

RE: [fw-wiz] Pix 501 configuration question

Source: <http://www.derkeiler.com/Mailing-Lists/Firewall-Wizards/2003-11/0033.html>

From: Josh Welch (jwelch_at_buffalowildwings.com)

Date: 11/07/03

To: <firewall-wizards@honor.icsalabs.com>

Date: Fri, 7 Nov 2003 11:00:31 -0600

Adam Lang said:

- > *This is probably an extremely basic question for this forum, but in an*
- > *hour of looking I haven't found a better forum to ask in, except paying*
- > *multiple hundreds of dollars to call up Cisco and ask them.*
- >
- > *I'm a total firewall newbie, and have just set up my first one for my*
- > *company, a Pix 501. I think I did a fairly good job of it, all things*
- > *considered, but there's one thing that I just can't figure out.*
- >
- > *A secondary company web server is behind the firewall, as are our*
- > *secondary DNS and two publicly available WebDAV servers. These*
- > *machines have been given one-to-one NAT... 123.456.789.195 maps to*
- > *192.168.1.195, for example, for the web server. This works fine from*
- > *the outside... anyone can connect to 123.456.789.195 on the web port*
- > *(and can't connect on any other port). And from the inside, of course,*
- > *anyone can connect to 192.168.1.195 on any port. However, I want my*
- > *fellow employees to be able to connect to 123.456.789.195 from INSIDE*
- > *the firewall. Hacks like the name-server-substitution stuff (where the*
- > *Pix substitutes 192.168.1.195 for the 'real' address when the lookup*
- > *passes through the firewall) are just not going to cut it.*
- >
- > *Is this possible? Why doesn't it work in the first place... is there*
- > *something inherently insecure about allowing people from inside to*
- > *connect to an inside machine's external ip? The pix is*
- > *123.456.789.195, and I can't imagine why it can't talk to itself. Do I*
- > *need to set up some sort of default routing? Do I need to somehow make*
- > *a rule translating 123.456.789.195 to 192.168.1.195 on the inside, even*
- > *though the setup tool doesn't appear to allow you to do that? (Maybe I*
- > *need to do it from the command line?) Do I need to ditch the Pix*
- > *because it just can't do this? (Please say no.)*
- >
- > *Thanks in advance for your help.*
- >
- > *--Adam Lang*
- >

I think that this is a matter of the Pix not being willing or able to route traffic back to itself. You might be able to make another firewall do it,

Firewall-Wizards: RE: [fw-wiz] Pix 501 configuration question

but its hard to say. We run iptables, and when we had a similar setting to yours, we had an internal DNS server so that the box was referenced by its private IP internally and its public IP externally. I don't remember if we did that because it wouldn't work, or because it was less complicated, but I think you're going to have to do it this way.

Josh

firewall-wizards mailing list
firewall-wizards@honor.icsalabs.com
<http://honor.icsalabs.com/mailman/listinfo/firewall-wizards>