



Product Demonstration Guide

Table of Contents

Introduction	2
Overview of Equalizing	2
Equalizing Scenario.....	2
Key Features of the NetEqualizer	4
NetEqualizer Dashboard	4
Reducing Network Congestion	5
Controlling P2P Traffic.....	7
Limiting Traffic	8
Monitoring for Possible DDoS Attacks	9
NetEqualizer Monitoring & Reporting	10
Where to Install the NetEqualizer	12

Introduction

In this guide we will take you through our behavior-based "equalizing" technology, so that you get a better understanding of how we approach traffic shaping. After we walk through an example of equalizing, we will then show you how to configure equalizing on the NetEqualizer to reduce network congestion. Several of our more popular features will also be reviewed, including controlling P2P traffic, setting up individual or shared traffic limits, spotting potential DDoS attacks, and real-time traffic monitoring and reporting.

Overview of Equalizing

Equalizing technology is our set of industry-leading, proprietary traffic shaping algorithms that automatically optimize your network bandwidth. Equalizing automatically relieves congestion and improves the overall user experience during peak periods on your network. During peak periods, equalizing gives priority to short, bursty, well-behaved, business-critical traffic such as web-based applications, web browsing, email, and voice-only VoIP. This enables most users to continue to have a great network experience, while slowing down live streaming video and large downloads, which can clog your network.

If you answer yes to one or more of these questions, Equalizing may be right for you:

- Do you want to improve response times for web applications, web browsing, e-mail, and Cloud/SaaS applications?
- Do you want to reduce the overhead of peer-to-peer (P2P), video streaming, or large downloads?
- Do you want to set individual or shared rate limits for users or subnets?
- Do you want to ensure priority for your VoIP calls?
- Do you want to reduce the threat from rogue applications opening 100's or even 1000's of connections to the Internet?

Let's walk through a simplified scenario, so that you can see how this would work on your network.

Equalizing Scenario

We know that you have thousands of users on your network. However, to simplify our example, let's focus in on two (2) of them, as shown in Figure 1 below. Imagine a situation with two users accessing the Internet at the same time over a shared link. The 1st person is downloading a large file, sending email, surfing the web, all while on a VoIP conference call; the 2nd person is trying to send a quick business email and surf the web. In a typical system, the 1st user will be getting almost all of the bandwidth to download the large file (blue line in Figure 1), bringing response time to a crawl. All other traffic, including the 2nd user's business email, is experiencing slow response times, while stuck waiting for the download to finish (five orange lines in Figure 1).

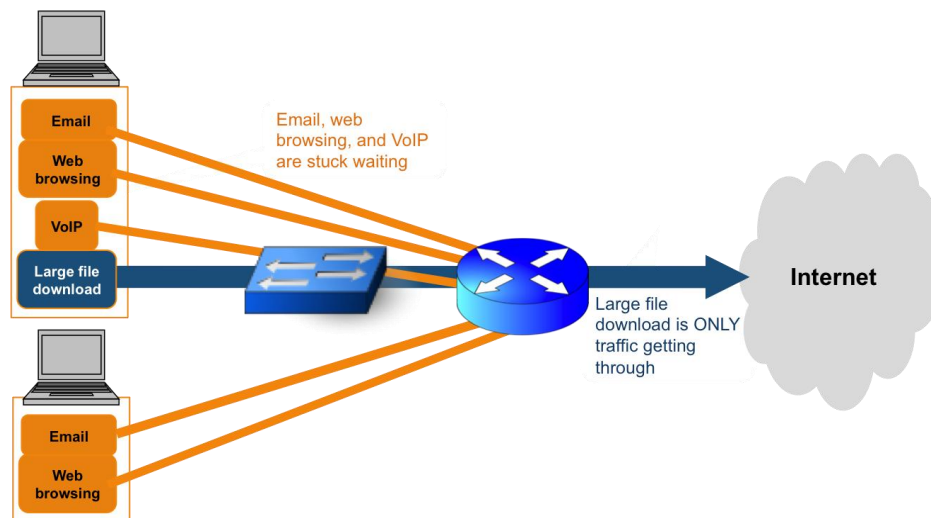


Figure 1: Without Equalizing

Note that **ONLY** the large file download is getting through. All other traffic is waiting.

The NetEqualizer solves this problem and many other similar bottlenecks automatically. *Equalizing looks at the behavior of the applications and their usage patterns.* By adhering to some simple rules of behavior, the real-time, latency-sensitive applications, such as email, can be differentiated from the heavy non-real-time activities, such as the large file download, and thus be granted priority on the fly, *without needing any specific policies to be set by the network administrator.*

Equalizing works on each data flow, shaping traffic at the IP pair level, and makes decisions based on the nature and behavior of each data stream. Equalizing is determined from the answers to these questions:

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

Once these answers are known, *Equalizing makes adjustments to flows by adding latency to low-priority tasks, so that high-priority tasks receive sufficient bandwidth.* As show below, with Equalizing all traffic is getting through, including emails, web surfing, and VoIP, while the large file download is being slowed down.

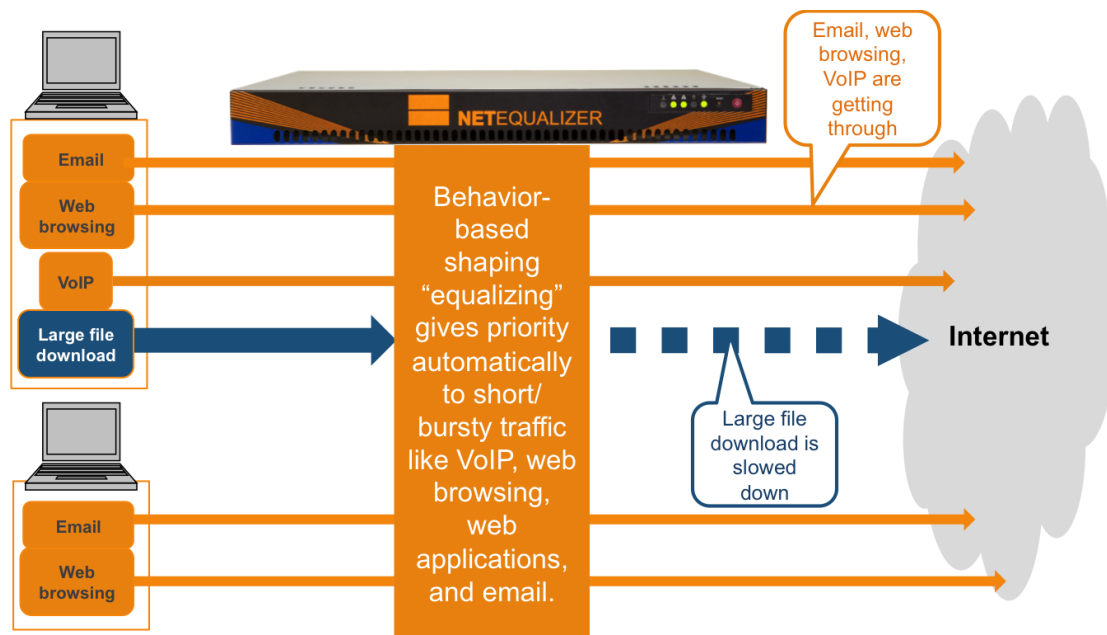


Figure 2: With Equalizing

Email, VoIP, and web browsing are getting through. Large File Download is being slowed down.

This scenario demonstrates the key concept behind Equalizing, to simply and elegantly minimize network congestion by keeping bandwidth "hogs" from taking more than their fair share of your network. Short/bursty traffic automatically gets priority over long/hoglike traffic.

In addition, when bandwidth hogs are slowed, the sending site is signaled to "back off". This reduces gridlock as well, as the traffic is not re-sending relentlessly on your network, thereby reducing congestion.

Equalizing optimizes the full use of your bandwidth, improving QoS during peak periods. Equalizing is a cost-effective way to improve network usability, increase user satisfaction, and reduce network complaints, all while minimizing ongoing configuration from your network administrators.

Key Features of the NetEqualizer

Although the NetEqualizer has many advanced features, you can configure our behavior-based shaping, also known as "equalizing", in just three (3) simple steps. Setup time from cabling to configuration will take only 1-3 hours for most network administrators.

We also offer a complementary review of your installation, once you have completed your configuration, to verify that you have optimized the NetEqualizer setup for your network environment.

NetEqualizer Dashboard

The NetEqualizer Dashboard provides an intuitive visual display of the status on critical data and settings within NetEqualizer. Think of the Dashboard as your command and control center for managing your NetEqualizer. On Figure 3 below, the key elements that make up the Dashboard are labeled: Key Functions, Information Buttons, Common Tasks, Status Indicators, and the Current Activity Graph.

Key Functions buttons are your main access point into configuring, monitoring, and reporting. They include: 1) Setup, 2) Real-Time Reporting (RTR), 3) DDoS, and 4) Maintenance. In this guide, we will focus on the first three functions.

Information Buttons provide a quick overview of key settings, and also can be clicked to edit the setting, where applicable. You can see the current software version that you are running, the system date & time, as well as your license key settings.

Common Tasks are shortcuts to popular features, including perform quick edits, show configuration, view active connections, and run diagnostics.

Status Indicators display on/off statuses for Equalizing, RTR (real-time reporting), Quota, and Packet Capture, so that you can quickly see which processes are currently running.

The **Current Activity Graph** is a view into Real-Time General Traffic, which is clickable and shows the total amount of upload and download data flowing through your NetEqualizer.

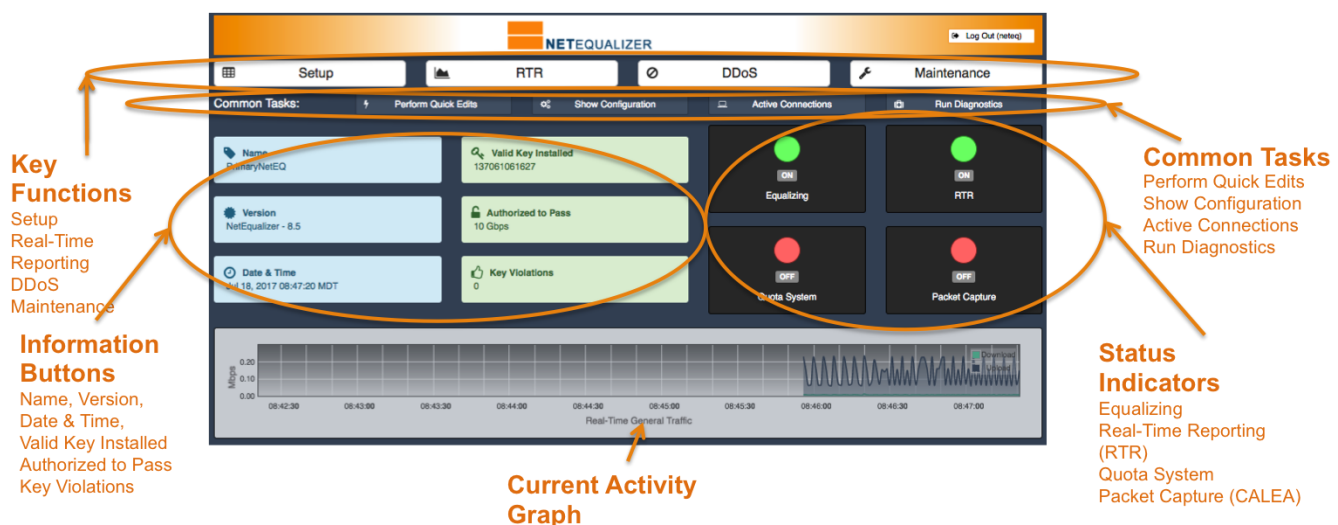
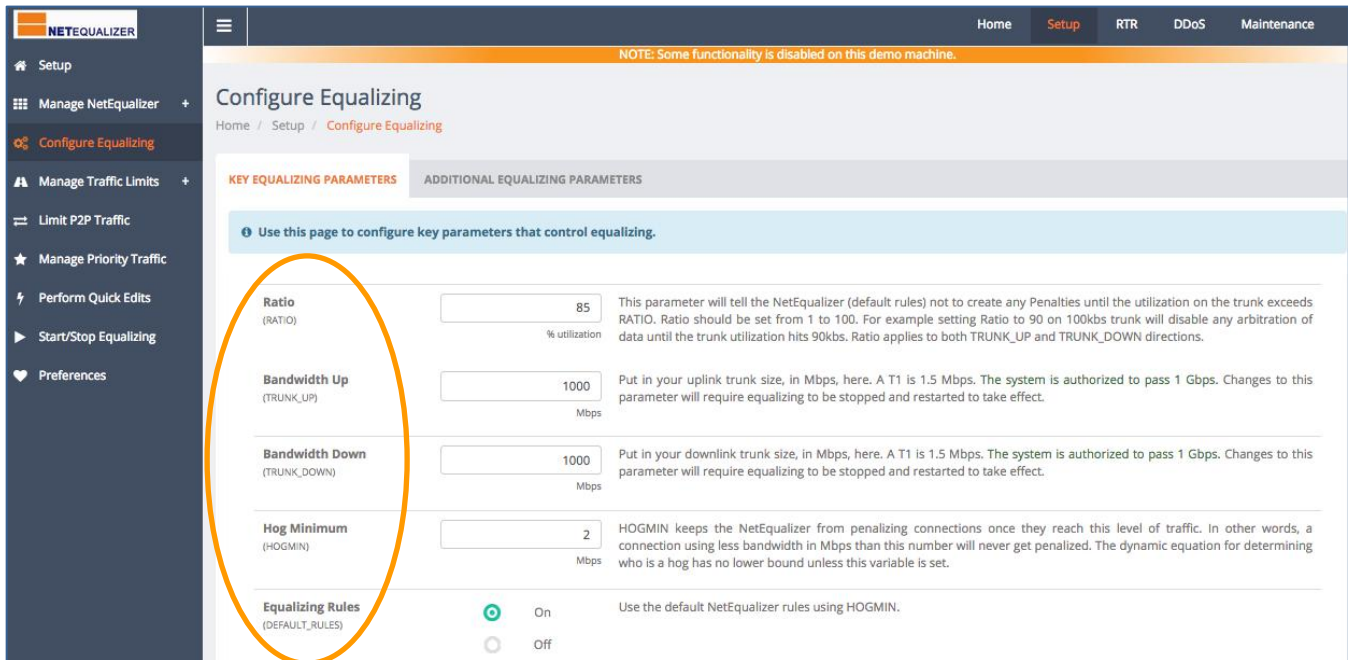


Figure 3: NetEqualizer Dashboard

Note: In this guide, clicking on a button is shown with brackets, such as: Click on -> [Button name]. Clicking on a menu item is shown without brackets, such as: Click on -> Menu name.

Reducing Network Congestion

First, we will discuss how to setup Equalizing to reduce congestion on your network. Equalizing is the most important feature of the NetEqualizer, as this is the key way that we shape bandwidth. There are several parameters that need to be set up in order to equalize, highlighted on the picture below. These are all customizable for your environment. To configure Key Equalizing Parameters, [Click on -> \[Setup\] -> Configure Equalizing](#). The following window comes up, defaulted to the Key Equalizing Parameters tab.



NOTE: Some functionality is disabled on this demo machine.

Configure Equalizing

Home / Setup / Configure Equalizing

KEY EQUALIZING PARAMETERS | ADDITIONAL EQUALIZING PARAMETERS

Use this page to configure key parameters that control equalizing.

Ratio (RATIO)	85 % utilization	This parameter will tell the NetEqualizer (default rules) not to create any Penalties until the utilization on the trunk exceeds RATIO. Ratio should be set from 1 to 100. For example setting Ratio to 90 on 100kbs trunk will disable any arbitration of data until the trunk utilization hits 90kbs. Ratio applies to both TRUNK_UP and TRUNK_DOWN directions.
Bandwidth Up (TRUNK_UP)	1000 Mbps	Put in your uplink trunk size, in Mbps, here. A T1 is 1.5 Mbps. The system is authorized to pass 1 Gbps. Changes to this parameter will require equalizing to be stopped and restarted to take effect.
Bandwidth Down (TRUNK_DOWN)	1000 Mbps	Put in your downlink trunk size, in Mbps, here. A T1 is 1.5 Mbps. The system is authorized to pass 1 Gbps. Changes to this parameter will require equalizing to be stopped and restarted to take effect.
Hog Minimum (HOGMIN)	2 Mbps	HOGMIN keeps the NetEqualizer from penalizing connections once they reach this level of traffic. In other words, a connection using less bandwidth in Mbps than this number will never get penalized. The dynamic equation for determining who is a hog has no lower bound unless this variable is set.
Equalizing Rules (DEFAULT_RULES)	<input checked="" type="radio"/> On <input type="radio"/> Off	Use the default NetEqualizer rules using HOGMIN.

Figure 4: Configure Equalizing - Key Equalizing Parameters

Set the Ratio Parameter

We first set the Ratio Parameter, which determines when Equalizing kicks in. In Figure 4, Ratio is set to the default of "85". This means that your network is considered congested when your traffic reaches 85%.

Set your Network Trunk

We need to tell the NetEqualizer your network trunk size, as Equalizing decisions to balance your traffic are all based off of trunk size. As equalizing is bi-directional, you set both Bandwidth Up (traffic from LAN to WAN) and Bandwidth Down (traffic from WAN to LAN). In Figure 4 above, both Bandwidth Up and Bandwidth Down are set to 1000Mbps (1Gbps).

Define what level of bandwidth use is a Network Hog

During peak times of congestion, Equalizing automatically gives connections less than (<) Hog Minimum priority, while connections >= Hog Minimum are slowed down by adding a latency penalty. Hog Minimum defaults to .5Mbps (62,500 Bps), so that VoIP, email, web applications, and web surfing are all below Hog Minimum. Hog Minimum can be increased based the size of your network pipe and your bandwidth usage patterns. In Figure 4 above, we set Hog Minimum to 2Mbps for our 1Gbps pipe. We provide recommended settings in our Quick Start and full User Guides.

Keep Equalizing Rules set to "ON".

Finally, we make sure Equalizing Rules is set to "ON". Equalizing Rules set to "ON" tells equalizing to kick in and shape your traffic. The NetEqualizer monitors your traffic once a second. When your traffic peaks at Ratio, in our example at 85% percent utilization, equalizing kicks in, automatically shaping your network traffic.

Once these Equalizing parameters are set, the NetEqualizer can prevent brownout and gridlock during peak periods on your network. We will see how the NetEqualizer does this in our next section.

Equalizing in Action

Each row in Figure 5: Active Connections Table below depicts one active connection pair, that is, one local IP address on your network communicating with a remote IP address on the Internet. I have sorted this example by Wavg descending. The 1st row, Index 1, shows a large file download from Host Name ip-107-180-27-177.ip.secureserver.net to IP 192.168.1.113. This file download is consuming a lot of bandwidth, as the Wavg column (weighted average) for this row is an average of 3.1 megabits per second. In contrast, row 2 shows a low bandwidth application, browsing a website, is only .21 Mbps.

In our example, Row 1 (download) is using 15 times the amount of bandwidth of Row 2 (web browsing), and is what we call a "bandwidth hog". You can see in the Figure 5 below that a penalty is being applied to Row 1. During peak periods on the network, our equalizing traffic shaping immediately takes action by creating a temporary policy to slow down Row 1, a bandwidth hog, so that Row 2 and other low bandwidth application traffic continues to flow.

At peak (85% saturation), without traffic shaping you are at risk of what we call gridlock or brownout. When this happens all usage comes to an agonizing crawl and voice calls drop. Equalizing understands this behavior, and shapes your traffic to prevent brownout during peak periods.

This is equalizing in action. It is time-tested as the most effective way to keep your network operating smoothly.

ACTIVE CONNECTIONS Update Data

Use this page to view all active connections running through NetEqualizer.

C = Country Lookup, DNS = DNS Lookup, AR = All Rules Lookup, T = Traffic History, P = Penalty History, P2P = P2P Analysis
NB: Search supports plain text

5 records per page

Index	SRC Port	DST Port	Wavg (Mbps)	Avg (Mbps)	DST	SRC	Plcl	Port	Pool	Penalty
1	50081	54876	3.10	3.82	192.168.1.113 C DNS AR T P P2P	ip-107-180-27-177.ip.secureserver.net. C DNS	TCP	2	5	yes
2	44092	443	0.21	0.22	ec2-54-152-146-218.compute-1.amazonaws.com. C DNS T P	192.168.1.100 C DNS AR T P P2P	TCP	1	0	no
3	54876	50081	0.09	0.11	ip-107-180-27-177.ip.secureserver.net. C DNS	192.168.1.113 C DNS AR T P P2P	TCP	1	5	yes
4	80	54883	< 0.01	0.05	192.168.1.113 C DNS AR T P P2P	192.168.1.143 C DNS AR T P P2P	TCP	2	5	no
5	443	54881	< 0.01	0.05	192.168.1.113 C DNS AR T P P2P	public.comet.vip.bf1.yahoo.com. C DNS T P	TCP	2	5	no

Showing 1 to 5 of 22 entries (processed in 0.00060796737670898 s)

First Previous 1 2 3 4 5 Next Last

large file download → 3.10

web browsing → 0.21

Figure 5: Active Connections Table

The NetEqualizer creators, through careful studies of hundreds of customer networks, have discovered a typical user base behavior. Network users typically mix business-type activities, such as sending emails, accessing web applications, and browsing the web, with recreational activities, such as watching video or downloading music files. Brownout is almost always the result of users monopolizing large amounts of bandwidth for recreational, non-urgent activities. The NetEqualizer prevents brownout by ensuring that recreational activities do not consume all of your available bandwidth.

As every situation is unique, we do also offer ways to identify legitimate video that you wish to run without being shaped. This is typically used sparingly for business or training videos.

Equalizing's fairness-based shaping is an elegant solution to managing your network congestion automatically, as needed. It maximizes the use of your network trunk, and helps to reduce user complaints, all while minimizing network administration required.

Controlling P2P Traffic

In addition to equalizing, if you are concerned about possible P2P (peer-to-peer) traffic on your network, we recommend turning on Connection Limits to control P2P traffic. They work bi-directionally on individual IPs or entire Class B or Class C subnets, to limit both inbound and outbound connections, and are effective on *both encrypted and unencrypted* traffic. Connection Limits will prevent excessive connections from completely overwhelming your routers and access points, not to mention that they could be the major reason all your bandwidth is being consumed.

P2P applications can seek out 100's or 1000's of remote sites on the Internet, running locally from a client on your network. In order to determine whether P2P is running on your network, use our Connection Counts Report to see if any of your IPs are running a huge number of connections. From the Dashboard, [Click on -> \[RTR\]](#). On the RTR Menu, [Click on -> Active Connections -> View Connection Counts](#).

50 records per page

NS: search supports plain text

Index	IP	In	Out	Total
1	192.168.1.113 C DNS AR T P P2P	4	4	8
2	192.168.1.143 C DNS AR T P P2P	1	1	2
3	192.168.1.112 C DNS AR T P P2P	1	1	2
4	192.168.1.100 C DNS AR T P P2P	1	1	2
5	172.217.12.14 C DNS AR P2P	1	1	2
6	172.217.11.228 C DNS AR P2P	1	1	2
7	172.217.11.226 C DNS AR P2P	1	1	2
8	74.125.69.189 C DNS AR P2P	1	1	2
9	54.152.146.218 C DNS AR P2P	1	1	2
Index	IP	In	Out	Total

Showing 1 to 9 of 9 entries (processed in 0.00045990943908891 s)

First | Previous | 1 | Next | Last

Figure 6: View Connection Counts – no P2P traffic

You can see in the example in Figure 6 that each IP is only running a small number of connections, with Totals < 10, as circled in blue above. P2P is not active on this network. If P2P traffic was running, you would see Totals >100.

If you detect P2P traffic, or are concerned about preventing it from consuming your network, set Connection Limits. Connection Limits prevent any IP from consuming 100 or 1000's of connections on your network, effectively blocking P2P traffic. Connection Limits inoculate your network from P2P abuse. From the Dashboard, [Click on -> \[Setup\]](#) -> [Limit P2P Traffic](#). In Figure 7, we use Limit P2P Traffic to set a connection limit for an individual IP (88.91.77.233 /32) and for an entire subnet (192.168.1.0 /24).

NETEQUALIZER

Home Setup RTR DDoS Maintenance

NOTE: Some functionality is disabled on this demo machine.

Limit P2P Traffic

Home / Setup / Limit P2P Traffic

Use this page to set connection limits for P2P traffic.

- Use [Quick Edit P2P Traffic](#) to add and delete connection limits without having to restart equalizing.
- IP addresses are described using [CIDR notation](#) – a CIDR of 32 means "this IP address only".
- Any existing connections do not count towards the limit.
- Since connections are bi-directional, connection limits are rounded to positive even integers.
- Changes to connection limits will require stopping and restarting the equalizing process to take effect.
- No changes are made to the connection limits until they are explicitly saved.

	Host IP	/	CIDR	Connection Limit
1	192.168.1.0	/	24	60
2	88.91.77.233	/	32	2

Save Changes Reset

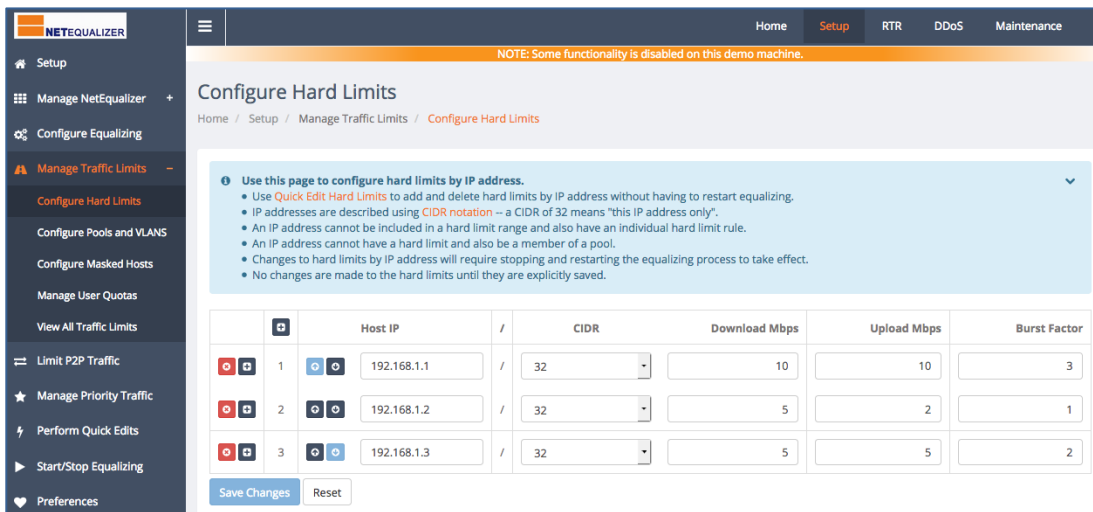
Figure 7: Limit P2P Traffic by setting Connection Limits

Limiting Traffic

In addition to our revolutionary automated equalizing features, we provide a full feature set that allows you to set inbound and outbound bandwidth limits by IP address, entire Class B or C subnets, VLANs, or Pools.

Traffic Limits are useful if you wish to set an upper limit (cap) to the amount of bandwidth that can be used. We offer two types of limits, individual and shared. Hard Limits are individual limits, giving a defined amount of bandwidth to each user (IP). Pools and VLAN Limits are used to share a defined amount of bandwidth across a “pool” of users (IPs). While not demonstrated here, you can also define User Quotas to limit traffic over time by user (IP) or IP subnet.

From the Dashboard, [Click on -> \[Setup\] -> Manage Traffic Limits](#). Then [Click on -> Configure Hard Limits](#) to set inbound and outbound limits by IP address, or Class B or Class C subnets. Hard Limits are additive. All IPs in the hard limit range EACH get the defined bandwidth. In our example in Figure 8, 192.168.1.1 /32 is limited to 10Mbps up and down.



Configure Hard Limits

Home / Setup / Manage Traffic Limits / Configure Hard Limits

NOTE: Some functionality is disabled on this demo machine.

Use this page to configure hard limits by IP address.

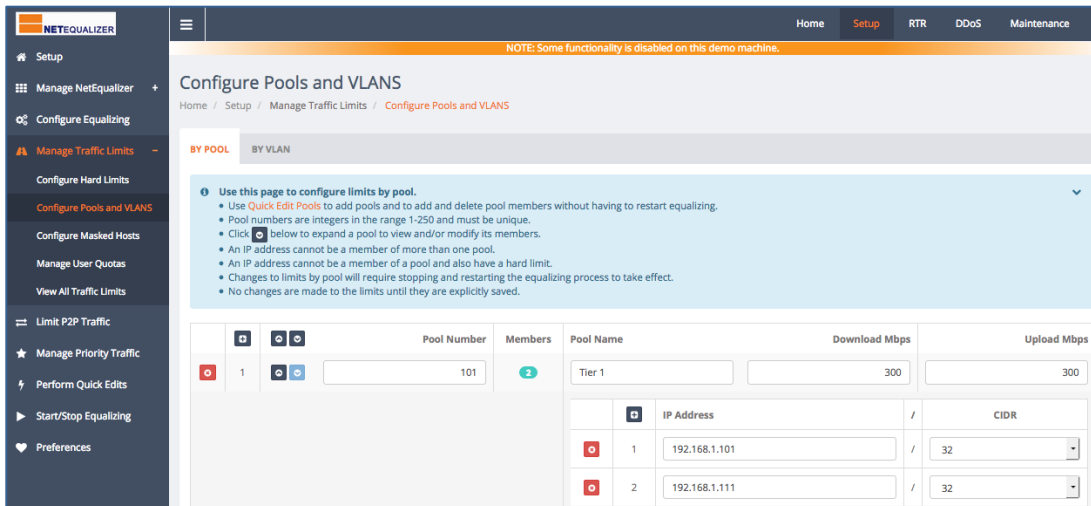
- Use **Quick Edit Hard Limits** to add and delete hard limits by IP address without having to restart equalizing.
- IP addresses are described using **CIDR notation** – a CIDR of 32 means “this IP address only”.
- An IP address cannot be included in a hard limit range and also have an individual hard limit rule.
- An IP address cannot have a hard limit and also be a member of a pool.
- Changes to hard limits by IP address will require stopping and restarting the equalizing process to take effect.
- No changes are made to the hard limits until they are explicitly saved.

	Host IP	CIDR	Download Mbps	Upload Mbps	Burst Factor
1	192.168.1.1	32	10	10	3
2	192.168.1.2	32	5	2	1
3	192.168.1.3	32	5	5	2

Save Changes Reset

Figure 8: Configure Hard Limits

From the Dashboard, [Click on -> \[Setup\] -> Manage Traffic Limits](#). Then [Click on -> Configure Pools and VLANs](#) to set up limits by Pool, which enable all IPs and IP subnets within the Pool to **SHARE** bandwidth. In our example in Figure 9 below, Pool #101, named Tier 1, is limited to 300 Mbps up and down and has two (2) Pool members. Each Pool member can use a portion of the 300Mbps available. While we do not show it here, VLAN Limits work the same as Pools, set up by VLAN id. Pools are typically set up to align with access points, buildings, or groups of people, such as departments.



Configure Pools and VLANs

Home / Setup / Manage Traffic Limits / Configure Pools and VLANs

NOTE: Some functionality is disabled on this demo machine.

BY POOL BY VLAN

Use this page to configure limits by pool.

- Use **Quick Edit Pools** to add pools and to add and delete pool members without having to restart equalizing.
- Pool numbers are integers in the range 1-250 and must be unique.
- Click **+** below to expand a pool to view and/or modify its members.
- An IP address cannot be a member of more than one pool.
- An IP address cannot be a member of a pool and also have a hard limit.
- Changes to limits by pool will require stopping and restarting the equalizing process to take effect.
- No changes are made to the limits until they are explicitly saved.

	Pool Number	Members	Pool Name	Download Mbps	Upload Mbps
1	101	2	Tier 1	300	300

	IP Address	CIDR
1	192.168.1.101	32
2	192.168.1.111	32

Figure 9: Configure Pools and VLANs – By Pool tab

Monitoring for Possible DDoS Attacks

A Distributed Denial of Service Attack (DDoS) occurs when a hacker illicitly gains access to a system, takes it over, and then uses it to command many systems to flood a target network with traffic. The flood of traffic quickly overwhelms the target network, and causes the network to become inoperable for its normal purposes.

The NetEqualizer enables you to monitor for DDoS activity through our DDoS Monitor. The DDoS Monitor is used to analyze *unrequested incoming traffic* to look for inbound traffic that occurs both at high frequency and is repeated a large number of times, which is behavior typical of a DDoS attack. From the Dashboard, [Click on -> \[DDoS\]](#).

DDoS Monitor

DDOS MONITOR Update Data

C = IP to Country Lookup, DNS = DNS Lookup, AR = All Rules Lookup, T = Traffic History by IP

Use this page to view all uninitiated requests running through the NetEqualizer.

25 records per page Search:

Index	SRC IP	DST IP	Port	Seconds	Count	Rate	Blocked
0	10.0.10.104 C DNS AR T	10.0.10.2 C DNS AR T	2	25	66	2	no
1	10.0.10.102 C DNS AR T	10.0.10.2 C DNS AR T	2	116	1930	16	no
2	10.0.10.108 C DNS AR T	10.0.10.2 C DNS AR T	2	93	2355	25	no
3	10.0.10.107 C DNS AR T	10.0.10.2 C DNS AR T	2	25	49	1	no
4	10.0.10.109 C DNS AR T	10.0.10.2 C DNS AR T	2	2	6	3	no
5	10.0.10.106 C DNS AR T	10.0.10.2 C DNS AR T	2	99	2756	27	no
6	10.0.10.103 C DNS AR T	10.0.10.2 C DNS AR T	2	16	32	2	no
Index	SRC IP	DST IP	Port	Seconds	Count	Rate	Blocked

Showing 1 to 7 of 7 entries (processed in 0.00045895576477051 s) First Previous 1 Next Last

Figure 10: DDoS Monitor

The DDoS Monitor displays all uninitiated requests coming into your network. You can see how persistent the request is (Seconds) and how often it is hitting your network in the last second (Rate), which then gives you an overall view (Count) of how active the attack is. For example, in our table above, Index 5 has been running for 99 seconds, hitting the network 27 times per second, for a total of 2,756 hits.

By analyzing the values of Count, Rate, and Seconds, you can identify which external IP addresses you want to block. In Figure 10 above, Index #1, #2, and #5 are candidates to consider blocking.

If you decide you need something more proactive to mitigate a DDoS attack, we offer a DDoS Firewall (DFW) feature, and provide consulting to help you configure it to block standard DDoS attacks. The DDoS Firewall tool (DFW) can be purchased as a NetEqualizer add-on module.

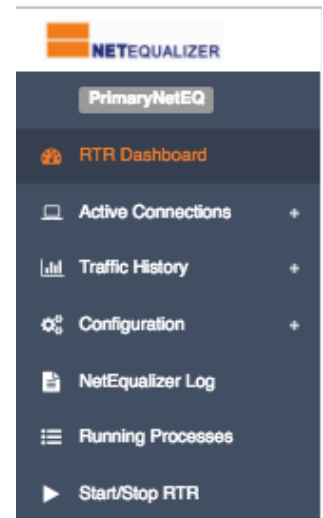
NetEqualizer Monitoring & Reporting

NetEqualizer Real-Time Reporting (RTR) enables you to monitor and report on your network traffic. Real-Time Reporting provides both real-time (Active Connections) and historical reporting (Traffic History), in both tabular and graphical formats. Active Connections show you what is happening right now on your network. Traffic History Reports are available in timeframes up to 4 weeks.

One of the things that has always differentiated the NetEqualizer from other monitoring and shaping tools is that *we have the actual data for every user accurately updated by the second*. Thus, we are able to make shaping decisions based on usage every second. RTR gives you visibility into real-time network traffic and can help you to get a sense of "what is going on now" on your network. They can also be used to see bandwidth usage trends over time, in troubleshooting efforts, and to help with capacity planning.

From the Dashboard, [Click on -> \[RTR\]](#). The RTR Reports Menu and the RTR Dashboard will be displayed. Key areas of the RTR Menu are described below. Popular report examples follow:


- **RTR Dashboard** - Graphical view of traffic in real-time flowing through NetEqualizer. Also shows traffic in Pools.
- **Active Connections** - Sortable and searchable real-time tabular view of all connections, # of connections, or penalties active on the NetEqualizer at this moment. Also includes Quota Reports and P2P Analyzer.
- **Traffic History** - Graphs that show up to 4 weeks worth of upload and download bandwidth usage or penalties for your entire network, selected IPs, VLANs or Pools. Also shows upload and download Top Talkers on your network.
- **Configuration** - View how you have defined key parameters, traffic limits, priorities, and P2P limits. Use to validate your settings.
- **NetEqualizer Log** - Displays key activity on the NetEqualizer, such as limits being applied, and penalties being added or removed.



Active Connections

For a live look at the BRAIN table of the NetEqualizer, from the Reports Menu, [Click on -> Active Connections](#). In Figure 11 below, you can view the **Active Connections Table**, which shows each connection and the bandwidth (Wavg and Avg) it is consuming on the network. Active Connections is sortable and searchable, so that you can focus on the connections you are most interested in viewing. Use this to easily find bandwidth hogs by sorting on Wavg and displaying largest to smallest (descending).

In Figure 11, Index #1 has the largest bandwidth usage, at 17.26 Mbps, and is being equalized (penalty = yes). You can click on a symbol below any IP address (C, DNS, AR, T, P) to view associated IP-level reports. You can also search by any IP address to view all traffic for any particular user.

100  records per page

Search:












Index 	SRC Port 	DST Port 	Wavg (Mbps) 	Avg (Mbps) 	DST 	SRC 	Pttl 	Port 	Pool 	Penalty 
1	443	60328	1.774144	17.259304	192.168.1.113 C DNS AR T P	173.194.54.216 C DNS AR P	TCP	2	3	yes
2	57137	443	0.19148	0.154064	ec2-54-152-146-218. compute-1.amazonaws. com. C DNS T	192.168.1.100 C DNS AR T P	TCP	1	0	no
3	60328	443	0.057016	0.537632	173.194.54.216 C DNS AR P	192.168.1.113 C DNS AR T P	TCP	1	3	yes
					public1.comet.vpn.qq1.					

Figure 11: Active Connections Table

IP Reports & Traffic History

In Figure 11 above, if you click on a symbol (C, DNS, AR, T, P) below any individual IP address or Host Name, you will bring up the appropriate IP-level Report. Click on -> "T" (Traffic by IP). This will bring up the **Traffic History by IP Graph**, which shows bandwidth usage over time for the selected IP or Host Name, as shown in Figure 12 below. In this case, we clicked on a Host Name, ec2-54-152-146-218.compute-1.amazonaws.com, in Row #2 of Figure 11. The graph defaults to the last 1 hour. You can see that as I clicked through on a Host Name, the "Filter data: by Host Name" field is populated. The graphs displays selected bandwidth usage: upload, download, or both. In our example 58.39MB of data has been downloaded in the last 1 hour.

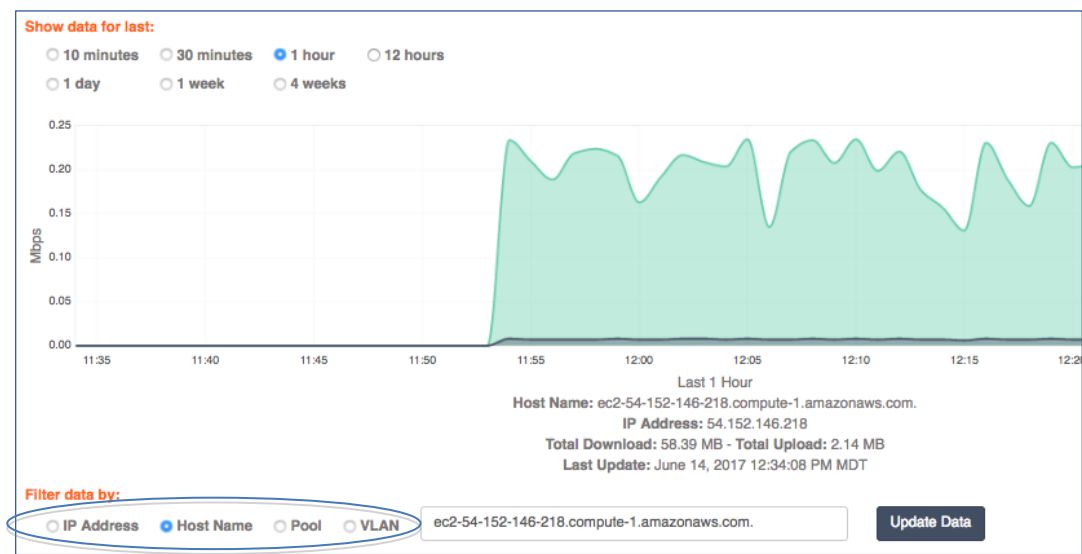


Figure 12: Traffic History by Host Name

Each Traffic History report/graph is available in time increments from 10 minutes to 4 weeks, so that you can focus on real-time analysis and troubleshooting, or zoom out to see trends over time for capacity planning. We also enable you to export data to a server to study over longer periods of time. As this is a huge amount of data (traffic across all IPs), a separate reporting data warehouse should be used. For most troubleshooting, capacity planning, and trend analysis, we find 4 weeks of data will suffice.

NetEqualizer Log

We offer a view into the **NetEqualizer Log**, where you can see key activity on the NetEqualizer, including penalties being applied (traffic slowed down) or removed (traffic speeding up). In the example in Figure 13 below, you can see a NEW PENALTY (in orange) on line #419 of the Log, and then PENALTY INCREASES (in red) on line #s 420, 421, and 426.

Line #	Type	Value
426	INCREASE	08/15/17 12:17:21 INCREASE PENALTY IP: 192.168.1.113 107.180.27.177 POOL: 5 Traffic Up: 7532 Traffic Down: 286102 Hogmin: 10000 VLAN: TCP BUFF: 1499 DELAY: 45 TOS: 1
425	INFO	08/15/17 12:17:21 Traffic up: 7532 Traffic down: 286102 POOL 5
424	INFO	08/15/17 12:17:21 Traffic up: 1 Traffic down: 1 POOL 3
423	INFO	08/15/17 12:17:21 Traffic up: 25583 Traffic down: 282106 POOL 0
422	INFO	08/15/17 12:17:21 Traffic up: 1 Traffic down: 1 POOL 4
421	INCREASE	08/15/17 12:17:15 INCREASE PENALTY IP: 192.168.1.113 107.180.27.177 POOL: 5 Traffic Up: 2810 Traffic Down: 112010 Hogmin: 10000 VLAN: TCP BUFF: 1499 DELAY: 40 TOS: 1
420	INCREASE	08/15/17 12:17:09 INCREASE PENALTY IP: 192.168.1.113 107.180.27.177 POOL: 5 Traffic Up: 19809 Traffic Down: 558734 Hogmin: 10000 VLAN: TCP BUFF: 1499 DELAY: 35 TOS: 1
419	NEW PENALTY	08/15/17 12:17:07 PENALTY IP : 107.180.27.177 192.168.1.113 POOL: 5 Traffic Up: 28884 Traffic Down: 1019729 Hogmin: 10000 VLAN: TCP WAVG: 11639 BUFF: 1498 DELAY: 5 TOS: 1
418	INCREASE	08/15/17 12:17:03 INCREASE PENALTY IP: 192.168.1.113 107.180.27.177 POOL: 5 Traffic Up: 3902 Traffic Down: 255999 Hogmin: 10000 VLAN: TCP BUFF: 1499 DELAY: 30 TOS: 1
417	REMOVE	08/15/17 12:17:02 PENALTY REMOVE: 107.180.27.177 192.168.1.113 POOL: 5 TOS: 1
Line #	Type	Value

Figure 13: NetEqualizer Log

Where to Install the NetEqualizer

The NetEqualizer operates as a transparent bridge on your network. There is typically no need to change anything in your network configuration to install the appliance. Simply install the NetEqualizer between your Firewall/Router and Network Switch, or anywhere on your network that you can "see" the individual IP addresses and bandwidth that you want shaped. Once installed, you will use the Management Port and the Factory Default Settings to access it via a web Graphical User Interface.

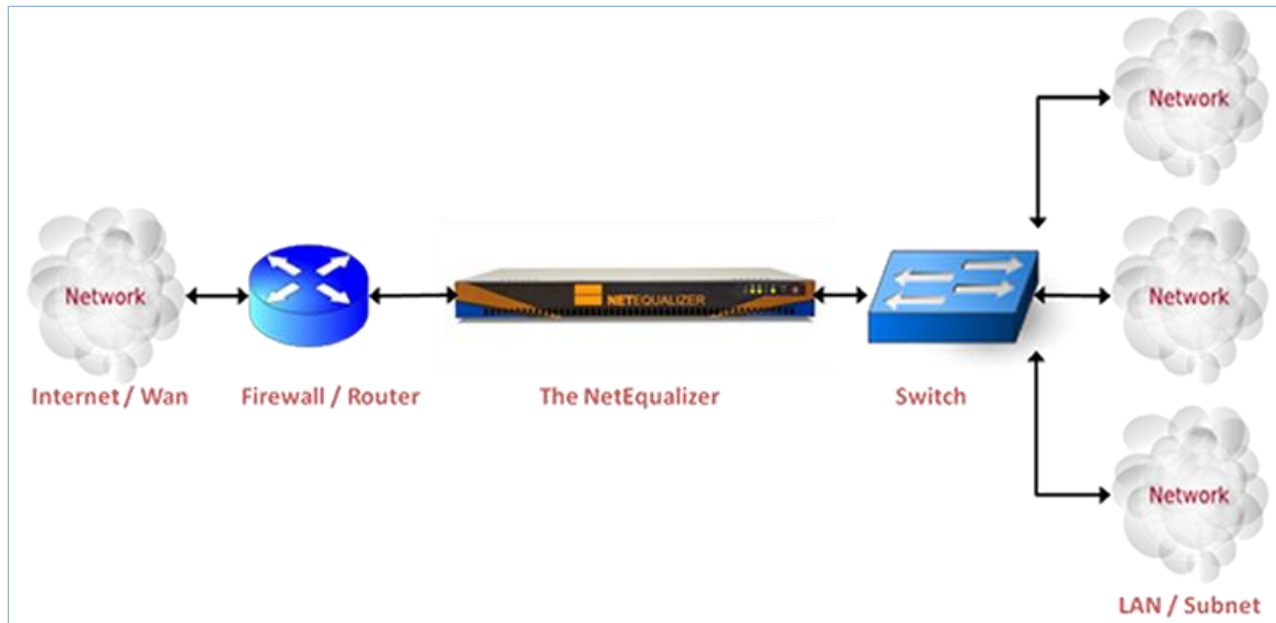


Figure 14: NetEqualizer Installation

Congratulations!
You made it through the Product Demonstration Guide.

*If you had your own NetEqualizer, it would be up & running now,
automatically solving your network congestion.*

Interested in learning more?
Contact Sales: sales@apconnections.net or call 303.997.1300 x103.