

How to Configure Bandwidth Policies or QoS

<https://campus.barracuda.com/doc/14713382/>

Limited network resources make bandwidth prioritization necessary. To ensure that important, business-critical applications are given enough bandwidth, the Barracuda NextGen Firewall X-Series provides traffic shaping (also known as "packet shaping" and "Quality of Service") methods to let you prioritize network resources according to factors such as the time of day, application type, and user identity. You can identify the traffic and assign its priority using firewall rules.

Bandwidth Policies

There are eight different bandwidth policies. They are listed in the following table, in order of decreasing priority:

Bandwidth Policy	Description
VoIP	Highest priority before all other bandwidth policies. Traffic is sent with no delay.
Interactive	Highest priority.
Business	Very high priority.
Internet	Medium priority. If more than 10 MB of data is transferred in one session, the priority of the traffic in that session drops to the same as Background.
Background	Next lower priority.
Low	Low priority. Low and Lowest Priority are limited to 5% of the available bandwidth.
Lowest Priority	Lowest priority. Low and Lowest Priority are limited to 5% of the available bandwidth.
Choke	Applications assigned this are unusable, but will not seek another way to send traffic. For example, if you wish to block Skype traffic, assign this policy to the Skype application.

Queues and Rate Limits

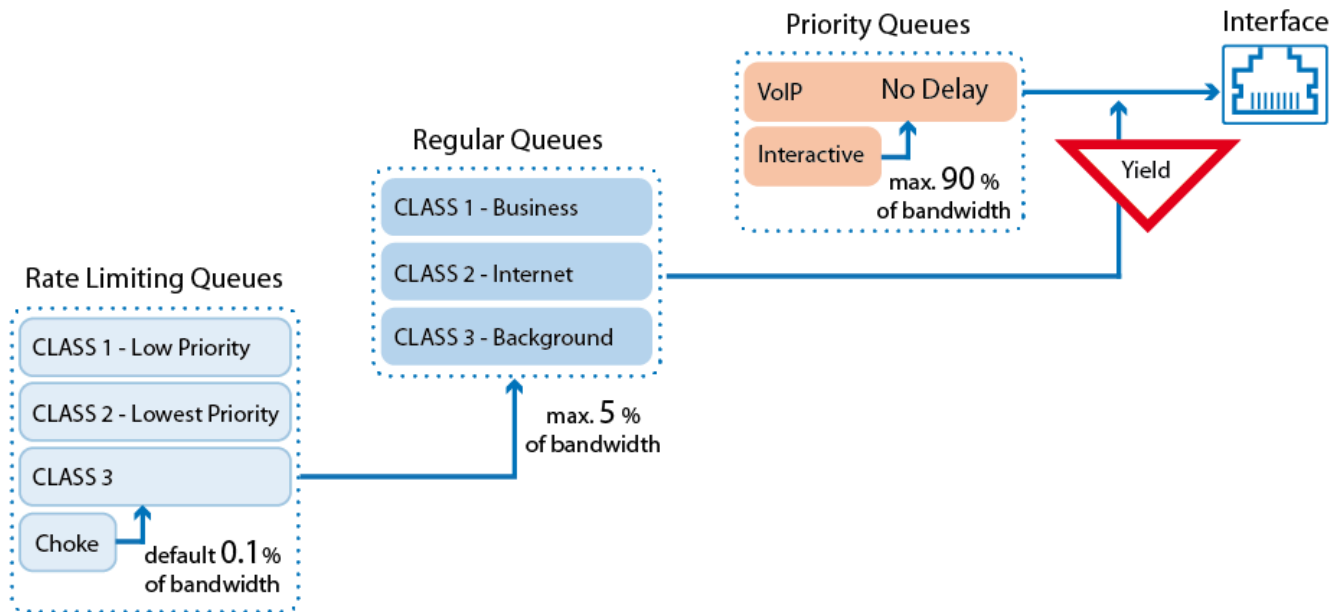
The following diagram shows how the eight bandwidth policies are divided into queues:

- The Priority Queues always take precedence.
- The Regular Queues can use unlimited bandwidth.
- The Rate Limiting Queues are collectively limited to 5% of the maximum link bandwidth.

The rate limits always apply, so even if there is no other traffic, the traffic in the Rate Limiting Queues

never uses more than 5% of the bandwidth.

The classes within the Regular and Rate Limiting queues are weighted relative to the other classes in the same queue. Class weights are enforced only when the link is saturated.



Customize the Class Weights and Rate Limits

On the **FIREWALL > QoS** page, you can set the weight ratios for the classes within the same queue and modify some of the rate limits.

Assign a Bandwidth Policy to a Firewall Rule

Before you begin, verify that you specified a bandwidth for each interface you want to enable QoS on:

1. Go to **NETWORK > IP Configuration**.
2. In the **Network Interface Configuration** section, select the interface and click the **No/Yes** link in the **Use QoS** column.
3. Enter the bandwidth assigned by your ISP for outbound and inbound connections.

To assign a bandwidth policy to an access rule:

1. Go to **FIREWALL > Firewall Rules** and edit the rule.
2. Select the bandwidth policy from the **Adjust Bandwidth** drop-down menu.

Monitor Bandwidth Policy Assignment

To monitor which bandwidth policy is assigned to active network sessions, go to the **BASIC > Active Connections** page. The assigned policy of a network session is displayed in the **Bandwidth Policy** column. You can also manually override the assigned bandwidth policy by using the drop-down menu in the **Bandwidth Policy** column.

Figures

1. qos_scheme.png

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.