

## Re: OWA\_Frontend\_Firewall

---

*Source:*

<http://www.tech-archive.net/Archive/Exchange/microsoft.public.exchange.admin/2005-04/msg00406.html>

---

- *From:* "Rich Matheisen [MVP]" <[richnews@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:richnews@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx)>
  - *Date:* Sat, 02 Apr 2005 21:09:13 -0500
- 

"Mark Arnold [MVP]" <[mark@xxxxxxx](mailto:mark@xxxxxxx)> wrote:

>On Fri, 1 Apr 2005 12:11:19 -0600, "Luke" <[nomail@xxxxxxx](mailto:nomail@xxxxxxx)> wrote:  
>  
>>company policy says that i can NOT have any ports open on the firewall from  
>>the WAN to LAN..  
>>  
>>so i have to put OWA in the DMZ and have a limited number of ports open from  
>>the OWA server in the DMZ to the exchange server and DC's on the LAN  
>>  
>Inflexible policies, dontcha just love them.

And you think that allowing an encrypted stream of data from the Internet to a Microsoft server on your LAN is secure? I think you've drunk the kool-aide.

>Well, the article gives you the guidance there.  
>You might still want to consider using the ISA in the DMZ (where the  
>ISA is a workgroup box not joined to the domain) and that way you only  
>open 443 from Internet to ISA and then 443 from the ISA to the  
>Exchange,

If you have any form if IDS you'll do a lot better terminating the SSL connection at the ISA srver (or whatever you use to provide the SSL). You can't see inside an encrypted data stream.

>either direct to the BE or to an FE (choice is yours on that  
>score; assuming you only have one BE)  
>It's certainly a lot safer than opening several ports to the FE and to  
>GCs between a DMZ and a firewall.  
>Present them with the options and show them the results of their  
>policy.

Web-mail is insecure, too. If the policy takes that risk into account it probably already knows that firewalls are not impermiabile and that a "real" DMZ wouldn't allow any of the stuff needed to permit access to a mailbox server from outside the network.

—  
Rich Matheisen  
MCSE+I, Exchange MVP  
MS Exchange FAQ at [http://www.swinc.com/resource/exch\\_faq.htm](http://www.swinc.com/resource/exch_faq.htm)  
.

---

- **References:**
  - ◆ **OWA Frontend Firewall**
    - ◇ From: Luke
  - ◆ **Re: OWA Frontend Firewall**
    - ◇ From: Mark Arnold [MVP]
  - ◆ **Re: OWA Frontend Firewall**
    - ◇ From: Luke
  - ◆ **Re: OWA Frontend Firewall**
    - ◇ From: Mark Arnold [MVP]
  - ◆ **Re: OWA Frontend Firewall**
    - ◇ From: Luke
  - ◆ **Re: OWA Frontend Firewall**
    - ◇ From: Mark Arnold [MVP]
- Prev by Date: **Re: Why can't I telnet in to SMTP?**
- Next by Date: **Re: Multiple Routing Groups**
- Previous by thread: **Re: OWA Frontend Firewall**
- Next by thread: **Multiple Routing Groups**
- Index(es):
  - ◆ **Date**
  - ◆ **Thread**