What really breaks the "end-to-end nature of the Internet"

Lori MacVittie, 2008-25-07

IPv6 was supposed to eliminate NAT (Network Address Translation). But in order to make the transition from IPv4 reasonable and less painful, it's being added to IPv6. It's intended use in being included in IPv6 is to create gateways that bridge between IPv6 and IPv4 while the transition occurs.

The IETF is not thrilled however. It's description of how it feels about NAT and the necessity to include it make it sound like school-children forced to allow ***that kid*** to play in their game of kickball. And then they put him in far right field. And I mean ***far*** right field so it's obvious what they think of him.

This Network World article describes NAT as "much maligned" and reminds us that purists hate it for breaking the end-to-end communication model on which the Internet was designed.

From the article:

> NAT is deployed in routers, servers and firewalls, and it adds complexity and cost to enterprise networks. Internet purists hate NATs because they break the end-to-end nature of the Internet; this is the idea that any end user can communicate directly to another end user over the Internet without middle boxes altering their packets.

I'm guessing purists hate a whole lot of technologies because there are a ton of other technologies and products that are essentially "middle boxes altering packets."

The problem is I don't ***want*** any end user communicating directly with me. I want their packets inspected, sanitized, and thoroughly cleansed before they get anywhere near me. I ***want*** them altered or nuked into the ether, particularly if they're full of nastiness or hell-bent on destroying the delicate balance that is my desktop.

Alteration of packets is a necessity to address protocol errors and perform all sorts of interesting application delivery functions. Alteration of packets is necessary to add caching control to web applications that are not written with caching in mind; it's necessary to rewrite URIs, and to protect sensitive data from escaping the confines of the data center. Alteration of packets by "middle boxes" (i.e. intermediaries or proxies) is a requirement for optimizing and securing application data.

And more than just solving the lack of IPv4 problems, NAT has become a primary security mechanism for ensuring end users aren't directly reachable by external applications. Even if I had enough IPv4 addresses to put all the machines in my home on the public Internet, I wouldn't. That's just asking for trouble, especially when some of those machines are being used by teenagers whose idea of security is using "hotbutterfly99" as their username on HotMail or Yahoo. And there's not that much difference between those teenagers and many corporate employees.

Geoff Huston, chief scientist at APNIC and an expert on IPv4 address depletion

> Huston says NATs are useful for addressing, packet filtering and other functions. He says the real problem with NATs is that they lack standards, and that is an area where the IETF can make improvements in NATs for IPv6.
>
> "The IETF's position of ignoring NATs some years back forced NAT software builders to exercise their own creativity when designing their version of NATs," Huston says. "This variation of NAT behavior is a far, far worse problem than NATs themselves."

But it goes deeper than just a lack of standards and being "impure". When it comes down to it the root of the problem - what really breaks the end-to-end model of the Internet - is people. It's the nature of people to do things they shouldn't, to code applications without concern or regard for the bigger picture, to just outright make mistakes, and in some cases to be malicious and hell bent on destruction. So long as it's people writing applications and using the Internet, alteration of packets by "middle boxes" is going to be a requirement if we want to keep applications secure, fast, and available. Especially secure.

Packets are going to continue to be altered when IPv6 is fully adopted whether NAT remains used or not, because people can't be upgraded to a new version that addresses our behavior, and we don't have a way to enforce a behavioral RFC on every Internet user in the world.

Besides, given all the good that comes out of "middle boxes altering packets": optimization, scalability, application layer networking, acceleration, and of course, security, I'm just not convinced that NAT and other technologies breaking the end-to-end nature of the Internet is a bad thing after all.

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com