

## Re: Deny rules...

**Source:** <http://www.tech-archive.net/Archive/ISA/microsoft.public.isa/2004-04/0350.html>

---

**From:** Tony Su (*anonymous\_at\_discussions.microsoft.com*)

**Date:** 04/10/04

Date: Sat, 10 Apr 2004 10:30:04 -0700

Jim has a very good point which is why for a Financial services client I have not implemented it.

And, the situation he describes is interesting. If IP spoofing IDS is turned on, is it evaluated before anything else or can someone successfully spoof and cause another alert to trigger which might cause a blocking PF? I'd been relying on the former and hope that if there is an order IDS is applied in a complex attack is the case.

I agree that using a tool as powerful as Blockattacker must be used carefully. For one client involved in Financial Services (Broker trading), because of the excessive number of attacks they're getting, I'm going to create a duplicate of specified alerts and turn that duplicate on and off at specified times to quickly build up lists of blocked IPs during specific times I can monitor... and not run it regularly during business hours.

As for the BlockAttacker being subject to false positives, it <has> happened from time to time but the only times I'm aware it has happened is usually shortly after initial configuration. No remote SysAdmin should be doing anything anyway that should trigger an alert like doing an all port scan. And, IMO ISA's packet analysis is pretty good. Although I haven't seen any documentation on how it works, I assume it's pretty straight-forward, filtering for string lengths and character strings... and since SMTP, HTTP and other commands are pretty standard plus lengths should all be according to RFC specification, I assume that there is very little room for packet analysis error.

So, of course every situation should be handled carefully, but in general I find that the BlockAttacker can be <very> useful.

As for whether the script works or not, I have found that a blocking PF will block access from the remote IP address

Re: Deny rules...

to any ISA IP address, port or service, published or not.  
But, as long as the "attacker" still has a session open,  
the PF may not yet be effective... but close that initial  
session and try again and you should find the block  
working.

If you are writing code to populate a Client set, remember  
that you have to stop/restart the ISA services immediately  
after creating the Client Set and maybe after pointing a  
Web Publishing rule to it although I have found that a  
stop/restart has not been necessary if I modify the  
entries in the Set.

Tony Su

>-----Original Message-----  
>Thanks good point..  
>  
>*The way i do it.. is everything has to do with clients  
sets conserning  
>remote access ..  
>The Script makes sure the ip to be blocked is not it's  
own ip.  
>I have few outside servers to connect from to my servers  
and i get mails  
>conserning everything  
>and most cases i have very important things be sent to me  
by SMS message to  
>my telephone.  
>I have my ISA with its reporting system.. and then i have  
Snort inside my  
>reporting direct to SMS.  
>  
>Still there are holes i'm working on that i consider  
risky ..i'm hoping to  
>be lucky untill i'm finished.  
>  
>I just feel like i must get this to block auto even if  
not for a short  
>period of time, i thouhgt it might be smarter than  
>noting at all.  
>  
>But as you say this mack adres spoof is actually to easy  
with macspoof in  
>lin that you got me to think . =)  
>  
>Still i think about if it's not better to block 99% of  
scanners and then  
>when he or himm who knows his way around  
>and will get trouhg no matter if i have this auto block  
or not...*

Re: Deny rules...



>> *created..*  
>>  
>> *then i test a web page .. behind a published server..*  
and it shows..  
>> *then i telnet the site on port 80 to be sure and it*  
*answers fine.*  
>>  
>>  
>> *Any ideas ? ..*  
>>  
>> *Regards*  
>> *Steinki.*  
>>  
>>  
>>  
>>  
>>  
>> *"Tony Su" <anonymous@discussions.microsoft.com> wrote*  
*in message*  
>> *news:1aaba01c41e9b\$a9c264f0\$a301280a@phx.gbl...*  
>> *The code is pretty much spelled out in a page at*  
>> *msdn.microsoft.com, this code was created awhile ago.*  
>> *Configure IDS alerts to trigger and run the script.*  
>>  
>>  
>> <http://www.toolzz.com/Downloads/ISATools/Jalojash/BlockAtta>  
>> *cker.zip*  
>>  
>> *Before deploying, understand how it works and if you*  
>> *accidentally block yourself how to regain access to your*  
>> *server so you can remove the block.*  
>>  
>> *I have found that although a block can be created for*  
*any*  
>> *one address on the external interface, the actual effect*  
*is*  
>> *to a block which effectively denies to <all> IP*  
*addresses*  
>> *on the external interface.*  
>>  
>> *Tony Su*  
>>  
>>  
>>  
>>  
>>  
>>  
>> >-----Original Message-----  
>> >Hi.  
>> >

>> >I'm cowboycoding deny script to create automatic deny  
>> packed filters  
>> >triggered by action,  
>> >they get created and look perfect but they just dont  
>> block..  
>> >  
>> >pf.PacketDirection = fpcPfDirectionIndexBoth  
>> >pf.SetLocalHost fpcPfDefaultProxyExternalIp  
>> >pf.LocalPortType = fpcPfAnyPort  
>> >pf.RemotePortType = fpcPfAnyRemotePort  
>> >pf.SetRemoteHost fpcPfSingleHost, WshEnv  
>> ("ALERT\_PARAMETER\_1")  
>> >  
>> >Even when i create them manually they just dont affect  
>> servers that are  
>> >published.  
>> >  
>> >I have about 60 ip's on my external interface and  
>> servers that are  
>> >published have one ip each .  
>> >  
>> >Is it possible that deny rules dont work for this ? or  
am  
>> i doing the whole  
>> >thing wrong..?  
>> >  
>> >Any info would be nice..  
>> >Regards.  
>> >Steinki..  
>> >  
>> >  
>> >  
>> >.br/>>> >  
>>  
>>  
>  
>  
>.  
>