

## RE: Firewalling with a webserver and DB

*Source:* <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2001-07/0030.html>

---

*From:* Tommie Porter ([tporter at xcaliber.com](mailto:tporter@xcaliber.com))

*Date:* 07/18/01

Matt,

But the DB on the internal network. You only put servers on the DMZ that are DIRECTLY accessible from the Internet(or any other insecure network). Put in the necessary rules to allow the webserver to talk to the DB on the internal network. Only give it access to what it needs.

For your FW rules, only allow port 80 into your DMZ IF all you have are webserver(s) on there. You have to allow all ports greater than 1023 out though. As clients computers will use these ports dynamically to talk to your server on port 80.

TP

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

From: Bartel, Matt [[mailto:Matt.Bartel at qg.com](mailto:Matt.Bartel@qg.com)]

Sent: Tuesday, July 17, 2001 1:33 PM

To: '[security-basics at securityfocus.com](mailto:security-basics@securityfocus.com)'

Subject: Firewalling with a webserver and DB

If I am running a setup as follows:

Internet<->Firewall<->DMZ<->Firewall<->Internal Network

and I am running webserver(s) in the DMZ that need to pull info out of databases (that hold confidential information), where is the best place to put the db's??? If I put them in the internal network, I would have to make a rule to allow the webserver(s) to access the db's through the FW (which defeats the point of the FW)...if I do not allow the webserver(s) to go through the FW, then they cannot access the db's, unless I would put them in the DMZ...What is the safest way to do this? What would basic, sample rules look like that would be optimal in this type of a setup be?

Also, one other really dumb question, while I'm on a roll:

I know that I should \*only\* allow port 80 into the DMZ, but do you allow \*ALL\* ports to go out??? Doesn't the webserver use all different local ports to talk out onto the Internet? If I wanted to do the following (assuming there is no internal network):

Internet<->Firewall<->Webserver

Can I allow \*only\* port 80 to run through the FW to the Internet (both ways)? I am using IIS 5, and I am under the belief that IIS opens ports (source ports???) on the local machine to talk out to the world...If I only

RE: Firewalling with a webserver and DB

SecurityFocus BASICS: RE: Firewalling with a webserver and DB

allowed 80 to go out, wouldn't that effectively block the webserver from talking onto the net, since it picks high ports (like 5000, or whatever)?

Thank you.

–Matt

---

- *Vorherige Nachricht:* Sam T: "Re: oracle question"
- *Vielleicht als Antwort auf:* Bartel, Matt: "Firewalling with a webserver and DB"
- *Nächste im Thread:* Bell, James (AZ76): "RE: Firewalling with a webserver and DB"
- *Nachrichten sortiert nach:* [ Datum ] [ Thread ] [ Subject ] [ Autor ] [ Attachment ]