

## Re: Blocking IM servers

**Source:** <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2002-12/0672.html>

---

**From:** NeoSadist ([neos@dist](mailto:neos@dist))

**Date:** 12/07/02

From: "NeoSadist" <neos@dist>  
Date: Sat, 7 Dec 2002 04:44:52 -0700

"Apu - N" <[Nahasapeemapetilon@simpsons.net](mailto:Nahasapeemapetilon@simpsons.net)> wrote in message  
news:BbaI9.3052\$Vf3.35394@vixen.cso.uiuc.edu...

> Hi,  
> This is for a project of mine. We want to block all IM using the  
> firewall. Where can I get a list of IP addresses or server names of the  
> major IM services? I googled around for a bit and did not come up with  
> anything relevant. Any help would be appreciated.  
> Thanks  
> /A  
>

You can contact the program maker, or better yet, download and install them yourself.

However, here's a general "out of the box" configuration that certain IM programs I've used wanted. Remember, this is assuming you want to use port restrictions to control these applications. There's a better way to do this, so keep reading.

### MSN MESSENGER:

Login is over msnp (1863), http (80) and https (443). For voice and download, it needs tcp and udp over all the dynamic ports (1024-65535). However, it can be configured to use "blind" proxy, i.e. specifying http proxy in its config for connections, yet specifying no proxy address. If someone does that, there will be almost no way to stop it from logging in unless you find what the web address it uses to log in is. I use blind proxy behind my linksys firewall router so that it doesn't want the other ports.

### ICQ:

Login is usually 5190 I think, but it can be configured to use just about anything for that, and its online help suggests using https (443) to login if the default port can't be used.

It can also be told to "connect behind firewall", and also proxy, which are both separate options. Also, its "listening" ports are defaulted to all dynamic ports (1024-65535, udp i think), but that also can be configured manually.

## comp.security.firewalls: Re: Blocking IM servers

Like MSN Messenger, it can be configured to use "blind" http proxy, see above for details.

Yahoo

I think this application is NOT able to use blind proxy. I also think that it logs in using one of the many aol ports. I don't remember, however. It does have a "I'm behind a firewall" option, but no configuration beyond that for that option. It's been a while since I've used it, so it's best to try to get help for yahoo messenger as if you're trying to ask them how to configure your firewall to allow it, then when they tell you what it uses, block that.

I don't know anything about AIM, other than it will probably want to use one of the aol ports.

### THE BETTER WAY:

A better way to configure things to restrict this in a work LAN environment is to put a restriction on all users not to be able to install software (except of course the administrators). This is possible using win2k pro, and even win9x (see [www.regedit.com](http://www.regedit.com) for win9x). Then, once they can't install anything, go and uninstall all traces of the messenger programs. That's the easier way to do it, I think, rather than modifying the firewall (although the firewall is probably not strict enough if they can connect, unless it's the "blind http proxy" method, which you can't restrict port 80 anyways if you're going to use the web). On win9x, you can also, using the registry, restrict what program names they can run, and then you could restrict these programs:

setup.exe (virtually all installers use that filename)  
msmsgs.exe (msn messenger)  
yim.exe (yahoo's exe, I think...)  
icq.com / icq.exe (for icq, I think it's .com)  
aim.exe / aim.com (aol instant messenger, i think)  
regedit.exe (so they can't hack back into their registry hive and disable what you've done)

By the way, if you're referring to windows popup messenger, which is part of the operating system, please reply to newsgroup and specify this, since it's totally different.