

CLOSING: Norton Personal Firewall 2003

Source: <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2002-12/1101.html>

From: Alsvik Ture (ture@alsvik.dk)

Date: 12/10/02

From: "Alsvik Ture" <ture@alsvik.dk>
Date: Tue, 10 Dec 2002 22:29:03 +0100

Thanks all!

Thank you for your comments and advice– that was very nice of you!

I have decided to leave this as it is. It seem to difficult for me to explain. What i write in one post is not read by everyone in the thread, so i have to write stuff more than twice....

People keep asking me about the way i've uninstalled the programs and what kind of rules i have created. And when i explain this, some thinks that's the reason – but later on the let me know that it's the only way to do it.

I understand that this is a lot of reading to understand everything. And even i find it hard to overview all the things written – so that's it! I'll go back to NPF2002 because it detects port scans, and NPF2003 doesn't! No differences in rules or programs or services or hardware. The only difference is NPF2002/NPF2003!

You guys think like i: Symantec is a well-known and a good security advisor (?) with trusted products, so if any user finds a hole or error or malfunction in their programs – we say to the user: "You idiot. You did something wrong!"

I haven't and i have tested myself several times to see if i did something wrong during uninstal, install or setup of rules and programs and what stuff i have enabled and at what level. But i can't find any differences from when i installed NPF2002 to when i installed NPF2003.

Just created a ghost from my present system on my "server" (which is running w2kpro) and after a "format c:" i reinstalled w2kpro – updated it to SP3 and installed NPF2002. It detects port scans. Formatted the computer and installed w2kpro and installed NPF2003. It DOESN'T detect port scans!

There are several other things i tested during this "change of firewall" session, and they all showed me the same thing as before: NPF2003 is not as "secure" as NPF2002. When i write secure in "" – it's because i don't know!!!But when it comes to protection of the computers behind the "server"

NPF2003 doesn't have any influence on the traffic to and from the internet to these computers. NPF2002 does. NPF2003 doesn't detect the port scans – and in my mind i find that a big issue.

When i write i have no rules – i mean that i haven't created ay rules! NPF has created "automatic" rules for me, and just ask me if it's ok to apply them (permit?, block? , automatic?). For the services i use on the internet i have answered "automatic" and that basically means "permit all traffic to and from these programs to any computer on the internet" – and that haven't changed since NPF2002.

The only thing that have changed is the "intrusion detection" features. Which is now more configurable. I can exclude and include different features. They are all by default enabled – also the one called "port scan"! And that's the one not doing its job right! I've added monitoring rules to all the ports on which i'm running services, so i can see what happens.

..... STOP STOP.....

Here i go again! Stop me!
Thank you for your help, interest and concern.
I'll think i'll wait for Symantec to respond.
They actually did today. I've sent them 6 mails and today i got one back:

Hi Ture,
Thank you for contacting Symantec Online Technical Support.
In your message, you wrote:

>I'm running a webserver, ftpserver, smtpserver, webmail and pop3server – these ports are now showed as open

Ture, Norton Personal Firewall (NPF) isn't designed for servers. And I gather from your message that you have installed NPF on a server. For more information refer to the following article:

Title: 'Norton Internet Security and Windows NT, 2000, and XP Servers'

Document ID: 2000053008391436

> *Web URL:*

<http://service1.symantec.com/Support/nip.nsf/docid/2000053008391436?Open&src>

=w

Please let us know if we can be of further assistance.

Regards,

Symantec Authorized Technical Support

Same problem here: I've positivly stated that i'm using w2kpro, but referring to my services as "server" made these guys (just like you guys) think it was a server os. Just to hooked up on finding it to be my error or my understanding or reading problem.!

Bye bye – i'll drop by one day if i find any answers or solutions to my problem!

But i guess i need to fix this with Symantec in a dialogue with one of their support–dudes. Just to many trying to help here, and even though i think all of you guys really want to make a difference, you just can't spend the entire day reading all my posts. So you end up with questions, that you caould have found the answer to in an earlier post from me. That's means i have to answer the same questions over and over again, and the thread just grows larger and larger with the same questions and answers!

Sorry if i'm annoying anyone. That's not my intention.

It's to find a solution with out spending hours a day writing my problems over and over again!

If Symantec turns me down, i'm back here crying :o)

Ture A.