

Re: SP1 enables Windows XP firewall how to turn it off?

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2005-05/msg05345.html>

- *From:* "Susan Bradley, CPA aka Ebitz – SBS Rocks [MVP]" <sbradcpa@xxxxxxxxxxxxx>
 - *Date:* Mon, 23 May 2005 06:48:28 -0700
-

Yes, it's home computers that VPN in that infect office computers... so why not add an additional layer to protect those systems.

If only 10% of network admins would have wanted that on.... we need to educate our network admins of how these risks are coming in the door

Microsoft TechNet Radio:

<http://www.microsoft.com/technet/community/tnradio/default.aspx>

Listen to that and see if you still think the same...

Leythos wrote:

In article <xn0e2l4t19f02qh005@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>, steve.foster@xxxxxxxxxxxxx says...

Leythos wrote:

In article <uoKflegXFHA.2l28@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>, marina@xxxxxxxxxxxxxxxxxxxxxxxxxxxx says...

Hi CLevere,

Why would you want to do that??? That is not necessary and not safe at

Re: SP1 enables Windows XP firewall how to turn it off?

all.

Rather tell us with which
program you have a problem.

Acually, you don't know that it's unsafe. I have never used a personal
firewall on any of our servers or workstations and secure the border
properly. All systems are protected from inbound attachments, HTTP is
filtered against malicious scripts/active-x, etc....

Once upon a time, this was generally a secure
option. But I don't believe this is adequate any
more in many environments.

Got news for you, but with a properly configured firewall,
proper filtering of HTTP sessions, proper blocking of
attachments, and such, there is little that can make it
inbound to the users desktop. In the 25
+ years I've been working with computers, servers, and
systems, not one client or any of my own has ever been
compromised by a virus or exploit.

Today, with laptops, PDAs and other "roaming"
devices that come and go between the corporate LAN
and other networks, as well as much increased
remote access (particularly VPN), the "perimeter"
is a much more nebulous concept than it used to be.

Sorry, but with PDA's and such, there is nothing a firewall
will do, as those devices connect via USB, and the Windows
firewall does nothing to block a USB device. Those devices
are, in a quality shop, covered under a Access Policy, and in
most cases, they are forbidden except where authorized. In our
case, only select managers and doctors and users are permitted
to utilize them. Also, a strict discipline policy is enforced,
as those devices are the second most dangerous threat to
security.

Keep in mind (as I kind of ranted above), windows firewall

Re: SP1 enables Windows XP firewall how to turn it off?

will do nothing to stop a PDA.

If the MD takes his laptop home, and he/his son/daughter gets to surf the net, there's a good chance that it will come back to the office with *something* nasty on it (even if it's got AV/AS s/w). At that point, your entire corporate LAN gets infected too.

If you notice, I never mentioned laptops. All laptops run a proper two-way firewall that has defined, configured, locked-down rules. The rules are not something that the user can change, they are defined by the IT department, and are not something the user may access.

The personal firewall that Windows forced down our throats for XP SP2 was bad enough, in a domain environment it should be disabled by default.

Why? Why should every machine have the ability to reach out and manipulate every other machine on the LAN? Do you give all your staff master keys to every lock?

Why should MS change the "domain" security structure when it's mostly the home users/computers that cause the problem. I'm willing to bet that if MS had asked if domain administrators wanted the firewall enabled by default, that less than 10% would have said YES.

In a properly configured domain, "Users" have little access across the network to others systems, only the management has the type of access you suggest, and that's the way it should be.

Windows firewall breaks one of the management/testing functions that domain admins have had since it's start.

Re: SP1 enables Windows XP firewall how to turn it off?

There are many applications that it does not properly detect and auto-configure exceptions for (such as RAdmin and VNC) that are used in remote support of users in domains.

Like every other firewall on the planet, it needs configuration management. The tools are there to do this - it's called GPO.

And unlike every firewall on the planet, it was installed by default, enabled by default, and blocked non-MS remote management tools by default, and does nothing to block users from connecting outbound.

As for GPO, that's only good if you go and download the new functions for Windows 2000 server as the policy objects for SP2 management are not in the Windows 2000 install by default.

The only good thing about the firewall is that you can go into the DC, select the computers, and then stop and disable the Windows Firewall service remotely in most cases.

It still would have been better to have it DISABLED in a domain and enabled in a workgroup. This would have protected the audience most likely to benefit from it, and left alone the audience most impacted by its being enabled.

--

An open letter to the Security Community::
<http://msmvps.com/bradley/archive/2004/12/12/23540.aspx>

.