

Re: Blocking sites fails

Source: <http://www.tech-archive.net/Archive/ISA/microsoft.public.isaserver/2004-10/0195.html>

From: Dana Brash (dbrash_at_Phongsaly.com)

Date: 10/13/04

Date: Wed, 13 Oct 2004 19:14:16 +0800

So I set it up in my lab here, as close to your config as I could duplicate.

I have a hardware firewall, and behind that my LAN. I installed ISA in Single NIC mode on my file server, created a mess of rules (cool that you can do that) just like I would on a regular firewall.

Then, with my client in place, trusty FWClient running, I started messing with URL deny's.

When a URL is denied in the rules, I get a deny just like with the firewall configuration, FW Client on OR off.

BUT, when I remove the proxy information from my connection settings, I can get right past it.

SO, back to Chris' original question "Why is this?". Actually, it makes perfect sense as my hardware firewall is my default gateway and now I'm only checking with it. My packets do not look at the proxy server, go to the proxy server, and much less ask the proxy server for permissions. They go directly to the default gateway and out, just as I've configured them to.

What to do about this, then....

I would recommend setting a nice solid GPO that both sets the Proxy Settings and disables the user access to it.

Places to play:

Computer Configuration > Administrative Templates > Windows Components > Internet Explorer > Make proxy settings per-machine (rather than per-user)

User Configuration > Windows Settings > Connection > All

User Configuration > Administrative Templates > Windows Components > Internet Explorer > Disable changing proxy settings

"-Karl" <dinodod@gmail.com> wrote in message
news:1096853664.629221.126780@k26g2000oda.googlegroups.com...
>I am using the Single NIC method. I am in the beginning phases of

microsoft.public.isaserver: Re: Blocking sites fails

- > *deploying it and am having plenty of success and horror at the same*
- > *time.*
- >
- > *I am able to deploy it using SMS with no problems. NT4 boxes are a*
- > *pain when merging the registry settings as there is no way to disable*
- > *the popup box when the settings get merged. At least the users don't*
- > *know what it is. I am not able to repoint everyone to the ISA server*
- > *as the gateway at this time as we are not ready to move everyone over.*
- > *What advantage does that have over leaving the current settings intact*
- > *other than what yo mentioned above?*
- >
- > *Our company has a nice default policy that restricts the users from*
- > *accessing anything or modifying anything on their PC so we don't have*
- > *to worry about the curious people causing havoc on the systems (Thank*
- > *god for GPOs!)*
- >
- > *My horror issues with ISA have to do with external sites and port 443*
- > *ssl tunnel as per the logs. Seems I am having a devil of a time trying*
- > *to make a rule to allow access to some secured web sites. I work for a*
- > *hospital and most of the sites are secured sites. Right now, I have to*
- > *put those sites on the exception list until I am able to properly*
- > *configure ISA to allow access to these sites. Users are complaining*
- > *that the sites are slow and I am getting tons of failed connections in*
- > *the logs. I am trying to follow -->*
- > *<http://www.microsoft.com/technet/prodtechnol/isa/2004/plan/publishingwebservers.mspx>*
- >
- > *but I am still unable to configure the proper rule to allow my INT*
- > *clients access to the sites. I disabled Connection Limits and even*
- > *went on my ISA server and installed the certificate from the secured*
- > *servers. Maybe you know a little about how to configure ISA for*
- > *secured web site access? One of the sites in question is:*
- > *<https://www.avmed.com/providers/>*
- >
- >
- > *I also have a citrix server that I am working on but that is another*
- > *issue.*
- >
- >
- > *So that's my configuration and story.*
- > *-Karl*
- >