

Re: Mail server security – best practices?

Source: <http://unix.derkeiler.com/Newsgroups/comp.unix.bsd.openbsd.misc/2006-04/msg00135.html>

- *From:* jKILLSPAM.schipper@xxxxxxxxxxx
 - *Date:* 28 Apr 2006 00:44:31 GMT
-

sealinux@xxxxxxxxxxx wrote:

jKILLSPAM.schipper@xxxxxxxxxxx wrote:

It's not really possible to have a mail store that is not, at least indirectly, accessible from the wide internet (save in special cases).

That was my feeling as well, hence the quandry.

FWIW, IMHO it's most important to separate the web scripts from anything important. Both BIND and qmail are pretty secure, and while Apache itself is quite secure, PHP for instance isn't.

I've since acquired a separate machine to run Apache and PHP on. I'll have two servers in the DMZ then, one running Qmail and BIND, the other running Apache and BIND.

You could put a mail forwarder in the DMZ ('public servers'), if so inclined, but I'd recommend setting up the webserver in it's own private DMZ, and mail on a server that's 'half-internal' in that you seem not to need stored mail being accessible from the outside.

I can access the stored mail from the outside using OpenVPN. How wise is it to trust that? I still employ IMAP-SSL on the private server, though.

OpenVPN is not that bad, security-wise, and has an option to require each message to be stamped with a certain key (not at the appropriate computer now – see tls-auth).

Stock IPsec or OpenSSH is better, but tls-auth makes exploiting problems very difficult.

Re: Mail server security – best practices?

For maximum protection, configure a mail forwarder in the DMZ – MTAs are pretty secure, but spam and virus scans often use weird programs that are not quite as well-tested.

Let me see if I understand. The machine running Qmail in the DMZ would be set to forward incoming mail to my private server, also running Qmail, behind the firewall. The former would simply act as a conduit to the latter, which would deliver mail to the user's home directories. This would involve punching a hole in the firewall to allow connections to port 25 on the private server, but that can be locked down fairly tightly with pf rules. The main thing is for stuff I want kept private to not be widely available.

That's indeed the point.

Note that a compromised mail gateway would still lead to an attacker being able to read incoming mail; but not mail that was already stored.

Whether or not this is worth the trouble depends on quite a few things. I personally run Postfix with amavisd, clamav, spamassassin, and a selected subset of helper programs (especially, none of the weird/old archive programs that amavisd likes to have, and that seem to have been written before the concept of buffer overflow was widely known and/or cared about). Everything is chrooted, and the whole thing runs on OpenBSD.

Under these circumstances, I don't really see the need for a mail gateway. Some find it useful, though.

DNS could be kept where you want it, though the risk of a nasty DoS is less if you put it on a separate machine.

(Having visions of my wallet getting lighter and lighter and lighter . . .) Seriously, thank dog I'm running OpenBSD. There's no way I could afford the big iron and licenses required to run 'Doze.

Pointing all your machines to the web server, which is probably the easiest to compromise, may allow an attacker to effectively DoS you by shutting down BIND.

However, I would personally not mind sharing the mail gateway and the BIND daemon – sure, separating them would be better, but your cost argument is sound.

Re: Mail server security – best practices?

Re: Mail server security – best practices?

OTOH, you might want to run a DNS daemon on both DMZ'ed servers if said DNS is required for the proper functioning of a/your domain. Then again, a free ZoneEdit.com account (or similar) is likely to provide a more valuable backup.

Joachim

.