

RE: Protecting an Exchange server?

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2004-05/0262.html>

From: Jose Enrique Diaz Jolly (*enrique.diaz_at_cbbanorte.com.mx*)

Date: 05/22/04

Date: Fri, 21 May 2004 17:52:27 -0500

To: "Chris Santerre" <csanterre@MerchantsOverseas.com>

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

> **From:** Chris Santerre [<mailto:csanterre@MerchantsOverseas.com>]

> **Sent:** Tuesday, May 18, 2004 10:34 AM

> **To:** Jose Enrique Diaz Jolly; Mark G. Spencer;

> *security-basics@securityfocus.com*

> **Subject:** RE: Protecting an Exchange server?

>

> *Jose's recomendation below are quite good. We use Sendmail*

> *box in a dmz. Of course I use Spamassassin. (See link in*

> *sig!) Email has to go thru firewall twice before entering*

> *internal exchange server. IMHO no microsoft box should ever*

> *be attached directly to the internet.*

>

> *You can setup aliases to users, then a static route to*

> *internal server. This way you don't have to have actual users*

> *on the outside box, and the outside box will handle*

> *rejections. There are a few other neat things you can do as well ;)*

>

> *Jose, I'm interested in your secure OWA setup. Is there more*

> *info you can send me off list? Currently users outside the*

> *company have to VPN in to check email. I'd rather just shut*

> *that off :)*

>

Well, it is quite simple in principle. It depends on how much are you willing to pay. If your MS Network security is a must in your strict policies and rules and you have strict enforcement of MS security conventions, perhaps this is not a solution for you. Why? A few facts before:

- My MS Network is only my major office environment but not a productive or operational one.
- All my ops are held on different platforms.
- None MS is directly exposed to the internet, neither through strong firewalling.
- This solution requires (there may be other that do not) downgrade certain methods of authentication on windows as NTLM can not be proxied. This is only for the "site" on IIS serving OWA.
- Have a strong firewall policies and schemes?

SecurityFocus BASICS: RE: Protecting an Exchange server?

If you have no trouble with this, then the solution is amazingly simple.

The solution is based on the so called "Reverse Proxy". Usually, a proxy is one point to go outside from a restricted network; on the other hand, a reverse proxy is the oposite: a single entry point to a server or a network, beyond the DMZ in this case.

Apache has some features to do so. Thus, we may build a proxy (or a reverse proxy) only with a web server.

The linux box has strong security. All ports are closed, no services except those really necessary are on. The necessary ports for this host are just a few. NTP to a internal or DMZ server. SSH only from a few internal or DMZ servers or hosts. HTTP and HTTPS listening to the Internet. Domain client should be able to query either external or DMZ controlled DNS, to resolve the OWA server, and ability to resolve (forward) reverse names for requestors.

First step is set up a Linux box in order to serve Apache. You should setup your box as if you were to serve web pages. Define your "site" where you are willing to serve owa ie.: <http://webmail.domain.com/exchange>
Define your secure site also: ie <https://webmail.domain.com/exchange>
Write rules for redirect (I recommend use of mod_rewrite from http to https site). Make sure you have your certificate for SSL so you can assure your channel. If you prefer you can buy a certificate to make your site certificated and trusted.

Remember that the main commitment of this certificate is to permit encription for https.

Make sure you can resolve through your DNS the webmail.domain.com name.

Prepare your exchange's IIS to allow standard authentication, NTLM is not proxable. So we have to use standard.

If you prefer, you can create also a certificate to permit https between proxy and owa.

Regular http should work, but it is upon you. We decided to use a double encrypted communication.

On the https virtualhost configuration make, using ProxyPass and ReverseProxyPass sentences point to your "virtual server"

The very same name you are using for the front end to the internet. This is in order to mask the real owa name.

Once you have all your rules written start everything and voilà you have a proxied owa!

Details:

The Linux Box:

The solution, when built was with Red Hat 7.2 (Enigma); Tue software used was:

```
apache_1.3.26
mod_ssl-2.8.10-1.3.26
openssl-0.9.6g
```

On the Apache's config file:

SecurityFocus BASICS: RE: Protecting an Exchange server?

```
## SSL Support
<IfDefine SSL>
Listen 80
Listen 443
</IfDefine>
```

Between the collection of modules included on your apache you should make sure you load:

```
rewrite_module mod_rewrite.c
proxy_module mod_proxy.c
Ssl_module mod_ssl.c
```

Create a virtual host on your apache:

```
<VirtualHost webmail.mydomain.com:80>
ServerName webmail.mydomain.com
ServerAdmin you@mydomain.com
DocumentRoot /home/httpd/htdocs.webmail ;; May not exist.
CustomLog /var/log/httpd/extended_log.webmail extended ;; You decide wheter use regular or extended
ErrorLog /var/log/httpd/error_log.webmail
RedirectMatch ^/(index.html?)$ https://webmail.mydomain.com/exchange/ ;; Work around for easyness of URIs
RedirectMatch ^/exchange$ https://webmail.mydomain.com/exchange/
</VirtualHost>
```

```
<VirtualHost webmail.mydomain.com:443>
ServerName webmail.mydomain.com
ServerAdmin you@mydomain.com
DocumentRoot /home/httpd/htdocs.webmail ;; May not exist.
CustomLog /var/log/httpd/extended_log.webmail extended ;; You decide wheter use regular or extended
ErrorLog /var/log/httpd/error_log.webmail
RedirectMatch ^/(index.html?)$ https://webmail.mydomain.com/exchange/ ;; Work around for easyness of URIs
RedirectMatch ^/exchange$ https://webmail.mydomain.com/exchange/
```

```
ProxyPass /public/ https://webmail.mydomain.com/public/ ;; Here is where the magic is along with one
ProxyPassReverse /public/ https://webmail.mydomain.com/public/ ;; more little trick on the /etc/hosts file
ProxyPass /exchweb/ https://webmail.mydomain.com/exchweb/ ;;
ProxyPassReverse /exchweb/ https://webmail.mydomain.com/exchweb/ ;;
ProxyPass /exchange/ https://webmail.mydomain.com/exchange/ ;;
ProxyPassReverse /exchange/ https://webmail.mydomain.com/exchange/ ;;
</VirtualHost>
```

On the /etc/hosts you should add an antry to make the little mischief to the resolver. The real name of your exchange doesn't really care. We make a match between the name of our webserver and the exchange server's address:

```
192.168.1.5 mailweb mailweb.mydomain.com
```

182.168.1.5 is the IP address of our private exchange server, while mailweb.mydomain.com is the apache's server name. Also you have to ensure that the resolver acts in this way, modifying if necessary the order of

SecurityFocus BASICS: RE: Protecting an Exchange server?

search (resolve) a name:

Make sure the order of search in /etc/nsswitch.conf is:

hosts: files dns

Basically that's all.

Hope this helps you.

Ethical Hacking at the InfoSec Institute. Mention this ad and get \$545 off any course! All of our class sizes are guaranteed to be 10 students or less to facilitate one-on-one interaction with one of our expert instructors. Attend a course taught by an expert instructor with years of in-the-field pen testing experience in our state of the art hacking lab. Master the skills of an Ethical Hacker to better assess the security of your organization.

Visit us at:

http://www.infosecinstitute.com/courses/ethical_hacking_training.html
