

SecurityFocus Microsoft: Re: Ye Olde OWA Topic (Was RE: Website inside or outside domain)

## Re: Ye Olde OWA Topic (Was RE: Website inside or outside domain)

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ms/2003-02/0079.html>

---

**From:** Steve ([securityfocus@delahunty.com](mailto:securityfocus@delahunty.com))

**Date:** 02/18/03

From: "Steve" <[securityfocus@delahunty.com](mailto:securityfocus@delahunty.com)>

To: "shannong" <[shannong@texas.net](mailto:shannong@texas.net)>, "Henry Sieff" <[hsieff@orthodon.com](mailto:hsieff@orthodon.com)>, <[focus-ms@securityfocus.com](mailto:focus-ms@securityfocus.com)>

Date: Tue, 18 Feb 2003 14:58:43 -0500

I submit that you give up more functionality you desire for OWA than security you gain by requiring access via the VPN. In other words requiring the VPN client to get to the OWA box kills most of the benefit of using OWA in the first place. For example your employee is in an airport and wants to check his/her email, can easily be done via OWA but not easy if they have to have a VPN client configured. I have seen a solution that worked well using Citrix to provide a Java web interface to the full Outlook email client.

STEVE

----- Original Message -----

From: "shannong" <[shannong@texas.net](mailto:shannong@texas.net)>

To: "Henry Sieff" <[hsieff@orthodon.com](mailto:hsieff@orthodon.com)>;

<[focus-ms@securityfocus.com](mailto:focus-ms@securityfocus.com)>

Sent: Saturday, February 15, 2003 1:08 PM

Subject: RE: Ye Olde OWA Topic (Was RE: Website inside or outside domain)

Of course, if you're using a VPN device then there's no need to deal with any DMZs or any other separation of OWA from your inside network. You just VPN to the network and then connect to OWA/Exchange which resides "next" to Exchange. This of course requires client side software and configuration.

I'm working for a customer right now where we are deploying a reverse-proxy that does authentication of the users on the Internet before allowing them access to any inside web servers. All requests are re-written to look as though they came from the proxy. This is probably the best method to deploy web servers to the Internet securely.

Of use your firewall to authenticate. Although users still access the servers directly, the firewall can authenticate the user before

Re: Ye Olde OWA Topic (Was RE: Website inside or outside domain)

SecurityFocus Microsoft: Re: Ye Olde OWA Topic (Was RE: Website inside or outside domain)

allowing them to access the services. Checkpoint and Pix firewalls can do this.

In Pix 6.3 due out in March, the Pix will be able to do secure authentication for HTTP and HTTPS before allowing access.

-----Original Message-----

From: Henry Sieff [mailto:[hsieff@orthodon.com](mailto:hsieff@orthodon.com)]  
Sent: Thursday, February 13, 2003 10:24 AM  
To: 'KEITH KOOYMAN'; [focus-ms@securityfocus.com](mailto:focus-ms@securityfocus.com)  
Subject: Ye Olde OWA Topic (Was RE: Website inside or outside domain)

> -----Original Message-----

> From: KEITH KOOYMAN [mailto:[pcsolutions101@hotmail.com](mailto:pcsolutions101@hotmail.com)]  
> Sent: Wednesday, February 12, 2003 3:00 PM  
> To: [focus-ms@securityfocus.com](mailto:focus-ms@securityfocus.com)  
> Subject: RE: Website inside or outside domain

>

>

> As I have followed this thread I have noticed that no one has

> addressed the

> similarities between this situation and OWA. Essentially,

> this is much the

> same scenario, where a public web server is in the DMZ and

> the question is:

> How do I allow access to the back-end Exchange Server?

The same logic applies: IF you must do ANY of these, then you have to establish some sort of control over access to the OWA server itself;

it

can't just be a public web server. You can do this through a VPN, with the

OWA server being at one end and your pre-approved clients being at the other

end. Put the OWA server on its own segment with whatever VPN device you

choose, and then you can open up holes between OWA and the backend, since

you have established a reasonable level of assurance that the only traffic

coming into that segment is legit.

> You can:

> 1. Put a firewall between the DMX and the LAN (many firewalls have a

> preconfigured DMZ so a second firewall is not needed) and

> open up so many

> ports from the DMZ to the LAN that the firewall is useless =

> the official

> Microsoft solution

Bad (but mitigated by the suggestion above).

Re: Ye Olde OWA Topic (Was RE: Website inside or outside domain)

SecurityFocus Microsoft: Re: Ye Olde OWA Topic (Was RE: Website inside or outside domain)

- > 2. *You can leave the front-end in the DMZ and use pass-through authentication which takes web traffic straight to your back-end = not desirable*

Might as well not even use OWA at that point; I mean, its not like the interface is that great.

- > 3. *Multi-home the front-end public web server, use TCP/IP filters, IPSEC and firewall rules to filter, authenticate and encrypt traffic going to the back-end; a good idea but time consuming and difficult to set up*

Horrible horrible horrible. At that point, you are essentially putting ALL of your faith in the integrity of the software and in your ability to manage the rule sets. All it takes is one mistaken mouse-click and presto, your web server is now routing from your DMZ to your LAN. And, you are also implying that your public web server can be hardened enough to make it a firewall (that is, a device enforcing a boundary between different trust levels); it can't be done.

- > 4. *Move the front-end public web server to the LAN = not desirable*

Again, why not just move the Exchange server to the DMZ and ditch OWA; same level of security, better interface, less moving parts.

- > 5. *Use a third party hybrid solution = expensive*

Depends what you mean. Add an additional leg to your network, throw in a vpn device (and I think you can probably even use PPTP running on a hardened Win2K server and get away with it; at least you get some benefit) and your basically done. You can do it all on \*BSD too. Doesn't have to be expensive, although the judging factor is how much the security is worth to you.