

Re: Firewalls – Reviewed

Source: <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2005-06/0323.html>

From: Walter Roberson (roberson_at_ibd.nrc-cnrc.gc.ca)

Date: 06/15/05

Date: 15 Jun 2005 17:45:50 GMT

In article <1118853724.975022.111700@g14g2000cwa.googlegroups.com>, neophite <jpbaca02@comcast.net> wrote:

:I also understand DNS and it's functionality, however, it's not true
:that it runs specifically on the inside to forward outside.

I must have missed the posting in which anyone said that it did?

: I need a

:NS on the outside because I am "primary" for my domain, therefore the
:need to have a secured DNS server on the outside of my firewall, or
:part of the firewall.

What you want is not really a DNS server on the outside: what you want more is a DNS server on a DMZ ("Delimeterized Zone") — something that can be –reached– from the outside, but has its ports secured by the firewall, and which can only reach to the inside systems to the extent that you have specifically configured.

:Same goes for my SMTP traffic. I host my MX record, therefore need a
:secure SMTP server on the outside.

Again, not on the outside, on a DMZ.

You will see DMZ listed against quite a few low–end devices, but in many of the low–end devices, "DMZ" is just a way of saying, "an address which is not subject to the firewall protections, and which is expected to have been secured some other way." The "DMZ" on such devices might operate in public IP space, or might operate in the private NAT'd IP space, but on the low–end devices there often is little or no barrier between the "DMZ" and the "inside".

A proper DMZ requires an extra interface (or at least use of VLANs) and mechanisms for seperately configuring the interactions between outside and DMZ, outside and inside, and DMZ and inside.

I do not happen to be familiar with any consumer–class firewalls that provide a real DMZ. There are probably some out there; I just don't know of them.

comp.security.firewalls: Re: Firewalls – Reviewed

Earlier I mentioned the Cisco PIX 501: it does NOT have DMZ capability (the Cisco PIX 506/506E does, but only via VLANs; the lowest commonly-available PIX model with separate interfaces is the 515 and 515E.)

--

History is a pile of debris

-- Laurie Anderson