

## [fw-wiz] \*\*\*SPAM\*\*\* Re: IPv6 support in firewalls

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Firewall-Wizards/2007-08/msg00042.html>

---

- *From:* Dave Piscitello <dave@xxxxxxxxxxxx>
  - *Date:* Thu, 23 Aug 2007 17:06:55 -0400
- 

I'm sorry, but you are not using the term end-to-end in the correct context.

End-to-end has less do with addressing and more to do with where you put functionality. Read Saltzer, Reed and Clark's article on End to end principles in system design (ACM) or some classic articles by David Cheriton, et. al.

End-to-end was directed at the notion of "smart connection endpoints, dumb network", as opposed to a telephony model of "smart network, dumb endpoints (phones)".

Today, very few end user applications and connections are end-to-end addressed. Look at SSL VPNs. Look at many web or other application data centers.

We have far more "box in the middle" configurations than end-to-end addressable connections today, and as my respected colleague, Craig Melson has already stated so elegantly

"One of the great things about the perceived scarcity of IPv4 space on the Internet is that it finally forced most of the institutions that were still using public addresses for everything with an Ethernet port in it to implement NAT."

Almost any firewalled configuration uses IP masquerading and that's hugely important. Do you really think it's better to assign public address space behind firewalls? Do you really want everyone to know every IP address block your organization uses internally by querying an RIR?

These combined are reasons to implement IPv4 forever:–)

Having said this, I agree with much of what you say about writing an IPv6 firewall. Aside from writing secure code for the IPv6 kernel, a big chunk of the work is deciding what of the IPv6 datagram header pose security threats and how you intend to use or dispose of them. Vendors who wrote ALGs/proxies may in fact have some advantage over "intensely, pervasively and ecumenically stateful inspection" (aye, Cap'n).

It's not that it is hard Patrick, it's that we have hundreds of security vendors competing for a tiny fraction of IT budgets, so margins count. Few product development teams will place IPv6 implementation at the top of the feature list until the market matures. Currently, I would hesitate to even call the IPv6 market nascent (in terms of promise of revenue).

So we are stuck between the ro