WHAT'S MISSING FROM (AT LEAST SOME) CURRENT TRAFFIC SHAPING APPLIANCES?

1. Capacity

— Current units are available with gigabit ethernet interfaces, but typically cannot shape much beyond an OC3's worth of traffic. This makes it difficult to deploy shapers in some of the locations where one might want to do so (e.g., on an OC12 link, or on a hot gigabit uplink, for example).

2. Density

— Current units typically deliver only a single shaped interface per box (rather low port density). If you need to shape a lot of subnets, you end up using up a lot of U's worth of rackspace.

3. Security

— Current units may not offer SSL encryption of administrative web pages or SSH encrypted console access or support for challenge/response one time password schemes. TCP wrappers-like filtering and logging functionality would also be highly desirable.

4. Coordination

— Current units commonly do not make it possible for a group of shapers to share a common policy amongst multiple units. For example, assume you have ten separate shapers shaping ten subnets, and would like to limit total Kazaa traffic through that set of shapers to no more than 10Mbps in aggregate. For most shaper products, there is no clean way to handle that currently (and no, if we want to hold all ten to no more than ten Mbps in aggregate, it is NOT acceptable to just set a one Mbps cap on each individual box -- that would greatly overcontrol/overlimit that set of subnets with respect to allowing (for example) two subnets to burst to 5Mbps each if nothing else was using part of that 10Mbps aggregate limit)

5. Administrative Flexibility

— Current units commonly offer only "Look" (read) access and "Touch" (write) access via a single password for each class of access. That coarse level of access control fails to deliver the sort of granularity one would ideally like. At a minimum, every user should have a unique username and password, so that access and changes can be attributed/logged. Shared passwords are a really bad idea. Moreover, ideally, multiple levels of access (according to a defined set of roles) should be available. Roles might include:

- — administrator (full access, including the ability to create new accounts or change or delete existing accounts)
- — installer (needs to be able to write the basic configuration screen, including IP addresses, netmask, default gateway, NTP server address, etc., but nothing beyond that)
- — policy administrator (needs to be able to twiddle the policy knobs, but should have no need to reconfigure the interfaces)
- — operations staff (needs to be able to determine if the box is healthy overall, but needs no access to policy data; should be able to gently reboot the box).
- — managerial level policy oversight (needs to be able to see aggregate level data, but not any individually identifiable data, nor should this class of user be able to change anything)
- — staff/audit level policy oversight (can see all data, including individually identifiable data, but cannot change anything)
- — per-IP-limited access to data (for example, a student conduct officer should be able to get a per-IP tailored view of what the shaper has seen in terms of traffic for a particular dotted quad only, granted by the policy administrator)
- — offer general (public) access to unpassworded web pages with only selected data displayed (ala MRTG)

6. Connections To A Database With User-Level Administrative Data

— From a policy enforcement point of view, we deal with users, not FQDN's or dotted quads. It would be really handy if shapers were smart enough to be able to use a site supplied database or flat file mapping to make connections between FQDN's (or dotted quads) and "real names" (or jack locations, say), instead of requiring a separate manual lookup by the user when an interesting address is noticed.

7. Management by Exception

Shapers should have enough flexibility to allow me to tell the shaper what data I want to routinely ignore, and what's an important exception condition. Don't drown me with clutter and irrelevant data. Let me concentrate on flying the plane...

8. Price

The price/unit needs to come down. It is outrageous for a shaper to cost 20X or 50X what a 10/100/1000 ethernet switch costs. A lot more people would buy 'em, and deploy 'em where they need 'em, if they could just afford 'em.