

## Re: ISA server at DMZ to join DC in internal network

**Source:** <http://www.tech-archive.net/Archive/ISA/microsoft.public.isaserver/2004-12/0210.html>

---

**From:** Thomas W Shinder [MVP] ([tshinder\\_at\\_hotmail.com](mailto:tshinder_at_hotmail.com))

**Date:** 12/30/04

Date: Wed, 29 Dec 2004 22:37:10 -0600

Hi Carlos,

And how are those trojans going to get on the ISA firewall? Only if you allow admins to use the ISA firewall as a workstation. Otherwise, only gross misconfiguration could lead to this condition.

I always join my back-end ISA firewalls to the domain to take advantage of the significant security benefits from domain membership (firewall client, pre-authentication, etc)

HTH,

--

Tom

[www.isaserver.org/shinder](http://www.isaserver.org/shinder)

Get the book!

Tom and Deb Shinder's Configuring ISA Server 2004

<http://tinyurl.com/3xqb7>

MVP -- ISA Firewalls

"Carlos" <[wt\\_know@hotmail.com](mailto:wt_know@hotmail.com)> wrote in message

news:uiL7drL7EHA.1204@TK2MSFTNGP10.phx.gbl...

: Hi,

:

: I have ISA 2004 server in DMZ. I wish to controll the "policy" in ISA based

: on AD users/groupings and many other things. I "have to" join the ISA server

: to internal domain controller for it to work.

:

: I have several domain controllers in the internal network. I opened the firewall to allow the ISA server to join one of the DC that has "no critical" files reside in it.

:

: Is it SILLY to allow a DMZ machine to join internal network which defeat the

: purpose of separating DMZ with internal network ? If I do not do so, how could I control the ISA policy base on users, groups, OU and many other things ?

:

: Alternatively, I can setup a DC in the DMZ. Open the firewall for this DMZ's

: DC to connect to internal DC. The ISA server will use the DMZ's DC. Does

microsoft.public.isaserver: Re: ISA server at DMZ to join DC in internal network

: this sound safer ?  
:  
: In order for outsiders to penetrate to the internal network, he has to  
: exploit the ISA server first and run "trojans" in the ISA server as I only  
: open the firewall for DMZ internal ip to one of the DC server only. The  
only  
: server that is compromise is the DC and not my entire internal network  
right  
: ?  
:  
: Anyone here use ISA 2004 in DMZ and join to internal domain for whatever  
: reasons ?  
:  
: Thanks  
:  
: Carlos.  
:  
: