

## Re: Windows Server 2003 and ICF on a domain controller

**Source:**

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.general/2004-08/2762.html>

---

**From:** Miha Pihler (*mihap-news\_at\_atlantis.si*)

**Date:** 08/30/04

Date: Mon, 30 Aug 2004 22:11:00 +0200

Hi Tony,

Do you have two network cards in your DC? If yes and one leads to the internet then enable ICF only on this card.

It is not recommended configuration if you enable ICF on DC towards your clients. It was never designed for this. Also note that blocking ICMP (ping) is not supported for DC at all (towards clients). These are few things that will break in AD if you block ICMP

- File Replication Service
- Active Directory replication
- GPO link speed detection

ICMP is a legitimate protocol that many applications in the IP world rely on for proper behavior. You can even get lower file transfer speed or terminated connections if you disable ICMP (ICMP Source Quench).

Still if you would like a list of ports and protocols here it is

RPC endpoint mapper 135/tcp, 135/udp  
NetBIOS name service 137/tcp, 137/udp  
NetBIOS datagram service 138/udp  
NetBIOS session service 139/tcp  
RPC dynamic assignment 1024-65535/tcp  
SMB over IP (Microsoft-DS) 445/tcp, 445/udp  
LDAP 389/tcp  
LDAP over SSL 636/tcp  
Global catalog LDAP 3268/tcp  
Global catalog LDAP over SSL 3269/tcp  
Kerberos 88/tcp, 88/udp  
DNS 53/tcp, 53/udp  
WINS resolution (if required) 1512/tcp, 1512/udp  
WINS replication (if required) 42/tcp, 42/udp  
Network time protocol (NTP) 123/udp

microsoft.public.windows.server.general: Re: Windows Server 2003 and ICF on a domain controller

Rule needs to permit inbound traffic on any port above 1023. If your firewall permits all this, there's very little reason to have a firewall.

Mike

"tony adduci" <tonyadduci@discussions.microsoft.com> wrote in message news:98316044-0718-4F6A-B5E2-088D99224819@microsoft.com...

> Hello,

> I have a Windows 2003 server that is a domain controller for 5 windows xp computers. I have a dsl line with 5 statics and I would like to be able to use the ICF with Windows 2003 to serve as a firewall protecting this server

> from the internet requests and pings. (I have a ipmap on my cayman router that takes one of my public's and routes to my internal ip of my server –

I

> have to keep it this way for other reasons)

>

> So my question is after opening the appropriate ports such as filesharing, smtp, pop, remote desktop and ftp... and even the 135 port for RPC what other

> ports need to be opened for my domain controller to be able to serve and

> answer wins, dns and allow computers to join the domain?

>

> I read somewhere that RPC requests use random ports above 5000 but you can

> lock this down... Does anyone have a better way?

>

> Thanks!