

Re: ATTN Tony Whitmore please

Source: <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2002-10/5854.html>

From:

Date: 07/28/02

Date: Sun, 28 Jul 2002 21:52:26 +0100

Hi again Tobamore,

I've not used your router before, but I've just been looking up www.edimax.com and finding out about it.

The full manual is available for download in PDF from <http://www.edimax.com/DocLib/Manual/English/BR6004+ ME.pdf>. It does seem that the router is configured with ports 80 and 23 open on the public interface to allow remote configuration. This does seem a little insecure, but maybe the manufacturers were selling the product for use in firewalled corporate networks.

Pages 54 to 56 of the manual seem to hold the relevant information about how to stop this. Basically, log into your router using the ARM interface. Choose Configuration -> Advanced -> IP Filter. Here you have the opportunity to add or delete rules to your hearts content. In your situation you would want to "discard" packets for ports 23 and 80 from any remote IP address, or perhaps better yet accept packets for ports 23 and 80 from just your computer's local IP address. You can make sure your router password is strong by changing it under System Tools -> Change Password. Remember to rescan the ports after you have made configuration changes. I'm not sure of the exact details of this, but I haven't got the interface in front of me.

There may be another method. On page 42 the manual mentions about consequences of redirecting ports 80 or 23, and having to remap the ports to continue to allow remote access. It may be that under the Port Address Translation you could add rules forwarding ports 80 and 23 to non-existent local IP address, without remapping the services as suggested. The inference from the manual is that this would prevent access to those ports from external IP addresses. Again, if you try this be sure to scan your router afterwards to check.

Alternatively there may be an "allow remote administration" option which I've missed in the manual.

The manual doesn't mention what software is running underneath the web interface on the firewall, and how that can be configured. It may be based on linux, in which case you can use the ipchains tool to configure your

Re: ATTN Tony Whitmore please

comp.security.firewalls: Re: ATTN Tony Whitmore please

firewalling much more easily than through the web based interface. It could be a proprietary OS, which would have its own commands, and may not be as easy to configure.

If those ideas fail, the specifications on the website say that your router has ethernet upstream, so you could use the linux based firewall machine idea that I suggested in my last post. You would only need an old 486 machine with two ethernet cards, a few MB of RAM and a 100–500MB HDD. You could run Smoothwall or IPCop happily from that. Coyote Linux and floppyfw are both based on floppy disks and don't require a HDD at all! Smoothwall and IPCop both close all external ports by default, and so would restrict telnet and http access to just your local network. But I guess that really wouldn't be a preferred option!

Cheers,

Tony

"Tobamore" <tobamore@DELETE_MEyahoo.co.uk> wrote in message news:h4g8ku0rliocgtojhg5457uem2219v7611@4ax.com...

> *On Sun, 28 Jul 2002 16:28:02 +0100, "Tony Whitmore"*

> *<tony_whitmore@nospamhotmail.com> wrote:*

>

> *>You may be able to allow connections to the ports*

> *>only from your local ethernet interface. It should be possible to add a*

> *>"deny" rule to close the ports on your public interface, but leaving them*

> *>open on your local network. In addition you could restrict the range of*

> *>valid IP address to just your computer's IP address to stop anyone else*

> *on*

> *>your local network attempting to connect.*

>

> *Thanks Tony and Scott for your help guys. :-)*

>

> *I was wondering though Tony, could you suggest a simple way of doing the*

> *above? My router is an edimax br6004+ model and the manual isn't too*

> *clever,*

> *at least not for an idiot like me. :-)*

>

> *Thanks again guys, you are most helpful.*

>

> *#*

> *T.*

>

-
- ***Next message:*** [Duane Arnold: "Re: Firewall Newbie Help"](#)
 - ***Previous message:*** [Use.Netuser1.cs: "Re: Blocking Kazza"](#)
 - ***In reply to:*** [Tobamore: "Re: ATTN Tony Whitmore please"](#)
 - ***Next in thread:*** [: "Re: ATTN Tony Whitmore please"](#)
 - ***Reply:*** [: "Re: ATTN Tony Whitmore please"](#)
 - ***Messages sorted by:*** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)