

## Re: OWA connectivity

---

*Source:*

<http://www.tech-archive.net/Archive/Exchange/microsoft.public.exchange.admin/2006-11/msg02051.html>

---

- *From:* T-Kay <[TKay@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:TKay@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx)>
  - *Date:* Fri, 17 Nov 2006 11:35:01 -0800
- 

As I was driving home after my last post I was half expecting you to reply in this fashion.

First though I'd like to admit I made a mistake in talking about SMTP port 25 while we were discussing OWA which should be communicating HTTPS over port 443.

Secondly opening these ports from your DMZ towards your LAN is not insecure it is controlling what goes through to your LAN from your DMZ. Remember you're still allowing only port 443 towards your DMZ from the Internet. If you do not use this setup you're allowing port 443 towards your LAN and then from that on ALL ports are available. In my explanation only the ports mentioned will be available. On top of that I'd like to add that I would use secure LDAP in this setup over port 636 instead of port 389.

If you wish I can explain this better in a visio or some other picture, because what you are describing is far more dangerous than allowing OWA only through a DMZ. A DMZ is primarily brought to life to support publishing of websites. Whether or not you use a proxy server in this setup is up to you. If you have several websites to publish then it is preferable, but if you're only using OWA it could be more secure, but does not add much value since you still have your double defense firewall.

I have a lot of experience in setting up DMZ's firewalls and working with Exchange 5.5 2K and 2K3 with OWA's RelayServers and the like. I've not yet met a firewall specialist that would say yes to opening port 443 or 80 towards your LAN.

Tom

"Ed Crowley [MVP]" wrote:

Some of those are extremely dangerous ports. What you're suggesting as a secure proposal is opening up your entire Active Directory, Windows and Exchange infrastructure to a host on your DMZ. That is foolish in the opinion of myself and many, many others. Allowing SSL port 443 only to one host on your intranet, preferably through a proxy server, is far more secure and much easier to monitor and maintain.

--

Re: OWA connectivity

Ed Crowley  
MVP – Exchange  
"Protecting the world from PSTs and brick backups!"

"T-Kay" <TKay@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message  
news:4C1D431E-8081-4A7E-900B-AF16D437937A@xxxxxxxxxxxxxxxxxxxx

Exchange uses a different port to communicate with other exchange servers.  
Setting up an Exchange server in your DMZ will allow you to accept SMTP  
port  
25 traffic safely and only allow ports 691, 389, 3268, 88 from the front  
end  
server towards the internal exchange server and DC.

Allowing port 25 towards your LAN is asking for trouble.

I also understand you only worked with ISA server which, even though I  
think  
ISA is a good product, I feel is not a true firewall and should be used as  
proxy server only.

Tom

"Ed Crowley [MVP]" wrote:

I'm extremely confident that I can tell you that your advice is  
contrary  
to  
the opinion of the vast majority of Exchange MVPs for the  
reasons in my  
other post among others.

--

Ed Crowley  
MVP – Exchange  
"Protecting the world from PSTs and brick backups!"

"T-Kay" <TKay@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in  
message  
news:80C81209-F5C4-4E96-836E-0DA3907BF6CA@xxxxxxxxxxxxxxxxxxxx

Bryan,

Pointing directly to your internal mail server  
is not something I would  
expect from a firewall professional. Your  
setup with a DMZ and a front  
end  
OWA server is perfect. The reason for the  
connection problems could be  
any

Re: OWA connectivity

number of things. First I would check your firewall logs to check connectivity and rule out the possibility of a firewall misconfiguration.

I would need more information to your problem to be more helpful.

"Bryan" wrote:

I have recently been having trouble connecting to OWA. My configuration has a front-end server in a DMZ that I was hitting for OWA but I was told by my firewall vendor to change my rule to point directly to my back-end box on my LAN. Is this recommended? Any idea why I would have occasional trouble connecting to OWA when I was point to my front-end server?

Thanks.

--

Bryan