

## Re: IPSec Policy Doesn't Really Block

**Source:**

<http://www.tech-archive.net/Archive/Win2000/microsoft.public.win2000.networking/2004-09/0027.html>

---

**From:** Joseph Melika ([jmelika\\_at\\_hotmail.com](mailto:jmelika_at_hotmail.com))

**Date:** 08/31/04

Date: Tue, 31 Aug 2004 10:18:52 -0700

Steven,

Thanks for getting back to me on this. I did as you said and basically blocked all IP's mirrored from Any IP to My IP. I then created a couple of basic filters to allow port 80 and port 25 inbound from Any to My IP, also mirrored. That worked like a charm. But then I realized I could not go outbound, like surfing the web. So I enabled from My IP to Any IP mirrored policy, any protocol, and permit. That ends up disabling the inbound block filter. Once the enable outbound filter is set, I can Terminal Service into the server and hit all ports on it from any public IP.

Any ideas why that happens?

Thanks,

Joseph Melika

"Steven L Umbach" <n9rou@n0-spam-for-me-comcast.net> wrote in message news:yPPYc.88360\$Fg5.72942@attbi\_s53...

>I have created ipsec policies that work. I usually start with a mirrored  
>block all IP rule. The I add mirrored permit rules for the exceptions such  
>as the lan subnet, individual IP addresses, and then the specific  
>ports/protocols/addresses. Make sure you have the source and destinations  
>correct as that can be confusing. For instance to permit port 80 tcp into  
>my computer I would create a mirrored rule for source address:any IP  
>address, destination address:my IP address, protocol TCP, source port:any,  
>destination port:80. --- Steve

>  
><http://www.securityfocus.com/infocus/1559> -- this may help.

>

>

> "Joseph Melika" <jmelika@hotmail.com> wrote in message  
> news:uBtUfyujEHA.1404@TK2MSFTNGP09.phx.gbl...

>>I am having an issue with IPSec. I simply have a server sitting at a  
>>co-lo. It is serving on prts 80, 443, 5274, and 6667. I need to open  
>>those ports to the public but blocking everything else. I also need to  
>>permit the server to be able to talk to its neighboring computers, as well  
>>as some computers at a different subnet with no restrictions.

>>  
>> *Here is a list of IPSECPOL.exe commands I am using to create the policy.*  
>> *Please be aware of the possible word wrap.*  
>>  
>> =====  
>> *ipsecpol -w REG -p "Policy" -r "Local Site" -f*  
>> *x.x.x.0/255.255.255.0+x.x.x.x:\* -f x.x.x.x+x.x.x.0/255.255.255.0:\* -n*  
>> *PASS*  
>> *ipsecpol -w REG -p "Policy" -r "Remote Sites" -f*  
>> *192.215.60.0/255.255.255.0+x.x.x.x:\* -f*  
>> *206.16.86.0/255.255.255.240+x.x.x.x:\* -f*  
>> *206.16.76.32/255.255.255.240+x.x.x.x:\* -f 192.215.11.11+x.x.x.x:\* -f*  
>> *192.215.5.16+x.x.x.x:\* -n PASS*  
>> *ipsecpol -w REG -p "Policy" -r "Applications Ports" -f \*+x.x.x.x:5274 -f*  
>> *\*+x.x.x.x:6667:TCP -f \*+x.x.x.x:80:TCP -f \*+x.x.x.x:443:TCP -n PASS*  
>> *ipsecpol -w REG -p "Policy" -r "Block Everything Else" -f*  
>> *\*=x.x.x.x:\*:\* -n BLOCK*  
>> =====  
>>  
>> *x.x.x.x stands for the server's IP address, while x.x.x.0 stands for the*  
>> *24 bit subnet it's on.*  
>>  
>> *Now the issue is that when I create this policy and assign it, I am still*  
>> *able to connect to the server from home using Terminal Services. My home*  
>> *PC is not on any of the subnets listed above. How come the IPSec Policy*  
>> *doesn't work? I can do a netdiag /test:ipsec and I do see the policy*  
>> *applied. It just doesn't seem to be doing its job.*  
>>  
>> *One thing is that I did notice that the PASS and BLOCK did not actually*  
>> *use the existing filter action "Permit" and "Block". Each of those*  
>> *commands created its own filter action with the same name as the filter*  
>> *itself, i.e. Local Site. I even tried going to the UI and change the*  
>> *action to Block or Permit and restarted IPSec Policy agent, but still*  
>> *didn't work.*  
>>  
>> *Has anyone been able to get IPSec to work properly? Can someone give me*  
>> *any advice on this?*  
>>  
>> *I appreciate it guys!*  
>>  
>> *Joseph Melika*  
>>  
>  
>