

Re: Please help...

Source: <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2002-11/1882.html>

From: David (davidwnh@adelphia.net)

Date: 11/19/02

From: "David" <davidwnh@adelphia.net>

Date: Tue, 19 Nov 2002 14:21:01 GMT

I'm not familiar with Checkpoint but if it has SPI at the application level you may be able to filter via the application name. I'm not sure that this is even possible with checkpoint and suspect it isn't but if it is it's an easy solution.

Otherwise Yahoo messenger normally uses 5050 TCP(peer-to-server dest. port) and 5105 TCP(peer-to-peer listening port) and MSN Messenger 1863 TCP(peer-to-server dest. port). You can filter these ports however these clients can still obtain access via peer-to-server access or be configured to use a proxy if it is available using other ports . In this case you are dealing with dest. ports 20,21,25,37,80, and 119. Since some of these ports will be ones you may need other access to, your solution would be to filter the dns addresses these programs use to connect. Filtering IP addresses usually won't work with such clustered services. My version of MSN messenger connects to autos.msn.com and msimg.com at logon. I suspect autos.msn.com is a passport server and don't know if filtering this would break any other passport enabled services(not to mention that MSN messenger can be configured to use third party servers that do not need passport). I would start with filtering msimg.com and go from there. A similar investigation of server access then filtering should work with Yahoo also. To make things even worse Yahoo messenger can initiate connections via embedded uri links. In this case you would need to filter the "ymsgr:" uri handler that can be embedded into email and websites.

So basically block the Yahoo listening port, the server dns addresses, and if you think necessary the Yahoo uri handler.

Port 23 is telnet, but I suspect Neo meant 21 for FTP. The problem with this is you can download via http so allowing web access allows downloading software.

"NeoSadist" <neos@dist> wrote in message
news:utk8fu6re1s34e@corp.supernews.com...

>

> "*Dano Tang*" <dtang@macaucabletv.com> wrote in message

> news:arcpkn\$mab1@ctmsun0.macau.ctm.net...

>> *Dear all,*

Re: Please help...

> >
> > *Can anyone direct me how to solve to block the following 2 services within my network? I am currently using CheckPoint 4.1*
> >
> > *1. Microsoft MSN Messenger*
> > *2. Yahoo Messenger*
> >
> >
> > *Thanks in advanced!!*
> >
> > *Regards,*
> > *Dano*
> >
> >
>
>
> *First off, if people on your network are installing these things without permission, let their boss know that their employees are compromising the security of the company. Try to get a policy written that those employees that install ANY software without your permission in writing will be fined / punished / fired. Who runs the network? You or them? Who is going to be in trouble if it all goes down? You.*
> *But anyways, I'd block msn port (port 1863) for msn messenger. Also, I'd block port 23, since that will prevent them from downloading it and installing it in the first place.*
> *Then, I'd watch the logs (since I don't know the specific yahoo ports) and find out what ports are hitting yahoo alot, and which ports are being used to sign into hotmail and passport, which will enable you to block those sites or those ports, one or the other.*
>
>