

How to configure service console ...



[Tysonl](#) 7 posts since

Apr 24, 2008

I've spent most of today looking for information on the "esxcfg-firwall --ipruleAdd" command. I want to restrict SSH access to only 2 subnets (let's say 192.168.123.0/24 and 192.168.134.0/24). IP rules looks like it should be able to do it but I've not figured out the right combination of rules.

This is what I've tried (and the man page for esxcfg-firewall made it sound like it should work...)

```
esxcfg-firewall --ipruleAdd 0.0.0.0/0,22,tcp,REJECT,"Block_SSH"
esxcfg-firewall --ipruleAdd 192.168.123.0/24,22,tcp,ACCEPT,"Allow_123_SSH"
esxcfg-firewall --ipruleAdd 192.168.134.0/24,22,tcp,ACCEPT,"Allow_134_SSH"
```

My ressoning was that since SSH is open to the world to start I would deny all and then allow the two subnets I wanted. What actually happened is the black worked and the allows didn't.

This is the example from the man page I based these rules on

```
To allow only one host access specified port of COS
esxcfg-firewall --ipruleAdd 0.0.0.0/0,902,tcp,REJECT,"block_902"
esxcfg-firewall --ipruleAdd 192.168.1.1,902,tcp,ACCEPT,"allow_one"
```

Any help you can give would be awesome. Thanks all. Tags: firewall, security, hardening



[Chuck8773](#) 229 posts since

May 4, 2007 1. **Re: How to configure service console firewall to only allow access from certain IPs?** Jun 28, 2009 7:00 AM

I have never done this but if it is implemented like Cisco is, then the deny all should be the last rule. It follows a lazy evaluation. If your deny all is first it stops processing after it finds that match. Try putting it last.

Charles Killmer, VCP

If you found this or other information useful, please consider awarding points for "Correct" or "Helpful".



[Tysonl](#) 7 posts since

Apr 24, 2008 2. **Re: How to configure service console firewall to only allow access from certain IPs?** Jun 29, 2009 10:40 AM

👤 in response to: [Chuck8773](#)

I've tried entering the rules in reverse order and it doesn't change the behavior.

Thanks for the suggestion though.

How to configure service console ...



[Chuck8773](#) 229 posts since

May 4, 2007 3. **Re: How to configure service console firewall to only allow access from certain IPs?** Jun 29, 2009 11:31 AM

👤 in response to: [Tysonl](#) How are you verifying that it isn't working? I just set it up to block one host to port 902 and it worked. I will try to set it to allow only one and report back.

Charles Killmer, VCP

If you found this or other information useful, please consider awarding points for "Correct" or "Helpful".



[Chuck8773](#) 229 posts since

May 4, 2007 4. **Re: How to configure service console firewall to only allow access from certain IPs?** Jun 29, 2009 11:35 AM

👤 in response to: [Chuck8773](#) I set it up to block 0.0.0.0/0 and allow 192.168.1.247/32 and that worked. I verified by connecting a telnet session to the host on port 902. The VIC was still able to connect. Also, keep in mind that if you are connecting to virtual center, it still has access to the hosts.

Charles Killmer, VCP

If you found this or other information useful, please consider awarding points for "Correct" or "Helpful".



[Tysonl](#) 7 posts since

Apr 24, 2008 5. **Re: How to configure service console firewall to only allow access from certain IPs?** Jun 29, 2009 12:09 PM

I figured it out.

It works but there is a bug with the way rules are added.

Here is an example of adding some rules and the order they appear in the rules list. (for it to work the REJECT rule has to appear to the ACCEPT rule)

```
esxcfg-firewall --ipruleAdd 0.0.0.0/0,22,tcp,REJECT,"block"
esxcfg-firewall --ipruleAdd 192.168.123.0/24,22,tcp,ACCEPT,"allow123"
esxcfg-firewall -q
....
block
allow123
....
esxcfg-firewall --ipruleAdd 192.168.134.0/24,22,tcp,ACCEPT,"allow134"
esxcfg-firewall -q
....
allow134
block
```

How to configure service console ...

allow123

....


So as you can see the reason it didn't seem to work when I initially did this was that I was testing from a box on the 134 subnet and it ends up appearing before the REJECT rule and thus doesn't work.

I've verified this happens on two different ESX4 hosts. Think I found a bug; or at least an unwanted feature.



[Tyson1](#) 7 posts since

Apr 24, 2008 **6. Re: How to configure service console firewall to only allow access from certain IPs?** Jun 29, 2009 12:08 PM

 in response to: [Chuck8773](#) I was testing it by trying to ssh to the host. (I'm wanting to restrict SSH access to just our admin subnets)


I ended up figuring out the problem. See my above post for details.

Thanks for your help.



[Chuck8773](#) 229 posts since

May 4, 2007 **7. Re: How to configure service console firewall to only allow access from certain IPs?** Jun 29, 2009 6:59 PM

 in response to: [Tyson1](#) Glad it is working. Interesting bug though.

Charles Killmer, VCP

If you found this or other information useful, please consider awarding points for "Correct" or "Helpful".