

XRoads Networks

Edge Network Appliance How To Guide: Shaping

Edge Network Appliance How To Guide:

Shaping

©2007 XRoads Networks

17165 Von Karman, Suite 112
888-9-XROADS

Table of Contents

4 **Shaping Overview**

Components

- 4 User/Device Management
- 7 Application Shaping
- 9 VoIP Flow Control
- 9 P2P Flow Control
- 11 Scope-Based Shaping
- 12 Policy-Based Shaping

Edge Configuration Series

Shaping Overview

The Shaping menu is where one can control the application routing and traffic shaping functions of the Edge appliance.



- User/Device Management: Enables the ability to tie traffic flows to specific end-users based on their IP address.
- Application Shaping: Enables quick and easy prioritization of critical applications used within your network.
- VoIP Flow Control: Easily prioritize VoIP applications such as SIP, Vonage and VoIP PBX systems. Guarantees bandwidth for VoIP.
- P2P Flow Control: Prevent access to common peer-to-peer and instant messaging applications. Maintain control over sessions per end-user.
- Scope Based Shaping: Used to shape network usage by end-users during high traffic usage. Ensures available bandwidth for critical applications.
- Policy Based Shaping: Granular bandwidth control and prioritization for end-users and network nodes. Group based bandwidth control with high level statistical reporting and monthly totals.

User/Device Management

This feature enables the administrator to easily build IP host definitions in order to produce better reporting and bandwidth shaping policies. These definitions can be entered via the web GUI or by uploading a list of users.

The following screen shot shows example IP host definitions:

Select	Username	Description	Group	IP Addr	MAC Addr	Shaping Group
<input type="radio"/>	gorgec	Curious	Engineering	192.168.168.12		No Shaping
<input type="radio"/>	pres	Big Cheese	Executive	192.168.168.100		No Shaping
<input type="radio"/>	jsmith	John Smith	Sales	192.168.168.25		test

NOTE: Future versions of this module will be fully compatible with standard LDAP directories, including Active Directory.

Add Host Definition Via GUI

In order to create a new definition based using the GUI, select the Add User/Device button from the IP host list screen.

The screenshot shows a web interface for 'User/Device Management'. On the left is a dark blue sidebar with navigation links: 'Edge Routing', 'Contact Information', 'System Identification', 'Bandwidth Enforcement', and 'Remote PPTP Access'. The main content area has a title 'User/Device Management' and a dropdown menu. Below are several input fields with labels and help text:

- Name:** (Name for this user/device, i.e. webserver or jsmith). NOTE: This name is used to identify the user/device within the network reporting.
- Internal ID:** (Internal identification number for this user/device)
- Description:** (Description or comment for this user/device)
- Department / Group:** (Department / Group for this user/device, used for global reporting)
- IP Address:** (Enter the IP address for this user/device). NOTE: The IP address is used to identify the user/device within the network reporting.
- MAC Address:** (Enter the MAC address for DHCP binding - Example: 00:09:FB:03:CF:02)
- DHCP Allocation:** Provide DHCP address allocation for this user.
- Bandwidth Shaping:** A dropdown menu set to '--- No Shaping ---'. (Policy-Based Shaping group assigned to this user/device)
- PPTP Login:** (Enter the PPTP login name to allow remote access for this user, optional)
- PPTP Password:** (Enter the PPTP password for this user)
- Re-enter PPTP Password:** (Re-enter the PPTP password)

At the bottom are three buttons: 'Reset', 'Add / Update', and 'View Users/Devices >>'.

When adding a new IP host definition you have several options beyond the basic name and description of the host, these additional options include:

- 1 DHCP address binding to a MAC address.
- 2 Default bandwidth shaping policy (based on groups setup in Policy Shaping, which is outlined in the Policy Shaping section of this guide).
- 3 PPTP configuration for this IP host.

The process for creating a definition via the GUI is as follows:

- 1 Enter a user/device name.
- 2 Enter an identifying alphanumeric number for this host (if any).
- 3 Enter a description for this host.
- 4 Enter a group name for this host (will be used in the future for grouping hosts)
- 5 Enter the IP address for this host (if dynamic, use the DHCP settings and specify a MAC address for this host and use an IP address within the DHCP range).
- 6 Select a bandwidth group to assign to this host (if any)
- 7 Enable PPTP for this host (if applicable)

NOTE: See the PPTP section of the Firewall HowToGuide for more information on PPTP configuration.

Add Host Definitions Via CSV:

When adding many users, it may be easier to enter the users via a bulk import. This can be done by selecting the CSV Input button from the main page.

```
User/Device Name, Internal ID, Description, Group ID, IP Addr, MAC Addr, DHCP (on/off), Shaping Group, PPTP Login, PPTP Password
(NOTE: Always include a '+' at the end of each line)
gorgec,4509348,Curious,Engineering,192.168.168.12,,0,No Shaping,gorge,password+
pres,100000,Big Cheese,Executive,192.168.168.100,,0,No Shaping,,+
jamith,349384,John Smith,Sales,192.168.168.25,,0,test,,+
```

In order to properly add IP hosts via this method, make sure to include the following information in the proper order:

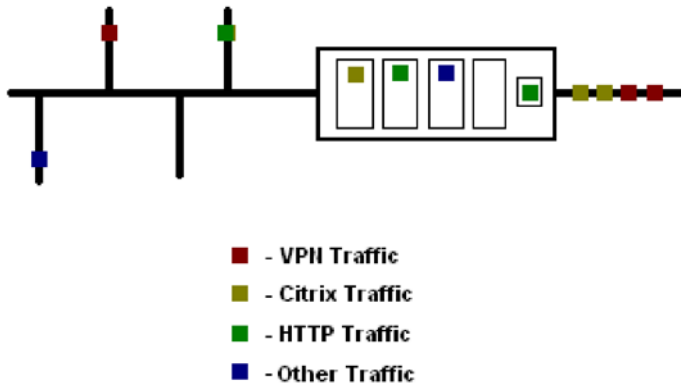
- 1 User/Device Name
- 2 Internal ID (if any)
- 3 Description
- 4 Group Name (if any)
- 5 IP Address (must be within the DHCP range if dynamic)
- 6 MAC Address (if dynamic)
- 7 DHCP on/off (on if dynamic)
- 8 Enter the shaping group (or enter 'No Shaping')
- 9 PPTP Login Name

NOTE: Use ',' between each field and a '+' at the end of each line. Do not use either of these characters in any of the actual fields or the import will not work correctly.

Application Shaping

The Edge XOS has made ensuring high prioritization of some of the most common critical network applications. This feature uses packet queuing techniques to ensure that critical network applications receive high priority when multiple applications are traversing the Edge appliance at the same time.

The example below shows the various queues within the Edge appliance. Each queue is assigned a different priority. Based on algorithms within the Edge XOS and inputs by the administrator the Edge will empty each queue based on their predefined priorities. Accelerated applications are automatically set to the highest priority.



There are five levels of bandwidth guarantee which can be assigned to various critical applications. Each level can be set with its own priority and bandwidth level. These levels are then assigned to those applications which are critical within your own network. The fifth level is the default level where all non-defined traffic will be regulated.

Application Shaping ▼

Enabled Disabled (Application Acceleration Services)

Level 1 - Bandwidth Guarantee	<input type="text" value="40"/>	% - Priority	<input type="text" value="1"/>
Level 2 - Bandwidth Guarantee	<input type="text" value="20"/>	% - Priority	<input type="text" value="2"/>
Level 3 - Bandwidth Guarantee	<input type="text" value="5"/>	% - Priority	<input type="text" value="3"/>
Level 4 - Bandwidth Guarantee	<input type="text" value="5"/>	% - Priority	<input type="text" value="4"/>
Default - Bandwidth for all non-classified applications	20 %	- Priority	<input type="text" value="5"/>

NOTE: These bandwidth guarantees are applied based on the bandwidth levels which are defined in the LAN and WAN interfaces. They also allow other application to use available bandwidth when critical applications are not in use.

Once you have set the bandwidth and priority for each level, the next step is to assign a level to a specific application and then enable the shaping for that application. Example: To enable SSL shaping, check the select box, then select the level which you configured above, and select when these shaping parameters will apply.

Select	Status	Group	Description	Level	Active@
<input type="checkbox"/>	Disabled	Internet	HTTPS Web SSL (Secure Sockets Layer)	Level1	Always On
<input checked="" type="checkbox"/>	Enabled	VoIP	SIP Protocol Support	Level1	Always On
<input checked="" type="checkbox"/>	Enabled	VoIP	RTP (Real Time Protocol)	Level1	Always On
<input checked="" type="checkbox"/>	Enabled	Client-Server	Citrix Services	Level1	Always On
<input type="checkbox"/>	Disabled	Database	Microsoft SQL Database	Level1	Always On
<input type="checkbox"/>	Disabled	Messaging	POP3 (Post Office Protocol)	Level1	Always On
<input type="checkbox"/>	Disabled	Messaging	Microsoft Exchange Support	Level1	Always On
<input type="checkbox"/>	Disabled	Internet	FTP (File Transfer Protocol)	Level1	Always On
<input checked="" type="checkbox"/>	Enabled	Internet	HTTP Web Browser Service	Level2	Always On

NOTE: The Active@ section allows the administrator to ONLY apply these shaping levels when total bandwidth usage has reach a certain percentage, i.e. at 80%.

VoIP Flow Control

The Edge appliance provides a simple and effective method for easily prioritizing and guaranteeing bandwidth for VoIP applications.

As the use of VoIP becomes more prevalent so do the potential pitfalls. The Edge appliance addresses two of the greatest concerns in both reliability (our multi-WAN capability with automatic failover) and quality of service (our traffic shaping engine).

In most cases, the Edge appliance can ensure guaranteed VoIP performance by:

- (A) Creating a prioritized queue for all VoIP based traffic.
- (B) Creating a separate bandwidth group specifically to allocate the necessary bandwidth needed for VoIP traffic.



The screenshot shows a configuration panel for 'VoIP Flow Control'. At the top is a dropdown menu with 'VoIP Flow Control' selected. Below it are two radio buttons: 'Enabled' (selected) and 'Disabled (VoIP Optimization Services)'. A note states: 'When enabled VoIP is automatically assigned Priority 1 application queuing.' Below this is a text input field containing '10%' with the label '- VoIP Bandwidth Partitioning (Default: 10%)'. At the bottom are two buttons: 'Update (Update VoIP partitioning settings)' and 'Apply Policies (Apply updated settings)'.

Enabling VoIP Optimization

Click the Enable button and enter the information requested regarding your VoIP deployment. Enter the amount of bandwidth you wish to allocate for VoIP traffic. Remember all VoIP traffic will be forwarded to this group when enabled.

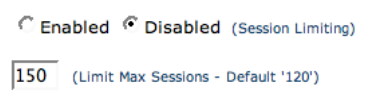
NOTE: Always allocate more bandwidth than needed when setting up VoIP guarantees to ensure overflow is not required.

P2P Flow Control

This feature provides protection from over-subscription of network bandwidth by peer-to-peer applications like Napster, KaZaA and others.

Session Limiting

The session limiting feature allows the administrator to place a cap on the number of new sessions which an end-user can initiate within a short period of time.



The screenshot shows a configuration panel for 'Session Limiting'. It features two radio buttons: 'Enabled' (selected) and 'Disabled (Session Limiting)'. Below the buttons is a text input field containing '150' with the label '(Limit Max Sessions - Default '120')'.

Session limiting is particularly effective on P2P applications which attempt to open many new sessions in order to download music files, etc. This feature minimizes the impact of those applications.

P2P/IM Blocking

The Edge XOS can block both peer-to-peer and instant messaging application by using its deep packet inspection and layer-7 classification technology. The Edge is able to monitor network flows and identify specific types of applications even when they are using standard ports like 80 for standard web traffic.

To enable P2P/IM blocking, simply select the Enable button.

Select	Status	Name	Description
<input checked="" type="checkbox"/>	On	AIM1	Instant Messaging AOL
<input checked="" type="checkbox"/>	On	AIM2	Instant Messaging AOL2
<input type="checkbox"/>	Off	XDCC	Instant Messaging IRC
<input checked="" type="checkbox"/>	On	MSN1	Instant Messaging MSN
<input checked="" type="checkbox"/>	On	MSN2	Instant Messaging MSN
<input type="checkbox"/>	Off	Yahoo	Instant Messaging Yahoo
<input type="checkbox"/>	Off	iTunes	Media Application
<input type="checkbox"/>	Off	QuickTime	Media Application
<input type="checkbox"/>	Off	ShoutCast	Media Application
<input type="checkbox"/>	Off	RTP	Media Application (Real Time Protocol)
<input type="checkbox"/>	Off	AppleJuice	P2P Application
<input type="checkbox"/>	Off	Ares (Best Effort)	P2P Application
<input type="checkbox"/>	Off	Azureus	P2P Application
<input type="checkbox"/>	Off	BitPump	P2P Application
<input type="checkbox"/>	Off	BitTornado	P2P Application
<input checked="" type="checkbox"/>	On	BitTorrent	P2P Application
<input checked="" type="checkbox"/>	On	BitTorrent2	P2P Application

Once enabled, you need to select those P2P and IM applications that you wish to block. To do this, simply click the checkbox next to the application in question.

NOTE: New P2P applications are being developed all the time. It is recommended that you obtain our maintenance package in order to receive the latest P2P/IM application signature updates.

Scope Based Shaping

This feature is commonly used by IT administrators to maintain an even distribution of bandwidth for end-users within a corporate or education environment. By simply defining a network scope and setting the inbound/outbound bandwidth thresholds no single user is able to use up network bandwidth.

Scope Based Shaping
▼

(Enter a description for this shaping scope)

(Enter a range of addresses for this scope)

Always On ▼ (Select when this scope will be applied)

(Set the maximum LAN>WAN bandwidth per address for this scope in kbps)

(Set the maximum WAN>LAN bandwidth per address for this scope in kbps)

Reset
Add / Update
Scope List >>

To create a scope:

- 1 Enter a name for the scope.
- 2 Define the scopes range 10.10.10.1 – 64 (will apply the bandwidth shaping rules to all addresses between 1 and 64)
- 3 Determine when these rules will apply.
 Note: The scope rule can always apply, or only when the total bandwidth reaches a certain percentage.
- 4 Allocate the maximum bandwidth that this user can use for uploads.
- 5 Allocate the maximum bandwidth that this user can use for downloads.

The scope rule will take effect once the Apply Policies button is selected. This button is found under the Scope List.

Total Policy Count = 45

Select	Scope Name	Network Scope	When Active	Outbound Rate	Inbound Rate	Policy Count
↻	manatv	125.8.17.1 - 28	90% Utilization	3000 Kbps	3000 Kbps	27
↻	manatv	125.8.17.20 - 28	90% Utilization	3000 Kbps	3000 Kbps	8
↻	manatv	125.8.17.20 - 30	90% Utilization	3000 Kbps	3000 Kbps	10

Policy Based Shaping

Traffic Shaping is a highly configurable feature that enables Edge administrators to completely control their network bandwidth. Traffic Shaping provides the ability to prioritize traffic, rate-limit users, and set QoS flags on outgoing packets.

Prioritizing traffic is basically the ability to determine which service and/or user gets access to bandwidth first. Those services and/or users with a high priority receive preferential treatment for allocated bandwidth within the each interface queue.

Rate-limiting sometimes called rate-shaping enables the administrator to control how much bandwidth an individual service or user may have going through the Edge device. This in effect sets the bandwidth limit for that particular service and/or user. For example, if you wish to set a group of users not to exceed 384Kbps, that can be done using the rate-limiting feature.

QoS (Quality of Service) is a flag set within an IP packet which tells downstream routers how to handle those packets. The problem with QoS only bandwidth management is that many routers do not support the QoS flag. QoS is useful when connecting multiple Edges device together as they can provide end-to-end QoS for applications like VoIP, Citrix, and others.

Edge Routing: Policy Based Shaping

Shaping Policy: big **Bandwidth Groups** (Select an existing, or create a new bandwidth group)

End User: gorgec (Select a user from Tools->EndUser Management)

OR

Layer Three Shaping: [] . [] . [] . [] (Enter an address or a range of addresses)
OR select 'ANY' from Network Mask to specify any host address

Service: SINGLE HOST (Network Mask)

Destination: (Define a Source or Destination for the address/network)

Service: ANY **New Service**

Source: (Define the Source or Destination for the port)

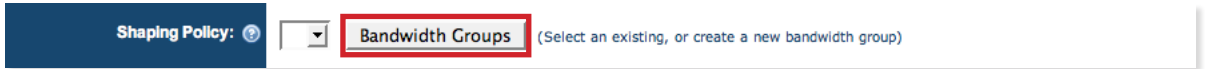
(When checked both an inbound and outbound rule will be created for non-range entries)

Class Of Service: No Change (DiffServ DSCP/ToS 802.1p packet marking for this shaping policy)

Reset Add / Update View Policies >> Apply Policies

Configuring Traffic Shaping

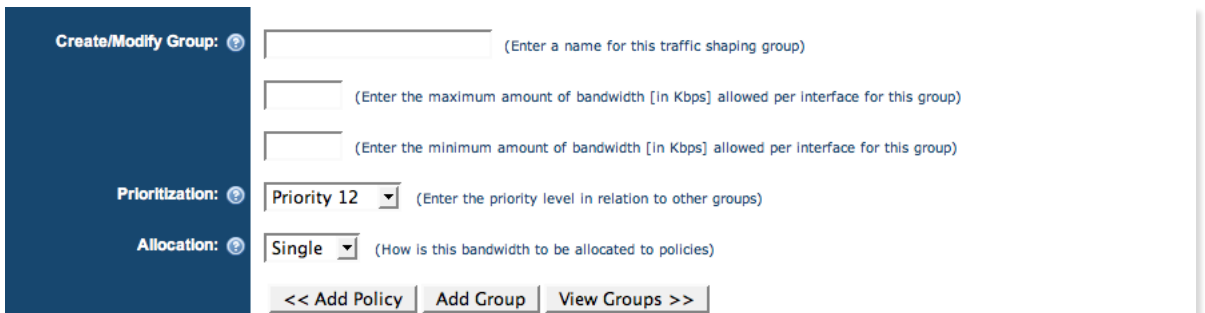
To configure traffic shaping the first step is to create a bandwidth group. The bandwidth group determines the maximum and minimum bandwidth speeds associated with this group. Click the “Bandwidth Groups” button to create a new group.



Shaping Policy: ⓘ ▼ **Bandwidth Groups** (Select an existing, or create a new bandwidth group)

Create A Bandwidth Group

Now enter a NAME that will be assigned to this group. Then enter the MAX and MIN bandwidth speeds for this group (example: 384 or 512 or 1544 = T1 line). Do not add ‘Kbps’ after the number as this is added automatically. All entries are entered in Kbps, so a 10Mbps rate would be entered as 10000.



Create/Modify Group: ⓘ

(Enter a name for this traffic shaping group)

(Enter the maximum amount of bandwidth [in Kbps] allowed per interface for this group)

(Enter the minimum amount of bandwidth [in Kbps] allowed per interface for this group)

Prioritization: ⓘ Priority 12 ▼ (Enter the priority level in relation to other groups)

Allocation: ⓘ Single ▼ (How is this bandwidth to be allocated to policies)

<< Add Policy Add Group View Groups >>

Setting Prioritization

At this point the administrator may also choose to set a priority for this group. All policies tied to this group will assume this priority. It is recommended that the default be used unless this bandwidth group is specifically going to be used for assigning application priorities.

Once the settings have been entered click the “Add Group” button.

Defining How The Policy Is Applied (Single or Shared)

Each bandwidth group can be applied either on a single basis, i.e. the amount of bandwidth in the group is assigned to each policy independently, or on a shared basis, i.e. the bandwidth is shared by all policies in a group.

Group Listing

At this point a list of bandwidth groups will appear. This list shows all of the currently configured groups and their associated settings.

When deleting a group, ALL associated policies will also be deleted.

To modify an existing group, simply select the group to modify and click the "Select Group" button. This will effect all policies assigned to this group.

Select	Group Name	MAX (Kbps)	MIN (Kbps)	Priority	Shared
	big	1500	1500	3	NO
	shared	10000	10000	6	YES
	small	50	50	12	NO
	test	64	64	2	NO

Creating Policies

Once a bandwidth group has been defined, shaping policies can then be assigned to the group. Shaping policies are defined on the main Traffic Shaping menu by entering the MAC address, the IP address, or the service type of the desire policy.

Policy Based Shaping

big Bandwidth Groups (Select an existing, or create a new bandwidth group)

(Policy Name)

gorgec (Select a user from Tools->EndUser Management)

OR

(Enter an address or a range of addresses)

OR select 'ANY' from Network Mask to specify any host address

SINGLE HOST (Network Mask)

Destination (Define a Source or Destination for the address/network)

ANY New Service

Source (Define the Source or Destination for the port)

(When checked both an Inbound and outbound rule will be created for non-range entries)

No Change (DiffServ DSCP/ToS 802.1p packet marking for this shaping policy)

The following shaping policies can be defined:

- IP Address (single or range)
- IP Network
- Service Type
- IP Address/Network AND Service Type

Additionally, the QoS bit can be controlled via the shaping policy allowing for more granular control within a particular bandwidth group.

Shaping Based On IP Address

A common method for shaping bandwidth traffic, the IP address of the target device is entered into the Layer Three Shaping parameter. A range of addresses may also be specified. If specifying a single address OR a range of addresses, make sure to select SINGLE HOST from the Network Mask drop-down menu.

Additionally, the administrator may tie the shaping policy to a particular service for the IP address/range.

Example: Shape all FTP traffic from 10.10.10.10 to 256Kbps would ensure that the user at 10.10.10.10 will not take up all of the bandwidth when they perform FTP downloads.

Shaping Based On IP Network

Similar to shaping based on an IP address, shaping based on an IP network allows the administrator to quickly shape their entire LAN without creating multiple rules. Simply enter the network address (example: 10.10.10.0) and select the appropriate Network Mask from the drop-down menu (example: 255.255.255.0).

Service shaping may also be applied to IP Network shaping.

Address Destination / Source Definition

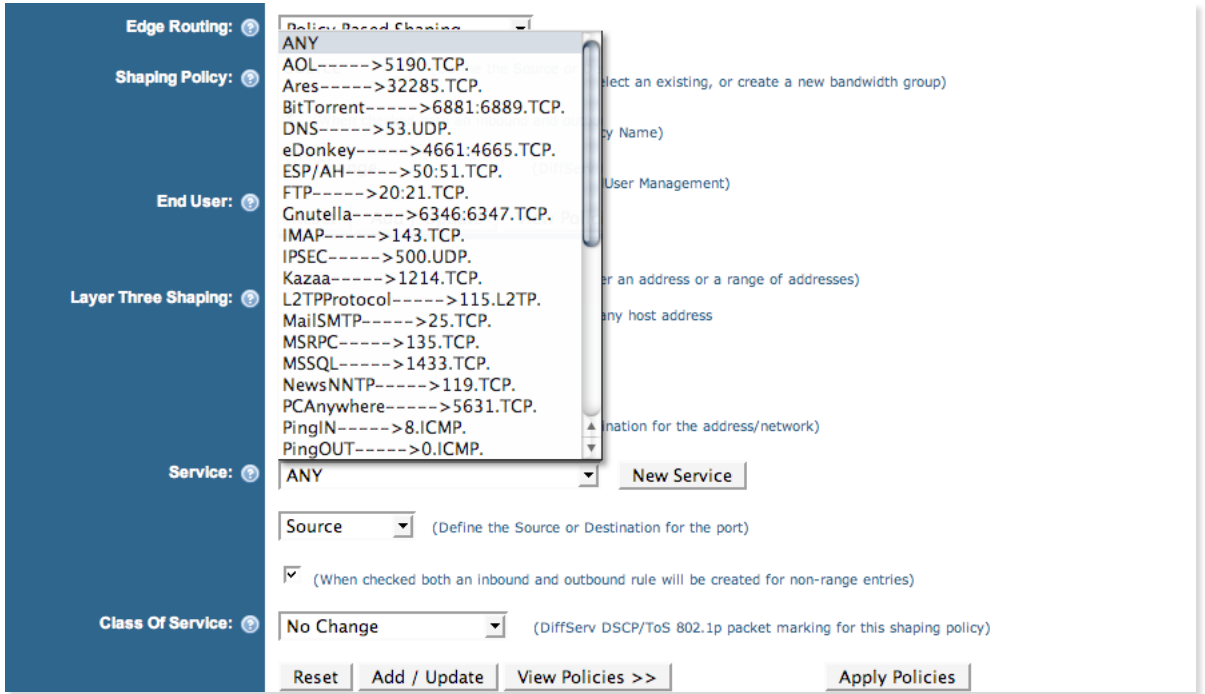
When shaping based on IP address information the rule will be applied based on whether the match is on the source address or the destination address.

Example 1: To rate-limit an end-user on the LAN network from downloading large files and using up a large portion of the network bandwidth, enter the IP address of the end-user and select DESTINATION as its matching criteria. This says that all traffic coming to this end-user should be shaped based on the associated bandwidth group.

Example 2: To rate-limit outbound traffic from a server on the LAN the administrator would enter the IP address of the server and select SOURCE as its matching criteria. This says that all traffic coming from that server will be rate-shaped based on the associated bandwidth group.

Shaping Based On Service Type (i.e. Web, Email, FTP, etc)

Service type shaping allows the administrator to shape traffic based on application.



Application Destination / Source Definition

When shaping based on an application the rule will be applied based on whether the match is on the source address or the destination port.

Example 1: To rate-limit an end-user on the LAN network from downloading large files and using up a large portion of the network bandwidth, enter the application type and select SOURCE as its matching criteria. This says that all traffic coming to this end-user should be shaped based on the associated bandwidth group.

Example 2: To rate-limit an end-user on the LAN network from uploading large files and using up a large portion of the network bandwidth, enter the application type and select DESTINATION as its matching criteria. This says that all traffic going out from this end-user should be shaped based on the associated bandwidth group.

Example 3: To rate-limit outbound traffic from a server on the LAN the administrator would enter the application type being used by the server and select SOURCE as its matching criteria. This says that all traffic coming from that server will be rate-shaped based on the associated bandwidth group.

Viewing Policies

Once a policy has been added, the policy may be viewed, deleted or edited using the "View Policies >>" button.

Shaping rules are applied in a "last to match" order, based on policy name.

Select	Policy Name	Bandwidth Group	User Alias	SRC/DST Address(es)	Shaping Host/Network	SRC/DST Port(s)	Shaping Port(s)	QoS	Kbps
<input type="radio"/>	PWC	test		DST	192.168.100.0/24	ANY	ANY	No Change	
<input type="radio"/>	PWC_reverse	test		SRC	192.168.100.0/24	ANY	ANY	No Change	
<input type="radio"/>	test	test		DST	10.10.0.1/SINGLE HOST	ANY	ANY	No Change	

This list of policies provides examples of a single host and IP address network.

DELETE and entry by selecting the entry and clicking the "Delete" button. If a range of addresses need to be deleted the "Delete All" button may be used. WARNING: The "Delete All" button will remove ALL shaping policies.

To modify a policy click the radio button for the policy and click the "Select" button.