly. Going back to the bank example we used earlier, we may see an employee fooled by a fake bank site, but ISA Server won't be. If the fake site is not on the employee's whitelist, ISA won't allow access to it-- possibly preventing the loss of large amounts of money from your bank accounts.

One objection might be, "Well, if I find an employee goofing off like that, I'll simply fire him or discipline him." You may well want to do that, and it's not unreasonable-- but by then, the damage may be done. Preventing the damage-- which could involve workstation or network downtime and substantial repair costs-- is far preferable to repairing it.

Another objection might be, "Why not use a blacklist instead?" We've tried that in some cases, but even the most brilliant network consultant cannot compile a list of even 5% of dangerous web sites. At best, we can review the logs and block objectionable sites found in the logs, but again, this is reaction rather than prevention. By then, the damage could be done, and someone determined to goof off will simply find new sites.

By now you should be convinced that Internet is a very powerful tool-- but like all power tools, one that needs to have suitable safety features to prevent it from backfiring. Start preparing your whitelists today and get on the road to relatively safe Internet access.