

Re: Windows Firewall on Domain Controllers

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2006-08/msg00985

- *From:* "Jorge Silva" <jorgesilva_pt@xxxxxxxxxxxx>
 - *Date:* Fri, 28 Jul 2006 20:22:23 +0100
-

Are you talking about Windows 2003 or Windows XP?
By default the Windows 2003 don't activate any FW.

--

I hope that the information above helps you

Good Luck
Jorge Silva
MCSA
Systems Administrator

"Ron" <rhardin@xxxxxxxxxxxxxxxxxxxxxx> wrote in message
<news:68FBE639-4A0C-4982-8F26-C09CC106F976@xxxxxxxxxxxxxxxxxxxx>

Jorje, thanks for responding. Quick follow-up: you say "don't run a FW on
a
DC", and that was my approach from the beginning. But as I stated,
updates
from Microsoft keep turning the Windows Firewall back on. So how does one
turn it off so it stays off?

--
Ron

"Jorge Silva" wrote:

Hi

- * Server 2003 defaults to Windows Firewall active.
- * Domain Controller doesn't work with firewally active unless it is manually configured for all the AD ports and you do some voodoo with RPC ports.

Re: Windows Firewall on Domain Controllers

Don't use firewall on a DC, use a different machine, if you can don't join the FW to the domain unless you have a good FW solution like ISA 2004 in a back to back configuration.

Assuming the above points are correct on my part, what is the best practice for administering the firewall on domain controllers (I have about 30 of them scattered all over the country)?

Again you shouldn't use a FW on a DC is a bad practice and represents security issues. Configuring FW on a DC depends on what you need to do with it, Applications,DNS,DHCP,Wins,SMB,Replication,etc.

Here's some ports to take:

By default, Active Directory replication over RPC (Remote Procedure Calls) takes place dynamically over an available port via the RPC Endpoint Mapper (RPCSS) using port 135;

Application protocol Protocol Ports
Global Catalog Server TCP 3269
Global Catalog Server TCP 3268
LDAP Server TCP 389
LDAP Server UDP 389
LDAP SSL TCP 636
LDAP SSL UDP 636
IPsec ISAKMP UDP 500
NAT-T UDP 4500
RPC TCP 135
RPC randomly allocated high TCP ports TCP 1024 – 65536

832017 Service overview and network port requirements for the Windows Server system

<http://support.microsoft.com/default.aspx?scid=kb:EN-US:832017>

224196 Restricting Active Directory replication traffic to a specific port

<http://support.microsoft.com/default.aspx?scid=kb:EN-US:224196>

Re: Windows Firewall on Domain Controllers

I hope that the information above helps you

Good Luck
Jorge Silva
MCSA
Systems Administrator

"Ron" <rhardin@xxxxxxxxxxxxxxxxxxxxxx> wrote in message
news:301A5C97-58EC-426D-B43E-4891BB4E10C0@xxxxxxxxxxxxxxxxxxxx

Need input on recommended best practices. Here's what I've
figured
out:

- * Server 2003 defaults to Windows Firewall active.
- * Domain Controller doesn't work with firewally active
unless it is
manually
configured for all the AD ports and you do some voodoo with
RPC ports.
- * Making a 2003 Server a Domain Controller doesn't
automatically
configure
the firewall
- * Turning off the firewall only fixes the problem temporarily
because
some
Windows Updates automatically turn it back on (without
telling you).

Assuming the above points are correct on my part, what is
the best
practice
for administering the firewall on domain controllers (I have
about 30
of
them
scattered all over the country)?

--
Ron Hardin, CHTP
Director of Technology
Davidson Hotel Company