

# Equalizing Compared to Application Shaping (Layer-7 “Deep Packet Inspection” Products)



## Author's Note:

We often get asked how NetEqualizer compares to Packeteer (Bluecoat), NetEnforcer (Allot), Network Composer (Cymphonix), Exinda, and a plethora of other well-known companies that do Application Shaping (aka “packet shaping”, “deep packet inspection”, or “Layer-7” shaping). After several years of these questions, and discussing different aspects with former and current application shaping with IT administrators, we’ve developed a response that should clarify the differences between NetEqualizer’s behavior-based approach and the rest of the pack.

We thought of putting our response into a short, bullet-by-bullet table format, but then decided that since this decision often involves tens of thousands of dollars, 15 minutes of education on the subject with content to support the bullet chart was in order. **If you want to skip the details, see our [Summary Table](#) at the end of this article, or refer to our [Summaries](#) located in the Review Panes throughout this article.** However, if you’re looking to really understand the differences, and to have the question answered as objectively as possible, please take a few minutes to read on...

**Editor's Note:** (Updated with new material March 19th 2012) Since we first wrote this article, many customers have implemented the NetEqualizer not only to shape their Internet traffic, but also to shape their company WAN. Additionally, concerns about [DPI and loss of privacy](#) have bubbled up. (Updated with new material March 31<sup>st</sup> 2010) Since we first published this article, “deep packet inspection”, also known as Application Shaping, has taken some [serious industry hits](#) with respect to US-based ISPs.

## How NetEqualizer compares to Bluecoat, Allot, Cymphonix, and Exinda

In the following sections, we will cover specifically when and where [Application Shaping](#) is used, how it can be [used to your advantage](#), and also when it may not be a good option for what you are trying to accomplish. We will also discuss how Equalizing, NetEqualizer's behavior-based shaping, fits into the landscape of application shaping, and how in many cases Equalizing is a much better alternative.

## Table of Contents

1. [What is Application Shaping?](#)
2. [Accuracy of Application Shaping](#)
3. [When Is Application Shaping the Right Solution?](#)
4. [What about the Reporting Aspects of an Application Shaper?](#)
5. [What is Equalizing?](#)
6. [Accuracy of Equalizing](#)
7. [When Is Equalizing the Right Solution?](#)
8. [What about NetEqualizer Reporting?](#)
9. [Conclusion](#)  
[Summary Table](#)

## 1. What is Application Shaping? [back to TOC](#)

Application Shaping is defined as the ability to identify traffic on your network by type, and then set customized policies to control the flow rates for each particular type. For example, Citrix, AIM, YouTube, and BearShare are all applications that can be uniquely identified.

As you are likely aware, all traffic on the Internet travels around in what is called an IP packet. An IP packet can very simply be thought of as a string of characters moving from

## Equalizing Summary

- Simple turn-key solution to optimize VoIP and Business Applications (corporate WAN)
- The most effective for shared Internet trunks
- Little or no recurring cost or labor
- Low entry cost
- Conceptually, it takes some getting used to
- Reporting by behavior (bandwidth hogs, P2P traffic) used to stop abuse
- Historical and graphical reporting via ntop
- Handles encrypted and unencrypted P2P without modifications or upgrades
- Supports Net Neutrality

## Application Shaping Summary

- *Good for static links where traffic patterns are constant (corporate WANs)*
- *Not the best fit for shared Internet trunks*
  - *Constant labor to tune with changing application spectrum*
  - *Expect approximately 15% of traffic to be unclassified*
- *Costly to maintain in terms of licensing and labor*
- *High initial cost*
- *Intuitive. Makes sense and easy-to-explain to non-technical people*
- *Detailed reporting by application type*
  - *Only a static snapshot of a changing spectrum*
- *False positives may show data incorrectly. No easy way to confirm accuracy.*
- *Violates Net Neutrality*

computer A to computer B. The string of characters is called the “payload,” much like the freight inside a railroad car. On the outside of this payload is the address where it is being sent. On the inside is the data/payload that is being transmitted. These two elements, the address and the payload, comprise the complete IP packet. In the case of different applications on the Internet, we would expect to see different kinds of payloads.

*At the heart of all current application shaping products is special software that examines the content of Internet packets, performing "deep packet inspection", as they pass through the packet shaper. Through various pattern matching techniques, the packet shaper determines in real-time what type of application a particular flow is. It then proceeds to take action to possibly restrict or allow the data, based on a rule set designed by the system administrator.*

## 2. Accuracy of Application Shaping [back to TOC](#)

As application shaping needs to examine the content of Internet packets, the [question of accuracy](#) comes into play. The challenges with classifying Internet packets are numerous. We will discuss the key challenges in detail below.

### Misclassification of Traffic

Traffic can easily be misclassified. For example, the popular peer-to-peer (P2P) application Kazaa actually has the ASCII characters “Kazaa” appear in the payload; and hence a packet shaper can use this keyword to identify a Kazaa application. Seems simple enough, but suppose that somebody was downloading a Word document discussing the virtues of peer-to-peer and the title had the character string “Kazaa” in it. Well, it is very likely that this download would be identified as Kazaa and hence misclassified. After all, downloading a Word document from a Web server is not the same thing as the file-sharing application Kazaa.

### Unclassifiable Traffic

The other issue that constantly brings the accuracy of application shaping under fire is that *some application writers find it in their best interest not be classified*. In a mini arms-race that plays out everyday across the world, some application developers are constantly changing their signature, and some have gone as far as to [encrypt](#) their data entirely.

Yes, it is possible for the makers of application shapers to counter each move, and that is exactly what the top companies do; but it can take a heroic effort to keep

pace. The constant engineering and upgrading required has an escalating cost factor. In the case of encrypted applications, the amount of CPU power required for decryption is quite intensive and impractical. We believe that other methods will be needed to identify encrypted P2P. But, this is not to say that application shaping doesn't work in some cases or provide some value. So, let's break down where it has potential, and where it may bring false promises. First off, the realities of what really happens when you deploy and depend on this technology need to be discussed.

## The Ninety Percent Rule

As of early 2003, we had a top engineer and executive join APConnections direct from a company that offered application shaping as one of their many value-added technologies. He had first-hand knowledge from working with hundreds of customers who were big supporters of application shaping. *The application shaper his company offered could identify 90 percent of the spectrum of applications, which means they left 10 percent as unclassified. So, right off the bat, 10 percent of the traffic is unknown by the traffic shaper.*

Is this traffic important? Is it garbage that you can ignore? Well, there is no way to know without any intelligence, so you are forced to let it go by without any restriction. Or, you could put one general rule over all of the traffic – perhaps limiting it to 1 megabit per second maximum, for example. Essentially, if your intention was 100-percent understanding and control of your network traffic, right out of the gate you must compromise this standard.

In fairness, this 90-percent identification actually is an amazing number with regard to accuracy when you understand how daunting application shaping is. Regardless, there is still room for improvement. So, that covers the admitted problem of unclassifiable traffic, but how accurate can a packet shaper be with the traffic it does claim to classify? Does it make mistakes?

### False Positives

There really isn't any reliable data on how often an application shaper will misidentify an application. To our knowledge, there is no independent consumer reporting company that has ever created a lab capable of generating several thousand different application types with a mix of random traffic, and then took this mix and identified how often traffic was misclassified. Yes, there are trivial tests done one application at a time, but misclassification becomes more likely with real-world complexity and diverse application mixes.

From our own testing with application technology freely available on the Internet, *we discovered false positives can occur up to 25 percent of the time*. A random FTP file download can be classified as something more specific. Obviously, commercial packet shapers do not rely on free technology like open source, and they may improve on it.

So, if we had to estimate based on our experience, perhaps 5 percent of Internet traffic will likely get misclassified. *This brings the overall accuracy of packet shaping down to 85 percent* (combining the traffic they don't claim to classify with an estimated error rate for the traffic they do classify).

### Constantly Evolving Traffic

Our sources say (mentioned above) that *70 percent of their customers that purchased application shaping equipment were using the equipment primarily as a reporting tool after one year*. This means that they had stopped keeping up with shaping policies altogether, and were just looking at the reports to understand their network (nothing proactive to shape the traffic).

This is an interesting fact. From what we have seen, many people are just unable, or unwilling, to put in the time necessary to continuously update and change their application rules to keep up with evolving traffic.

The reason for the constant changing of rules is that with traditional application shaping you are dealing with a cunning and wise foe. For example, if you notice that there is a large contingent of users using Bittorrent, and you put a rule in to quash that traffic, within perhaps days those users will have moved on to something new: perhaps a new application or encrypted P2P. *If you do not go back and re-analyze and reprogram your rule set, your packet shaper slowly becomes ineffective*.

And finally, lest we forget, application shaping is considered by some to be a [violation of Net Neutrality](#), due to the very nature of packet inspection.

## 3. When is Application Shaping the Right Solution? [back to TOC](#)

### WAN Optimization

There is a large set of businesses that use application shaping quite successfully, along with other technologies. This area is WAN optimization. Thus far, we have discussed the issues with using an application shaper on the wide-open Internet where the types and variations of traffic are unbounded.

*In a corporate environment with a finite set and type of traffic flowing between offices, an application shaper can be set up and used for WAN optimization with reliable results*. We have also achieved equal and sometimes better results with a NetEqualizer head-to-head in a WAN environment. We will discuss the benefits of Equalizing later in this article.

There is also the political side to application shaping. It is human nature to want to see and control what takes place in your environment. Finding the best tool available to actually show you what is on your network, and the perceived ability to contain it, plays well with just about any CIO or IT Director on the planet. The downside of detailed reporting over a simple heuristic solution is that it can create data confusion. We have addressed this subject in our article, "[The True Price of Bandwidth Monitoring](#)".

### It's an Easy Sell

An industry-leading packet shaper brings visibility to your network and a pie chart showing 300 different kinds of traffic. *Whether or not the tool is practical or accurate over time isn't often brought into the buying decision. The decision to buy can usually be "intuitively" justified*. By intuitively, we mean that it is easier to get approval for a tool that is simple to conceptually understand by a busy executive looking for a quick-fix solution.

As the cost of bandwidth continues to fall, the question becomes [how much a CIO should spend](#) to analyze a network. This is especially true when you consider that as the Internet expands, the complexity of shaping applications grows. As bandwidth prices drop, the cost of implementing such a product is either flat or increasing. In cases such as this, it often does not make sense to purchase a \$25,000 bandwidth shaper to stave off a bandwidth upgrade that might cost an additional \$200 a month.

## 4. What about the Reporting Aspects of an Application Shaper? [back to TOC](#)

Even if it can only accurately report 85 percent of the actual traffic, isn't this useful data in itself?

Yes and no. Obviously analyzing 85 percent of the data on your network might be useful, but if you really look at what is going on, it is hard to feel like you have control or understanding of something that is so dynamic and changing.

By the time you get a handle on what is happening, the system has likely changed. Unless you can take action in real-time, the network usage trends (on a wide-open Internet trunk) will vary from day-to-day.<sup>1</sup> It turns out that the most useful information you can determine regarding your network is an overall usage pattern for each individual. The goof-off employee/user will stick out like a sore thumb when you look at a simple usage report, since the amount of data transferred can be 10-times the average for everybody else. The behavior is the indicator here, but the specific data types and applications will change day-to-day and week-to-week.

<sup>1</sup> The exception is a corporate WAN link with relatively static usage patterns.

## 5. What is Equalizing? [back to TOC](#)

Overall, it is a simple concept. *Equalizing is the art form of looking at the usage patterns (aka traffic "behaviors") on the network, and then when things get congested, robbing from the rich (bandwidth hogs) to give to the poor.*

Rather than writing hundreds of rules to specify allocations to specific traffic as in traditional application shaping, you can simply assume that large downloads are bad, short quick traffic is good, and be done with it.

This *behavior-based approach* to traffic shaping usually mirrors what you would end up doing if you could see and identify all of the traffic on your network, but doesn't require the labor and cost of classifying everything. Applications such as VoIP, web-based business applications (SaaS, cloud-based apps), Internet browsing, and instant messaging (IM) all naturally receive higher priority, while large downloads, video, and P2P receive lower priority. This behavior-based shaping does not need to be updated constantly as applications change.

*Once equalizing is in place, it automatically shapes your network when it is congested, using algorithms to implement "fairness".* The concept of "fairness" enables your network to continue providing quick response times to the majority of your users while restricting bandwidth hogs. Low bandwidth users do not have to share the pain of a slow, congested network clogged by larger, network-hogging applications.

Each connection on your network constitutes a data flow. Flows vary widely from short dynamic bursts, such as when searching a small website, to large persistent flows, as when performing P2P file-sharing.

Equalizing is determined from the answers to these questions:

- 1) *How persistent is the data flow?*
- 2) *How many active data flows are there?*
- 3) *How long has the data flow been active?*
- 4) *How congested is the overall network trunk?*
- 5) *How much bandwidth is the data flow using, relative to the network trunk size?*

Once these answers are known, then Equalizing makes adjustments by adding latency to low-priority data flows, so that high-priority data flows receive sufficient bandwidth.

As we have stated, Equalizing logic is applied to individual data flows (IP pairs), which enables it to discriminate across traffic for an individual user. For example, a network user sending an email, while on a VoIP call, and downloading a large file will be treated as three (3) separate data flows. The VoIP and email will continue seamlessly, while the large file download will be slowed - to prevent the VoIP call from breaking up or the email to hang.

Equalizing traffic shaping ensures that a large bandwidth hog does not bring the network to a crawl and that business can continue as usual.

## 6. Accuracy of Equalizing [back to TOC](#)

As equalizing is not inspecting traffic, nor trying to determine the type of application for that traffic, *classification accuracy is not an issue.* The very nature of behavior-based shaping enables traffic to be managed and controlled without worrying about classification.

*Equalizing is looking at the size of the traffic and how the traffic behaves on your network.* These are the things that really matter when you think about it. If your goal is to optimize your network resources, understanding and responding to the nature of traffic on your network just makes sense. The additional overhead of attempting traffic classification is not required to speed up your network.

## 7. When is Equalizing the Right Solution? [back to TOC](#)

*Equalizing is the right solution when you are trying to shape traffic on a shared Internet trunk, or if you want a simple turn-key solution to optimize VoIP and Business Applications on a WAN link.*

Equalizing gets you out of the classification game. You do not have to worry about misclassification of traffic, unclassifiable

traffic, or only 90% of your traffic getting classified correctly - *as equalizing does not rely on classification to shape traffic.* Equalizing is the right solution for Internet traffic shaping, for all the reasons that application shaping is not. Equalizing has also been very successfully implemented on corporate WANs, where it can be used to give priority to VoIP and business applications over non-business-critical traffic.

Equalizing enables you to minimize management of your network pipe. You do not need to spend time keeping up with policy files that capture the latest types of applications. Equalizing works on all types of traffic, regardless of the application. This saves your network administrator time.

Equalizing maximizes the use of your bandwidth, which can help you to defer a bandwidth upgrade and also ensures that you are optimizing your existing bandwidth. Your bandwidth is available for all application types to use as needed. You do not need to allocate portions of your network to each application type, trying to determine in advance what to reserve for each type, which can leave valuable bandwidth unused.

Equalizing also saves you money. You no longer need to subscribe to expensive policy file updates. As we believe that bandwidth shaping should be affordable, we have priced our solution fairly, which we believe makes us *the most cost-effective solution on the market.*

### Handling P2P Traffic

Another key element in behavior-based shaping is connections. Equalizing takes care of instances of congestion caused by single-source bandwidth hogs. However, the other main cause of Internet gridlock (as well as bringing down routers and access points) is peer-to-peer traffic, and its propensity to open hundreds or perhaps thousands of small connections to different sources on the Internet. Over the years, the NetEqualizer engineers have developed very specific algorithms to spot connection abuse and avert its side effects.

Using connection limits, *the NetEqualizer is able to block both encrypted and unencrypted P2P traffic*, without the additional overhead of classifying traffic.

### Handling Video Traffic

Oftentimes, customers are concerned with accidentally throttling important traffic that might not fit the NetEqualizer model, such as video. We handle video traffic in two ways:

#### 1) The NetEqualizer Caching Option (NCO)

NCO is integrated with Equalizing, providing a comprehensive bandwidth management strategy. Traffic can be accessed from cache or accessed from the Internet and equalized, as needed. *NetEqualizer Caching Option caches all port 80 traffic file sizes from 2MB to 40MB, including YouTube videos.* Any

type of static content that is frequently accessed will benefit from caching.

#### 2) Prioritizing Live Streaming Video

For real-time streaming video, we find that in most cases this is run from a hosted or known server. The NetEqualizer has a low-level routine that easily allows you to give overriding priority to a specific server, either temporarily for one-time events, or permanently.

### Relieving Hidden Node Congestion

Equalizing Technology is the only traffic shaping technology that can relieve [hidden node congestion](#) in wireless networks.

An [independent study](#) by the [University of Limerick](#) validated that Equalizing technology solves the hidden node issue.

### Net Neutrality

And finally, equalizing [supports Net Neutrality](#), as it does not inspect Internet packets.

### It's a Harder Sell

Trusting a heuristic solution such as NetEqualizer is not always an easy step. Our model is very different than application shaping, so it takes some getting used to at first, and then our customers rave about their faster networks, and love the low maintenance "set it and forget it" aspect of our model.

## 8. What about NetEqualizer Reporting?

[back to TOC](#)

[NetEqualizer Reporting](#) is simple and streamlined. We offer both real-time and historical reports (via ntop) to give you visibility into your network traffic.

Real-time reporting enables you to see what is going on in your network at this moment, in order to actively monitor and manage your network usage. For example, two of our key real-time reports will help you to find traffic that is exhibiting a P2P pattern (P2P Locator), or look at bandwidth usage for a particular user/IP address (Instantaneous Bandwidth Usage).

Our historical reporting via [ntop](#) offers graphs and charts that can be used to look at trends in usage on your network, so that you can better plan for future bandwidth needs.

However, in our opinion, while some reporting is essential, complicated reporting tools tend to be overkill. When users simply want their networks to run smoothly and efficiently, detailed reporting isn't always necessary, and certainly isn't the most cost-effective solution.

Detailed bandwidth monitoring technology is not only more expensive from the start, but an administrator is also likely to

spend more time making adjustments and looking for optimal performance. The result is a continuous cycle of unnecessarily spent manpower and money.

## 9. Conclusion [back to TOC](#)

We hope that this white paper has given you the facts that you need to make an informed decision about what direction is right for you - application shaping or equalizing. If you have additional questions, please feel free to contact us via email:

[sales@apconnections.net](mailto:sales@apconnections.net) or call us at **303.997.1300 x103** to discuss further. ☆

## Summary Table: Equalizing Compared to Application Shaping [back to TOC](#)

Equalizing	Application Shaping
Simple turn-key solution to optimize VoIP and Business Applications (corporate WAN)	Good for static links where traffic patterns are constant (corporate WAN)
The most effective for shared Internet trunks	Not the best fit for shared Internet trunks Constant labor to tune with changing application spectrum Expect approximately 15% of traffic to be unclassified
Little or no recurring cost or labor	Costly to maintain in terms of licensing and labor
Low entry cost	High initial cost
Conceptually, it takes some getting used to	Intuitive Makes sense and easy-to-explain to non-technical people
Reporting by behavior (bandwidth hogs, P2P traffic) used to stop abuse Historical and graphical reporting via ntop	Detailed reporting by application type Only a static snapshot of a changing spectrum
Handles encrypted and unencrypted P2P without modifications or upgrades	Does not handle encrypted P2P False positives may show data incorrectly No easy way to confirm accuracy
Supports Net Neutrality	Violates Net Neutrality

### About APconnections, Inc.

APconnections is an innovation-driven technology company that delivers best-in-class network traffic management solutions to give our customers better networks, with zero maintenance, at the best prices. We specialize in turn-key bandwidth shaping and intrusion prevention system (IPS) appliances.

Since 2003, APconnections' mission has been to provide simple turn-key network optimization appliances to any network topology. Our products are simple to install, easy to use, require little maintenance, and are offered at the best prices.

APconnections is based in Lafayette, Colorado, USA. We released our first commercial offering in July 2003, and since then thousands of customers all over the world have put our products into service. Today, our flexible and scalable solutions can be found in many types of public and private organizations of all sizes across the globe, including: Fortune 500 companies, major universities, K-12 schools, Internet providers, law firms, hotels, hospitals, libraries, business centers, small businesses, non-profits, military, and government agencies on six (6) continents.

### About the NetEqualizer Product Family

NetEqualizer appliances are bandwidth shaping systems designed to optimize your Internet connection or WAN link, while giving priority to your important business and data applications. The flexible, scalable, and cost-effective bandwidth control products can be deployed in both corporate and service provider networks.

NetEqualizer is available in a range of configurations from 10Mbps up to 5 gigabits.