

Re: XPSP2 domain firewall settings

Source:

http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security_admin/2005-10/0384.html

From: Steven L Umbach (n9rou_at_nospam-comcast.net)

Date: 10/14/05

Date: Fri, 14 Oct 2005 12:15:37 -0500

I certainly agree that something does not add up. The article mentions connection-specific DNS suffixes which simply do not exist on most domain computers that use DHCP option 15. Instead I see the domain name as primary dns suffix. The other thing that does not add up is that when I look at the value for HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Group Policy\History\NetworkName registry entry I see the network IP that the computer is on as in 192.168.1.0 in my case. So does that mean that if the computer detects it is not on my regular network IP that is a trigger?? I suppose there could be other triggers such as failure to locate or contact a domain controller [which is pinged during startup] or authentication failure. Maybe the network IP is used since that would be determinable earlier in the startup cycle so that the firewall could be enabled early in the startup cycle. If it is triggered by network IP alone however the firewall might not be enabled if the computer is started on another network with the same network IP which is very possible within the private network addresses. I would also like more details on how the firewall profile is triggered but as know that is about the only information I have seen. ---
Steve

"Anthony Yates" <anthonyDINGyates@airDONGdesk.com> wrote in message news:eYW\$OEN0FHA.800@TK2MSFTNGP12.phx.gbl...

>I understand the Cable Guy article and the process described below. There
>must be more to it. As it is described the process does not fully make

>sense. I'd like to understand exactly how it works.

>

> "If the last-received Group Policy update DNS name matches....." My
> understanding of this is the reg key for Group Policy/History, which
> contains the FQDN of the domain controller, so basically this just means
> the DNS domain name that policies were received from. I'm not sure if this
> really means the last-received (e.g a week ago if now off the network).

>

> ".....any of the connection-specific DNS suffixes of the currently
> connected connections on the computer". The Primary suffix of a domain
> computer is the domain name, so it can't be that. The connection-specific
> suffix is whatever the DHCP server handed out. There are a few problems
> with this as it is defined:

> - Mine is blank (Windows DHCP) yet the PC firewall knows it is on the

> domain. It has to be using a different algorithm.
> – XP clients don't need a connection–suffix to resolve names, so there is
> no particular need for the DHCP to hand one out to them
> – If I have two domains on the same network, which suffix would DHCP hand
> out and which domain would then think it was or was not on the network?
> – It would be easy to fool the firewall with an incorrect DHCP assigned
> suffix.
>
> The way the process is described only really works in one direction. If a
> domain PC connects directly to the Internet, and if the ISP assigns a
> connection suffix, the computer will know that it is not on the domain.
> That seems a rather unreliable way to go about it. If the ISP does not
> assign a connection suffix it would be blank, exactly as it is on my
> network.
>
> Like I say, the process does not seem to make sense and I'd like to
> understand how it really works.
>
> Anthony
>
>
>
>
>
> "Steven L Umbach" <n9rou@nospam–comcast.net> wrote in message
> news:OnPkfcB0FHA.2960@tk2msftngp13.phx.gbl...
>> It can always be the same but I believe it compares it to the Group
>> Policy update DNS name which would only be available if connected to the
>> domain where a domain controller is available. The link below is from
>> Microsoft documentation and though it specifies connection–specific DNS
>> suffix it refers to DHCP option number 15 which is the domain name and
>> what you see in primary dns suffix in an ipconfig /all. Your problem with
>> the particular computer may be due to it not authenticating to the domain
>> at boot up and it used cached credentials instead to allow the user to
>> logon and then as soon as it can contact a domain controller the user is
>> authenticated to the domain. If it can not find a domain controller at
>> startup Group Policy will not be applied and you may find an error
>> reflecting that in the application log or for sure in the userenv.log
>> file. --- Steve
>>
>>
>>
>> *****
>> The network determination algorithm performs the following analysis:
>>
>> . If the computer is not a member of a domain, it is always attached
>> to another network.
>>
>> . If the last–received Group Policy update DNS name matches any of
>> the connection–specific DNS suffixes of the currently connected
>> connections on the computer that are not PPP or SLIP–based, then the
>> computer is attached to a managed network.

>>
>> . *If the last–received Group Policy update DNS name does not match
>> any of the connection–specific DNS suffixes of the currently connected
>> connections on the computer that are not PPP or SLIP–based, then the
>> computer is attached to another network.*
>>
>>
>> *Windows uses this network determination process during start up and when
>> it is informed by the Network Location Awareness service that network
>> settings on the computer have changed.*
>>
>> *The connection–specific DNS suffix of the connection over which the last
>> set of Group Policy updates were received is determined from its TCP/IP
>> configuration, which is typically configured using Dynamic Host
>> Configuration Protocol (DHCP) and the DNS Domain Name DHCP option (DHCP
>> option number 15). You can also manually configure connection–specific
>> DNS suffixes from the DNS tab in the advanced properties of the Internet
>> Protocol (TCP/IP) component, available from the properties of the
>> connection in the Network Connections folder.*
>>
>>
>>
>> *"Anthony Yates" <anthonyDINGyates@airDONGdesk.com> wrote in message
>> news:Onwt0i9zFHA.1264@tk2msftngp13.phx.gbl...*
>>> *It can't be the primary suffix, as that is always the same. There is no
>>> point comparing that with anything if the computer is a member of the
>>> domain. There must be a process for confirming whether the PC has logged
>>> onto the domain. If the process is as described then it seems a very
>>> unreliable way of knowing when you are off the domain.
>>> We occasionally get a PC where you can't use Remote Assistance or Remote
>>> Desktop until you reboot it. This seems to be caused by a faulty
>>> determination by the firewall of whether the PC is on the network or
>>> not. I don't mind if it only gets it wrong in one direction – on when it
>>> should be off. I am worried if it gets it wrong in the other direction –
>>> off when it should be on.*
>>>
>>> *Anthony*
>>>
>>>
>>>
>>> *"Steven L Umbach" <n9rou@nospam–comcast.net> wrote in message
>>> news:OeJIKM2zFHA.2652@TK2MSFTNGP14.phx.gbl...*
>>>> *I wonder if they really mean connection specific dns as that often if is
>>>> not configured. The domain name is usually configured in the DHCP scope
>>>> option 15 or even if you do not use DHCP when you run ipconfig /all on a
>>>> domain computer you will see primary dns suffix which I believe is
>>>> probably what is used. That is my guess and I can not confirm it.
>>>> Possibly it could also have something to do with whether a domain
>>>> controller can be contacted and used for authentication of the computer
>>>> account or not. --- Steve*
>>>>

>>>>

>>>>

>>>> *"Anthony Yates" <anthonyDINGyates@airDONGdesk.com> wrote in message*

>>>> *news:ulQfTX0zFHA.3124@TK2MSFTNGP12.phx.gbl...*

>>>>> *The Windows XP SP2 client is supposed to detect whether it is on or*

>>>>> *off the domain network by comparing the connection-specific DNS suffix*

>>>>> *to the last Group Policy.*

>>>>>

>>>>> *We do not assign a connection-specific DNS suffix in our (Windows)*

>>>>> *DHCP. Yet the PC's recognise they are on the network and activate the*

>>>>> *domain firewall policy. Can anyone confirm that there is a smarter*

>>>>> *piece of logic in place, such as whether the PC connected to the DC or*

>>>>> *not?*

>>>>>

>>>>> *Thanks,*

>>>>> *Anthony Yates*

>>>>>

>>>>

>>>>

>>>

>>>

>>

>>

>

>