[unisog] Traffic Shapers

Jeff Kell jeff-kell at utc.edu
Thu Jul 17 15:44:48 GMT 2008

- Previous message: [unisog] Traffic Shapers
- Next message: [unisog] Traffic Shapers
- **Messages sorted by:** [date] [thread] [subject] [author]

Kaminski, Eryk G. wrote:
> *I will need to procure a traffic shaper soon. I have it narrowed down to*
> *Packeteer and NetEqulizer. Besides the large difference in pricing, does*
> *anyone have any pro/cons for either device? I have heard Packeteer*
> *requires frequent fine tuning.*

The answer, as often found in our industry, is "It Depends" :-)
Primarily on what you are really trying to accomplish, and what you have to spend.

My opinions, for what they are worth...

I have never seen/evaluated a NetEqualizer. From my understanding, it is an "application independent" device which attempts to do just what it's name implies, equalize access to the available bandwidth. If you are not currently exceeding the available bandwidth, it does nothing. As you approach the limit, the largest consumers are shaped down to match the available bandwidth. If you are just after leveling out the playing field, this is a perfect fit, in theory. I don't know how the device actually performs it's throttling, and how various applications fare against its methods, e.g., TCP-based versus UDP-based.

For application-aware shaping, I have managed a Packeteer 6500 for a number of years, evaluated an Allot NetEnforcer 1020 for a number of weeks, and after a similar evaluation chosen a Procera PacketLogic 7620 going forward. Some comments and pros/cons on these follow.

The Packeteer was an apparent "gift from above" when it appeared on the market in the days of trying to respond to the Napster / Kazaa / Gnutella onslaught. They were very accurate and responsive to changes / additions in the early days, but have been dragging their feet a bit lately. In recent years, our traffic has been dominated by "HTTP" and "Unknown" traffic (a trait shared by all to some extent). Recent updates added classification of Flash, but they haven't added much in the way of granularity of their traffic classification.

The Allot provides a comparable classification tree of services, if not more than the Packeteer, and I was initially impressed, particularly with the price. But it does have it's limitations on the "depth" of inspection, at least the 1020 platform. For example, there was no "Flash" classification (went into HTTP). Documentation indicated that Flash could be identified in their "NetExplorer" platform, and this led to a very confusing chain of events. Suffice it to say that Flash cannot be identified on the 1020, nor any other Content-type, at this time. It is, however, supported on their lower end 400 and 800 platforms (which I did not evaluate).

The Procera was a modern-day "gift from above" in it's application classification when contrasted with the other two. Besides the factory-supplied services, it provides some powerful facilities to

define your own classifications. As an example, we created a classification to allow BitTorrent, but only for the Blizzard game updates (e.g., World of Warcraft) while blocking all other BT traffic. You can also classify traffic based on "properties" of the traffic - bulky, streaming, interactive, random-looking (e.g., encrypted), and a whole slew of others I have yet to explore.

Next we have the various approaches to "shaping".

Packeteer roughly divides up bandwidth into "partitions". Partitions can be defined with a minimum and maximum bandwidth, roughly similar to a committed/burst rate. You can also define the bandwidth limits as a percentage of the link speed, to allow for automatic reconfiguration if the link speed changes. You can then assign the various traffic classifications to a partition, and the partition controls the bandwidth rather than the overall link. Each classification can be prioritized in several ways with a "policy" - a priority, a rate, discard, never admit, etc, so that you can prioritize traffic within a partition. And finally, there are "dynamic partitions" where you can rate-limit based on the individual inside host IPs actively using a classification. The dynamic partitions are given a guaranteed and a burst rate, and what to do if the allocated bandwidth is exceeded (discard or "squeeze"). There are, however, limits on the number of dynamic partitions you can have based on your hardware model and software license.

Allot is similar, but uses "pipes" and "virtual channels". The "pipes" can be used to apply different policies to different groups of IPs, something that the Packeteer doesn't naturally do (you have to redefine the factory classes with specific source IP ranges for each different group you want to identify, or get their ISP version). The virtual channels then act similar to the Packeteer partitions. If you wish to do host-specific rate limiting, then you use "templates" at either the pipe or VC level. This lets you apply shaping rules to individual IPs rather than the collective traffic. But again, the number of pipes/VCs/connections is limited by your hardware platform and software license.

Procera has a radically different approach that takes some getting used to. Rather than classifying traffic into unique slots (traffic fits "here" and matches "this" rule), traffic shaping is done based on rules which pair up shaping objects (priority, bandwidth, etc) with matching criteria (host, client, server, port, service, property, time, vlan, etc). Traffic can match multiple objects at the same time, and the resulting "shaping" is taken as the highest priority of any matching object, subjected to the object with the least remaining bandwidth. This allows you to prioritize traffic based on the service (voice, gaming, video, web, bulk, etc) independent of your bandwidth constraints (dorms, main campus, guest, etc). And the bandwidth restrictions don't have to match up one-for-one either.

With the Packeteer we were originally only shaping our dorm traffic, and would limit them to 30% of our pipe M-F days, 60% M-F evening, and 90% all other times. We were able to easily extend this with the Allot to do both the main campus and dorms (campus not being subjected to limits) at the same time. But with the Procera, you can not only divide up the traffic as before, you can also allow each side to "borrow" from the other when bandwidth is available.

All of this shaping activity up to this point is based on real-time, short-term traffic patterns. If you've been trying to manage your bandwidth for any length of time, you've probably recognized that there are always a handful of "bandwidth hogs" that seem to consume gigs upon gigs, day after day, always pushing their limits.

Procera has a feature called "Volume Based Shaping". With VBS, you can define a volume "interval time", and various steps of bandwidth within that interval. For example, you can let everyone have unlimited bandwidth for their first 2 gigabytes a day, then cut them down to 2Mbps for the next 2, then set them at 512Kbps. Their "effective bandwidth" is calculated on the fly over the last 24 hours and becomes a "shaping object" to be evaluated with any other objects their traffic matches. Because the window is a sliding scale, everyone doesn't get reset at the same time.

Allot also had a "Quota" reference in their NetExplorer product, but it either wasn't supported on the 1020 or our eval license didn't permit it, I don't recall which, but it wasn't tested. To my knowledge, Packeteer does nothing of this sort.

Another Procera plus is that you can peer it with your border BGP router, and make policy decisions based on BGP AS-paths. For those of you with an Internet-2 connection, you can create separate shaping policies for your I2 traffic relative to commodity internet, but having the Procera shape based on the neighboring AS number (as long as your I2 paths traverse a different AS from your commodity traffic).

Procera has some other bells-and-whistles, like a handy firewall module. If you want to block traffic to a particular HTTP host NAME (as opposed to an IP), you can do it.

Hope that helps as a quick comparison. Again, just my opinions. The marketing folks at all the vendors seem to have been working overtime at over-hyping and buzzwording their respective offerings and complicating their pricing/licensing matrices, so beware of taking any of them on at face value. Get a test drive if you can, and kick the tires. It's the only way to really find out for yourself.

Jeff

- Previous message: [unisog] Traffic Shapers
- Next message: [unisog] Traffic Shapers
- **Messages sorted by:** [date] [thread] [subject] [author]

More information about the unisog mailing list