

## Re: general question on design options

---

*Source:* <http://www.tech-archive.net/Archive/ISA/microsoft.public.isa/2007-10/msg00033.html>

---

- *From:* SMadaras <[SMadaras@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:SMadaras@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx)>
  - *Date:* Wed, 3 Oct 2007 13:42:00 -0700
- 

"Phillip Windell" wrote:

"SMadaras" <[SMadaras@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:SMadaras@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx)> wrote in message [news:D2BB9E6E-786B-4DD8-AB5C-F3F223D94491@xxxxxxxxxxxxxxxxxxxxx](mailto:news:D2BB9E6E-786B-4DD8-AB5C-F3F223D94491@xxxxxxxxxxxxxxxxxxxxx)

David,

I'm running the configuration that you are considering. I have a Cisco 2800 series router with the K9 security package. It's configured as my edge router and handles all of my VPN connections and is configured as my first line of firewall defense. Behind that I have my ISA,

How do you get the VPN connections that terminate on the Cisco to get past the ISA into the LAN? Effectively the people would only be VPNing into the DMZ and not the LAN.

I have three interfaces on the Cisco router, the External, the DMZ, and an Internal. I have configured the External to route only VPN traffic to the Internal and nothing else. The Internal is configured to only allow traffic from approved private subnets. In this configuration both the ISA and the Cisco Internal interfaces sit side-by-side. Of course I could just configure the Cisco to passthrough all isa-kmp, esp and asp traffic to the ISA and let it be handled there, but this just seemed to be more of a burden. (And I'm a segregation nut..)

I agree with Phillip that in many cases this could be just "burning electricity", but even our IT auditors approved of the extra layer of security.

## Re: general question on design options

We've had auditors like that. They base a lot of what they like or don't like on "superstition" and not reality. Such as the superstition that a "Lan with a DMZ is more secure than one without" when the reality is that a LAN with a DMZ is just a LAN that has one more IP Segment and is neither more secure or less secure because of it. The DMZ usually gets in the way of the admin more than the hacker. If I were going to extract information from a LAN the method I would use would work even if they had 15 DMZs between them and the Internet,..they just wouldn't matter at all. Currently in today's Internet with today's type of threats that is exactly the case.

There are situations where they can be solidly justified, but I say that more by "faith" than by seeing a real example of one.

In my setup my "DMZ" really doesn't have anything else other than the ISA sitting on it. I agree that DMZ's are typically unnecessary (if you have a properly configured firewall), but they are sometimes useful for quickly hashing out connectivity issues or trying out something new.

(Also like the fact that I no longer have a single point of failure; if one device fails I can take it the loop and keep on trucking..)

Yes, but you still have to readdress the remaining device to eliminate the DMZ IP Segment when one is removed,...but you can't do that if there are machines that "live" on that segment unless you quickly redesign the access method to them such as putting them on the Public segment or moving them into the LAN and creating Publishing Rules (or Reverse NATs) for it.

You're right, it would not be a transparent failover, but in both failure scenarios (Cisco or ISA) I've narrowed down the reconfigure to maybe three steps, and possibly having all affected clients reboot to pick up the new gateway. We are a small non-profit and don't really have the funds to incorporate the type of equipment you mention below. As such, a 10-15 min interruption in service isn't that big a deal for us when compared to the expense needed to prevent it.

I have the redundancy you mentioned by using ISA2006 and a Watchguard Firebox X. But they run "side-by-side" and are completely independent of each other, and there is no DMZ. The LAN's topology is not disturbed no matter which one "quits" or which one is used for any particular purpose. Some of the key functions are duplicated on each even if not used so either can be a fallback device. I have ISA do most of the actual work because it is just a better product.

The WG is doing the Site-to-site VPN because it has matching devices at the

Re: general question on design options

other end. The ISA handles as the Remote Access VPN because the WG is not cable of using true DHCP for the VPN Clients (and hence DHCP Options and WPAD) and is not capable of filtering access after the connection is made.

Nice, this shows why you're so good at answering peoples questions! =P

--

Phillip Windell  
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-fd6eeb6cfa07/ts\\_rules.doc](http://download.microsoft.com/download/9/1/8/918ed2d3-71d0-40ed-8e6d-fd6eeb6cfa07/ts_rules.doc)

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/hardwarepartners.mspx>

---