

# Re: Firewall and ISA

---

*Source:*

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2007-10/msg02499.html>

---

- *From:* Leythos <[void@xxxxxxxxxxx](mailto:void@xxxxxxxxxxx)>
  - *Date:* Thu, 18 Oct 2007 07:08:22 -0400
- 

In article <#QF8J3WEIHA.1316@xxxxxxxxxxxxxxxxxxxxxx>, itanb@xxxxxxxxxxx says...

see inline

"Leythos" <[void@xxxxxxxxxxx](mailto:void@xxxxxxxxxxx)> wrote in message  
[news:MPG.218049022feeaf89989a68@xxxxxxxxxxxxxxxxxxxxxx](mailto:news:MPG.218049022feeaf89989a68@xxxxxxxxxxxxxxxxxxxxxx)

In article  
<F5B19C59-9099-43F1-B8A4-0BF7AB8CA330@xxxxxxxxxxxxxx>,  
ItanBarmes@xxxxxxxxxxxxxxxxxxxxxx says...

Can you elaborate on the problem with the low end firewall.  
Basically it  
blocks the ports i am telling him to block. What else would  
i want him  
to do?

Maybe I can intrude here:

1) Linksys uses NAT to protect you, claiming it's a firewall, but NAT is  
a ROUTING method, not a firewall function.

i guess what you mean by that is that it would be easier to hack to my  
network. Do you know any resource about the difference between the two  
methods, i would like to know more about this.

Google – look for NAT and then look for firewall – if you check, NAT  
does not have any firewall features, it has only ROUTING features.

2) Firewalls protect by doing a lot of things (at least todays firewalls  
offer a lot) – they filter content out of HTTP and SMTP sessions, they  
detect attacks and block the intruders IP, they provide detailed logs,  
they act as VPN Tunnel endpoints for branch offices and mobile users...

## Re: Firewall and ISA

I don't need VPN and mobile users can use RWW, i am aware of all there great possibilities, i just dont want to spend money on something that i use 10% of.

You mean you would not use:

- 1) Auto detection of multiple types of attacks with automatic blocking?
- 2) Filtering of users HTTP sessions for content you don't want them to download or be exposed too?
- 3) Filtering of SMTP (inbound email) sessions for bad file types or malicious headers or other files that you don't want on your server?
- 4) Filtering of FTP sessions?
- 5) Full access to the network for maintenance, remotely, over a VPN, so that you don't have to use Remote Desktop for maintenance – since RD can screw with your installation of patches?
- 6) Something to protect your NETWORK that is not on Windows non-dedicated server (meaning that ISA is not certified on a non-dedicated box).
- 7) Complete inbound and outbound logs with real-time monitoring showing ALL connections source/destination?
- 8) Ability to handle more than 1 public IP mapped to your LAN or a REAL DMZ network?
- 9) How about a real DMZ network that is isolated from your LAN?

Your Linksys won't handle the traffic of a fast DSL (or slow cable) connection without problems – I've seen a small sorority with 30 residents swamp Linksys routers causing them to reboot or fail until power cycled – a better unit, like the FVS-318 and the DFL-700 handled the traffic without a problem.

Are you saying that in addition to the ISA i need to get a new router? The Linksys is acting as a modem / router / AP / firewall. Don't forget that i only have 1 server and 4 desktops.

No, the "Router" works fine as router. ISA would work, but it's not certified on a non-dedicated box. The Linksys is a small unit, for very small shops. As for wireless, I hope you secured it with WPA-PSK ro WPA2.

Re: Firewall and ISA

Re: Firewall and ISA

You seem to think that your 1 server and 4 computers plays into the equation as significant for protection, it doesn't – you need to consider LOSS OF DATA and the cost of that. You could have 1 server and 1 PC and your loss, if it was SSN's or Credit Card info, or just your Quick Books files, could cost you thousands instantly, not to mention loss of company info or project info....

It's not about the hardware, that doesn't mean anything, it's about the cost of the data your business uses.

--

Leythos

- Igitur qui desiderat pacem, praeparet bellum.
  - Calling an illegal alien an "undocumented worker" is like calling a drug dealer an "unlicensed pharmacist"
- spam999free@xxxxxxxxxx (remove 999 for proper email address)

.