

Re: XPsp2 firewall – bug? – disables on certain networks

Source:

http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security_admin/2005-01/1766.html

From: John M (john.f.mannarino_at_usace.army.mil)

Date: 01/21/05

Date: Fri, 21 Jan 2005 09:04:58 -0500

I have reread the document from the cable guy and the "Deploying Windows Firewall Settings for Microsoft Windows XP with Service Pack 2" document from microsoft

<http://www.microsoft.com/downloads/details.aspx?FamilyID=4454e0e1-61fa-447a-bdcd-499f73a637d1&DisplayLa>

Even if the DNS suffix is different, the computer can get a new policy from a different domain controller. To me, I interpret this as "If the computer cannot contact a domain controller and get the current policy or a new policy, then it will be on an unmanaged network". I can see where the concern is from DHCP servers mimicking your domain settings.

We came down to two choices:

1) Make the domain profile and standard profile exactly the same, so it wouldn't matter where the computer was and deal with the consequences of some stuff not working for users while away from our network. Again, when using group policy for windows firewall, when we define port exceptions, you can not grant access by dns names, only by IP subnets.

2) Since our DNS server is accessible to the outside world, we could manually enter the DNS server and suffix settings for all connections. This can also be done via group policy. Thus, the computer would always be considered on a managed network and we just configure the domain profile.

Both give us the desired results because general consensus is that it is better to always have the firewall on no matter where the computer is.

"Torgeir Bakken (MVP)" <Torgeir.Bakken-spam@hydro.com> wrote in message news:ORF6xVw\$EHA.1524@TK2MSFTNGP09.phx.gbl...

> *John M wrote:*

>

>> *I'm curious as to where you learned that SP2 firewall determines*

>> *its connection via the DNS suffix, I could only find that it is*

>> *determined whether it can contact a domain controller or not.*

> *Hi*

>

microsoft.public.windowsxp.security_admin: Re: XPsp2 firewall – bug? – disables on certain networks

> *For the WinXP SP2 FW, contact with the domain controller is not
> a part of this determination process (where did you find that
> statement?).*
>
> *Here is how the SP2 firewall determines if it is to activate
> the domain or standard profile:*
>
> *If last-received Group Policy update DNS name match any of the
> connection-specific DNS suffixes of the currently connected
> connections (not PPP or SLIP-based) on the computer the FW's
> domain settings will be used. There is no way to change this
> behavior.*
>
> *From*
> *The Cable Guy – May 2004*
> *Network Determination Behavior for Network-Related Group Policy Settings*
> <http://www.microsoft.com/technet/community/columns/cableguy/cg0504.mspx>
>
> <quote>
> *To apply this behavior to Windows Firewall settings:*
>
> *() If the connection-specific DNS suffix of a currently connected
> connection on the computer that is not PPP or SLIP-based (such as
> an Ethernet or 802.11 wireless network adapter) matches the value
> of the*
> *HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Group
> Policy\History\NetworkName registry entry, Windows Firewall uses
> the domain profile.*
>
> *() If the connection-specific DNS suffix of a currently connected
> connection on the computer that is not PPP or SLIP-based does not
> match the value of the*
> *HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Group
> Policy\History\NetworkName registry entry, Windows Firewall uses
> the standard profile.*
>
> *You can determine the connection-specific DNS suffixes of the
> currently connected connections on the computer from the display
> of the ipconfig command issued from a command prompt.*
>
> </quote>
>
> *Read the Cable Guy article for more about this.*
>
>
> --
> *torgeir, Microsoft MVP Scripting and WMI, Porsgrunn Norway*
> *Administration scripting examples and an ONLINE version of*
> *the 1328 page Scripting Guide:*
> <http://www.microsoft.com/technet/scriptcenter/default.mspx>

Re: XPsp2 firewall – bug? – disables on certain networks