

How To Guide

XRoads Networks

Edge Network Appliance How To Guide:
Shaping

Edge Network Appliance How To Guide: Shaping

@2009 XRoads Networks

22642 Lambert St, Suite 403

888-9-XROADS

Table of Contents

Shaping Overview

Shaping Control

Dynamic Bandwidth Management

Policy Based Shaping

Network / Scope Shaping

Session Limiting

Application Shaping

Application Management

URL Shaping

URL Management

Edge Configuration Series

Shaping Overview

The shaping menu is where one can control the bandwidth resource management capabilities of the EdgeXOS platform. This document provides an overview of the traffic shaping and QoS features of this appliance. All of the shaping modules are controlled by under the “Shaping” menu option.

The logo for XRoads Networks, featuring the text "XRoads Networks" in a white, sans-serif font against a dark blue background with a subtle wave pattern.

Home Interfaces **Shaping** NetBalancing Firewall Site2Site Tools Reporting

Policy Traversal

It is important to note here the process by which policies traverse the EdgeXOS appliance and which policies take precedence over others. The following is an ordering of the modules with a last to match order, i.e. the last module to match is applied.

URL / Application Shaping

Network / Scope Shaping

Dynamic Bandwidth Management

Policy Based Shaping

Session Limits always apply and are not over written by any other module. Policy Based Shaping rules have the final say on how packets are shaped.

Shaping Control: Use this menu option to turn on/off the various shaping modules. The EdgeXOS platform incorporates a number of different techniques in order to shape traffic and prioritize applications.

Edge Routing: ? Shaping Control

Policy Shaping: ? Enabled Disabled (Enable Individual Shaping/Scope Rules)

Session Limiting: ? Enabled Disabled (Limit Maximum Sessions Per User)

Streaming Control: ? Lower Latency More Bandwidth (Optimize for Low Latency vs More Bandwidth)

Application Shaping: ? Enabled Disabled (Enable Application-based Shaping)

URL Shaping: ? Enabled Disabled (Enable URL-based Shaping)

Update (Update Traffic Shaping Features)

These methods include:

- Policy Shaping: This is the primary method recommended to guarantee bandwidth for certain applications. This tool provides for the creation of SPECIFIC shaping rules which gives granular control over nodes and applications. Using this tool one can carve out bandwidth resources to ensure responsiveness and availability or lock down users so that they can only utilize 'x' amount of bandwidth.
- Session Limiting: This tool should be used to limit the number of sessions that end-users can initiate within a second. If you have many P2P users and wish to limit the number of sessions that they are using, this is a good tool to use.
- Application Shaping: This module is used to create general rules for prioritizing different types of applications, i.e. web(http) may have a higher priority than email(smtp), or VoIP traffic may have the highest priority. Conversely you can set a lower priority for P2P or non-critical applications.
- URL Shaping: This module can be used to set a higher priority for specific websites like Google.com or set with a lower priority for websites like YouTube.com.

Dynamic Bandwidth Management: Use this menu option to determine whether the EdgeXOS platform will automatically control bandwidth hogs by limiting upload speeds and lowering priority for those IP addresses when network usage is above high.

The screenshot shows the configuration page for Dynamic Bandwidth Management. On the left is a dark blue sidebar with two main sections: 'Edge Routing' and 'Bandwidth Management', each with a help icon. The main content area is white and contains the following settings:

- A dropdown menu set to 'Dynamic Bandwidth Management'.
- Radio buttons for 'Enabled' and 'Disabled'. 'Disabled' is selected. A note in parentheses reads: '(Dynamic Bandwidth Management - This does use additional system resources)'. The 'Disabled' radio button has a green dot.
- A dropdown menu set to 'Level 1'. A note in parentheses reads: '(Select the severity of throttling, with the maximum throttling at Level 5)'. The dropdown arrow is pointing down.
- Radio buttons for 'Enabled' and 'Disabled'. 'Disabled' is selected. A note in parentheses reads: '(Automated Escalation Of Throttling Level)'. The 'Disabled' radio button has a green dot.
- Radio buttons for 'Enabled' and 'Disabled'. 'Disabled' is selected. A note in parentheses reads: '(Equalization Only During High Utilization)'. The 'Disabled' radio button has a green dot.
- A dropdown menu set to '100Mbps'. A note in parentheses reads: '(Set the maximum throughput speed)'. The dropdown arrow is pointing down.
- A dropdown menu set to 'Usage 90%'. A note in parentheses reads: '(Select the utilization level)'. The dropdown arrow is pointing down.
- An 'Update' button with a note in parentheses: '(Update dynamic bandwidth management settings)'. The button is light blue.
- A 'Bypass Policies' button with a note in parentheses: '(Add policies for bypassing specific sessions)'. The button is light blue.

The severity levels set the initial priority and bandwidth setting that a top user will be throttled to during periods of high utilization (as long as equalization during high utilization is enabled). The higher the level, the more those top users will be affected when throttling is initiated (as long as automated escalation is enabled). No matter what the initial level is set to the longer the top user remains a top user the more severe the throttling will become for that user (see Application Shaping for more details). If the user drops out of the top user group during the throttling then that user will no longer be throttled. If the user becomes part of the top user group once again throttling will be re-initiated. All throttling is done based on session and IP address.

The maximum throughput speed is the fastest possible speed that a throttled user can achieve, this does not guarantee that bandwidth it simply sets a maximum speed.

If DBM is used with equalization during high utilization enabled then the administrator can set the percentage of utilization that determines when throttling is performed.

Policy Based Shaping: The module provides network administrators with granular control over bandwidth resources and allows for the carving out of bandwidth for specific applications and the throttling of users or groups of users to specific levels.

Use this module to guarantee bandwidth for mission critical servers or to prevent users from flooding the network with low priority traffic and thus cause slow response times for those mission critical servers.

Use this module to force end-users to be throttled when they attempt to use more bandwidth than is allocated to them.

Use this module to set priority and bandwidth levels for specific websites.

How Does Policy Shaping Work?

As data packets go through the appliance they are examined by the XRoads Operating System (XOS) to see if any of the applied shaping policies match the packets traversing the appliance. If a match is made, stats regarding the packet are collected and stored. If the stats reach the threshold created by the policy then an action is performed, this action could be to redirect the packet to a lower priority queue or the packet is sent to a queue which has already begun to overflow, which means that the packet is dropped.

All packets must match in order to be shaped; else they are allowed to traverse the appliance without any manipulation by the XOS. The direction that packets are traveling does not matter, what does matter is whether the packets match the policy settings.

How Does One Setup Policy Shaping?

The first step when creating policy based shaping rules is to create bandwidth groups. It is always recommended to first create a “default” group, which is the shaping of last resort. This means that if the no other rules match the packet the packet will always match something.

The following is an example of a common configuration where there is a default group, a high priority group and a low priority group. This is just an example, many groups can be created with many different levels of priority and rate limit settings.

Group Name	BURST (Kbps)	Priority	Shared
1-Default	10	12	YES
HighPriority	1000	1	YES
LowPriority	500	7	NO

When creating a new bandwidth group there are several rates that should be entered. The maximum and burst rate fields determine the highest possible sustained throughput rate for a policy and what the maximum burst level is for a specific policy. The burst rate is designed to only allow for quick bursts of bandwidth when utilization is low.

The priority level determines the outbound queue to use, some of which are faster and accessed more often than others. There are 12 levels of prioritization.

Create/Modify Group: ?

(Enter a name for this traffic shaping group)

Prioritization: ?

(Enter the per interface burst amount in [in Kbps] when bandwidth is available)

Allocation: ?

(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)

(Enter the priority level in relation to other groups)

(How is this bandwidth to be allocated to policies)

(Enter the priority level in relation to other groups)

<< Add Policy

Add Group

View Groups >>

The “Allocation” option is used to determine what happens when multiple policies are assigned to the same group. Either each policy will get its own single allocation of the bandwidth specified in the group, or all of the policies will share the bandwidth specified in the group.

The Default Policy: The purpose of the default group is to throttle all packets which do not match one of the other policies. This ensures that the policies created cover all of the services that are expected and that no unexpected traffic is able to use bandwidth resources.

The following is an example of common policies that can be created.

Policy Name	Bandwidth Group	User	SRC/DST Address(es)	Shaping Host/Network
Default	1-Default		SRC	10.0.0.0/24
Default_reverse	1-Default		SRC	10.0.0.0/24
Critical_Server	HighPriority		DST	10.0.0.10/SINGLE HOST
Critical_Server_reverse	HighPriority		SRC	10.0.0.10/SINGLE HOST
Users	LowPriority		SRC	10.0.0.128/25
Users_reverse	LowPriority		SRC	10.0.0.128/25

These policies are the first item listed under the Policy Based Shaping menu.

The screenshot shows the 'Policy Based Shaping' configuration page. On the left, there is a sidebar with 'Edge Routing' and 'Shaping Definition List'. The main area displays a table of shaping rules. The table has columns for Select, Policy Name, Bandwidth Group, User, SRC/DST Address(es), Shaping Host/Network, SRC/DST Port(s), Shaping Port(s), QoS, BusHours, and Remove. Below the table are buttons for '<< Add Policy', 'Select', 'Delete', 'Save', and 'Remove'. At the bottom, there is an 'Apply Policies' button with a note: '(Policy Shaping must be enabled under Shaping Control)'.

Select	Policy Name	Bandwidth Group	User	SRC/DST Address(es)	Shaping Host/Network	SRC/DST Port(s)	Shaping Port(s)	QoS	BusHours	Remove
<input type="radio"/>	Default	1-Default		SRC	10.0.0.0/24	ANY	ANY	No Change	No	<input type="checkbox"/>
<input type="radio"/>	Default_reverse	1-Default		SRC	10.0.0.0/24	ANY	ANY	No Change	No	<input type="checkbox"/>
<input type="radio"/>	Critical_Server	HighPriority		DST	10.0.0.10/SINGLE HOST	SRC	80	No Change	No	<input type="checkbox"/>
<input type="radio"/>	Critical_Server_reverse	HighPriority		SRC	10.0.0.10/SINGLE HOST	DST	80	No Change	No	<input type="checkbox"/>
<input type="radio"/>	Users	LowPriority		SRC	10.0.0.128/25	ANY	ANY	No Change	No	<input type="checkbox"/>
<input type="radio"/>	Users_reverse	LowPriority		SRC	10.0.0.128/25	ANY	ANY	No Change	No	<input type="checkbox"/>

When adding a new policy the following screen is provided in order to enter the policy name, URL/IP information, address range or subnet sizing (or single host), and the direction the packet is traveling when matched, with the address and port information in the source or destination portion of the packet.

Edge Routing:	Policy Based Shaping
Shaping Policy:	1-Default <input type="button" value="Bandwidth Groups"/> (Select an existing, or create a new bandwidth group)
	<input type="text"/> (Policy Name)
End User:	--- None Selected --- (Select a user from Tools->EndUser Management)
	OR
Web Site / URL:	http:// <input type="text"/> (Enter a web site or URL address)
	OR
Layer Three Shaping:	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/> (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)
Service:	ANY <input type="button" value="New Service"/>
	Source (Define the Source or Destination for the port)
	<input checked="" type="checkbox"/> (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)
	<input type="text"/> (Optional, maximum bandwidth usage per day)
	<input type="text"/> (Optional, maximum bandwidth usage per month)
	<input type="checkbox"/> (Select to only apply this policy during normal business hours)
	<input type="button" value="Reset"/> <input type="button" value="Add / Update"/> <input type="button" value="View Policies >>"/> <input type="button" value="Apply Policies"/>

NOTE: Selecting the correct “source” and “destination” information is critical to making the policies work as intended. Keep in mind that when traffic originates on the LAN the source address is a LAN address and the destination address is a WAN address. When traffic is coming back from the WAN to the LAN, the source is the WAN and the destination is the LAN. The opposite is true for the application port information.

When trying to match outbound HTTP traffic the key is to match the SOURCE address and the DESTINATION port. Example: If the LAN addressing was 10.0.0.0/24, then the policy would be as follows (10.0.0.0/24 SRC, HTTP 80 DST), and the reverse is true for HTTP response traffic (10.0.0.0/24 DST, HTTP 80 SRC). Remember when applications make an outbound query, they place the port designation information in the DST portion of the packet and the responding server places the port designation in the SRC portion of the packet.

To use an end-users name over their IP address simply confirm that a user has been created and then select that user from the drop-down.

To use a URL over an IP address simply enter the URL instead of the IP address and/or range or subnet. In this case the subnet will be equal to “single-host”. This will cause the EdgeXOS to perform a lookup for that URL and add rules for all DNS responses.

There are sixteen levels of Classification which provide the administrator with the ability to setup QoS based on standard Diffserv packet tagging. Keep in mind that this functionality is ONLY useful if all devices in the packets path support ToS tagging.

To limit the maximum amount of cumulative bandwidth that a policy can support during a given day or month enter those values when adding a policy.

If this rule is ONLY to be applied during normal business hours click the radio button to enable. Business hours 9am to 5pm and are determined by the local clock setting.

Network / Scope Shaping: If the goal is to set a fast general rule for a range of addresses this module is the best choice. Simply enter a range of addresses to which the rule will apply and select the throttle level.

Edge Routing: ?	Network / Scope Shaping
Scope Description: ?	<input type="text"/> (Enter a description for this shaping scope)
Scope Range: ?	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/> - <input type="text"/> (Enter a range of addresses for this scope)
Scope Throttle: ?	Level 5 <input type="button" value="v"/> (Select the severity of throttling, with the maximum throttling at Level 5)
	<input type="button" value="Scope List >>"/> <input type="button" value="Add / Update"/>

The throttle level determines the shaping priority for the address range specified. This module could be used to quickly set everyone in one department to one level, and everyone in another department to a higher or lower level. These are the same levels used in the other modules (see Application Shaping).

Session Limiting: This module provides the ability to limit the number of new sessions initiated by the addresses specified per second. This tool is helpful in slowing down network traffic specifically when users are opening many new sessions quickly, like many P2P applications.

The default '30' sessions per second has been found to be a good average number, however this may need to be modified based on unique network requirements.

Application Shaping: To quickly set the general priority of one application over another use this module. Prioritization of applications is only useful during high traffic periods, but it does ensure that those applications with the higher prioritization gain access to bandwidth resources first over other applications.

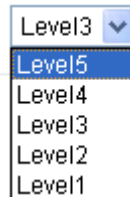
Select	Status	Name	Description	Category	Enable	Level
<input type="checkbox"/>	●	ftp	FTP (File Transfer Protocol) [top]	Internet	Enabled	Level3

An application must first be enabled; this is done under the Application Management section. Once enabled the throttle level can be set for the application. Applications with a higher throttle level will have a LOWER priority than applications with a lower throttle level. Level 1 is the highest priority while Level 5 is the lowest. Each level has additional built-in throttling so the degree of difference does matter.

Name	Description	Category	Enable	Level
ftp	FTP (File Transfer Protocol) [top]	Internet	Enabled	Level3

Default Throttle Levels

The EdgeXOS platform includes five default levels of throttling. Each level provides an incremental increase in the overall throttling which means that if there are two applications that are being throttled and one is a level 1 and the other is at level 5, there is a significant difference between the priority of each application.



There are no specific bandwidth limits set to these levels, nor do these levels match the priority levels set under the Policy Shaping groups. The EdgeXOS platform uses dynamic metrics to determine how to best apply these various throttling levels based on current system usage, available bandwidth, and other factors.

Application Mgmt: This menu option is used in conjunction with the Application Shaping module to enable applications for throttling/prioritization. By default the EdgeXOS platform comes with pre-loaded applications. Additional applications can be created by the network administrator. To create a new application simply obtain the TCP/UDP port information and determine whether any string information is required, ask support for assistance if necessary.



Select	App Name	Status	Description	Ports	Protocol	Category	String	Primary	Shaping Level
<input type="radio"/>	ANY	Off	ANY	0-655000	0	ANY		Off	Level 0
<input type="radio"/>	Avail	Off	Avail Backup Software	443/443	TCP	Backup		Off	Level 0
<input type="radio"/>	RepliStor	Off	RepliStor Backup Software	137/137	TCP	Backup		Off	Level 0
<input type="radio"/>	Retrospect	Off	Retrospect Backup Software	407/407	TCP/UDP	Backup		Off	Level 0
<input type="radio"/>	Veritas	Off	Veritas Utility	13724/13724	TCP/UDP	Backup		Off	Level 0
<input type="radio"/>	Veritas	Off	Veritas Backup Exec	3527+6101+6106+10000+13720+13721+13782	TCP	Backup		Off	Level 0
<input type="radio"/>	AOL	Off	AOL Instant Messaging Service	5190-5193	TCP	Client-Server		Off	Level 0

URL Shaping: To quickly set the general priority of one website and/or URL over another use this module. Prioritization of websites is only useful during high traffic periods, but it does ensure that those websites with the higher prioritization gain access to bandwidth resources first over other websites.

Edge Routing: URL Shaping

(Click here to request a new default URL rule.)

Update (Update all select rules) Apply Rules (Apply updated settings)

(Select a category to list) View All OR (Search for a specific URL) List/Search

Select	Status	URL	Description	Category	Enable	Level
<input type="checkbox"/>	●	www.cnn.com	New site	News	Enabled	Level5
<input type="checkbox"/>	●	www.google.com	Search engine	Search	Disabled	Level3
<input type="checkbox"/>	●	www.yahoo.com	Search site	Search	Disabled	Level2

Update Apply Rules Save

A website must first be created; this is done under the URL Management section. Once created the throttle level can be set for the website. The example above shows how cnn.com can be set for high throttling while google.com is given priority access when enabled. Websites with a higher throttle level will have a LOWER priority. Level 1 is the highest priority while Level 5 is the lowest. Each level has additional built-in throttling so the degree of difference does matter.

URL Mgmt: This menu option is used in conjunction with the URL Shaping module to enable websites for throttling/prioritization. To create a new website simply enter the URL for the website (using the fully qualified name) and determine what the default throttle level will be for this site. Keep in mind that setting a website to level 1 will most likely not have any affect unless under high traffic conditions.

Edge Routing: URL Mgmt

URL Listing: (This is a listing of URL's which are being shaped/throttled based on administrative requirements)

Select Delete Create (Select to modify, Delete to remove, Create to add new URL rules)

Select	URL Name	Status	Description	Category	Shaping Level
<input type="radio"/>	www.cnn.com	On	New site	News	Level 5
<input type="radio"/>	www.google.com	Off	Search engine	Search	Level 3
<input type="radio"/>	www.yahoo.com	Off	Search site	Search	Level 2

Select Delete Create (Select to modify, Delete to remove, Create to add new URL rules)