

## Re: ISA 2006 web proxy scenario

---

*Source:* <http://www.tech-archive.net/Archive/ISA/microsoft.public.isa/2007-05/msg00143.html>

---

- *From:* [guardian911@xxxxxxxxxx](mailto:guardian911@xxxxxxxxxx)
  - *Date:* 15 May 2007 12:48:58 -0700
- 

On May 15, 10:43 am, "Phillip Windell" <[philwind...@xxxxxxxxxxxxx](mailto:philwind...@xxxxxxxxxxxxx)> wrote:

<[guardian...@xxxxxxxxxx](mailto:guardian...@xxxxxxxxxx)> wrote in message

[news:1179243760.897961.271050@xx](mailto:news:1179243760.897961.271050@xx)

I have the following ISA2006 configuration: 4 ISA2006 Standard Editions servers, each with 2 NICs (External and Internal) in workgroup mode. The 4 servers are in 2 separate DMZ's – see below.

Internet → PIX → ISA2006 external array (DMZ) → Internal network ← ISA2006 internal array (DMZ) ← Internal users

I would like to consolidate this configuration by removing the ISA2006 internal array and having all traffic handled by the external array.

That's good. There is no point in the two arrays you have and no point in having two Back-to-Back DMZs one behind the other as you have now.

However, this has to happen without internal traffic being routed to the Internet.

Why would that ever happen to begin with? Things don't get routed somewhere "just because", ...things get routed to places because that is where they are supposed to go. Routing is determined by the destination, ...it doesn't matter if it is dealing with firewalls, proxys, or simple LAN routers, ...that doesn't change.

option #1 – Create a 3rd NIC in the ISA array and route all requests

Re: ISA 2006 web proxy scenario

for the published servers through that NIC. I'm not sure if this will work or if I need to use a NAT relationship.

No.

option #2 – Add a 2nd external interface on the PIX. NAT all internal user traffic destined to the published servers through the PIX's 2nd external interface which in turn will forward that to ISA's external interface.

No.

Option #3

Get rid of the internal array. Re-address the internal facing Nic of what was previously the external array and adjust the config of the ISA's to conform to the address change. You now have an Edge Array between the LAN and the DMZ. You now have a Back-to-Back DMZ sitting between the ISA Array and the PIX. So if you need a DMZ for some reason, that is where it is.

You would also be miles ahead if the ISA's were domain members, but that would involve saving the config of each ISA, uninstalling ISA, making the machine a domain member, reinstalling ISA, re-importing the config. In theory you can do it on running ISA's by adjusting the System Policies, but I have seen people just make a big mess for themselves in the process of trying that. I prefer to do it the safe way.

Debunking the Myth that the ISA Firewall Should Not be a Domain Member <http://www.isaserver.org/tutorials/Debunking-Myth-that-ISA-Firewall-S...>

--

Phillip Windell [www.wandtv.com](http://www.wandtv.com)

The views expressed, are my own and not those of my employer, or Microsoft, or anyone else associated with me, including my cats.

-----  
Understanding the ISA 2004 Access Rule  
Processing [http://www.isaserver.org/articles/ISA2004\\_AccessRules.html](http://www.isaserver.org/articles/ISA2004_AccessRules.html)

Troubleshooting Client Authentication on Access Rules in ISA Server  
2004 <http://download.microsoft.com/download/9/1/8/918ed2d3-71d0-40ed-8e6d-...>

Microsoft Internet Security & Acceleration Server:  
Partners <http://www.microsoft.com/isaserver/partners/default.asp>

Microsoft ISA Server Partners: Partner Hardware  
Solutions <http://www.microsoft.com/forefront/edgesecurity/partners/hardwarepart...>  
-----

Re: ISA 2006 web proxy scenario

Thanks Phillip.

I neglected to mention that the new consolidated array will be ISA 2006 Enterprise using new hardware. So I will be doing some of the export/import tasks you mentioned above.

.