

[fw-wiz] Nat Limitations?

Source: <http://www.derkeiler.com/Mailing-Lists/Firewall-Wizards/2007-10/msg00012.html>

- *From:* jason@xxxxxxxxxx
 - *Date:* Tue, 9 Oct 2007 09:03:24 -0400 (EDT)
-

Hello,

I'm interested in hearing some thoughts on a topology I'm considering in pursuing. On a mid sized college campus, we have the funding to physically segment the residence halls from the rest of the campus network. This is a huge win from a security perspective among other things. We've also begun using a separate provider for bandwidth. A long-term goal would be to hand the management of these buildings off to a company who can maintain it to reduce our headaches.

So, in building it we want to make it as portable as possible. As such, NAT comes to mind so we don't have to re-number it if a different provider takes it. It also has a number of other advantages which I'm sure are well known.

The problem is that I'm concerned about the number of translations that will happen in these buildings. Currently this part of the network is allocated a /19 and we estimate there are just over 4,000 residents.

I see some of the pitfalls being:

- * The cisco FWSM is limited to 256K concurrent translations. That's only 64 per user. Bit-torrent is likely to slaughter that.
- * It's harder to handle RIAA complaints since everything comes from a different public address.
- * Rate limiting (packet shaping) is currently done at the ISP for these buildings. We'll have to move that inside (more \$\$) or do protocol shaping instead of by IP address.
- * Certain applications may break, etc.

So my question is:

Has anyone tried to NAT this many of a certain type of user?

and

[fw-wiz] Nat Limitations?

Do the benefits outweigh the caveats?

Jason Mishka – "I'm like a Subway in a land of McDonalds..."

firewall-wizards mailing list

firewall-wizards@xxxxxxxxxxxxxxxxxxxxxxxx

<https://listserv.icsalabs.com/mailman/listinfo/firewall-wizards>