Howto: SIP Call Admission Control

Lisa Hallingström

Paul Donald

Bogdan Musat

Adnan Khalid

Per Johnsson

Rickard Nilsson

Table of Contents

How To Use Ingate Call Admission Control.....3

Ingate Firewall/SIParator® version: 4.6.2

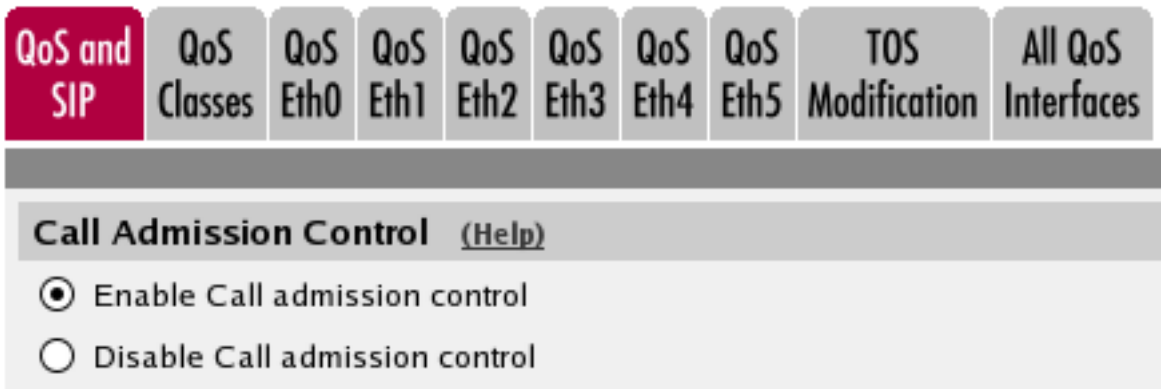
Document version: 1.1

How To Use Ingate Call Admission Control

This is how to configure your Firewall/SIParator to keep track of SIP calls through it and to reject new calls when there is not enough bandwidth for the new media.

This feature is *only available* when the *Quality of Service* module has been installed.

On the **QoS and SIP** page, you turn the Call admission control on.



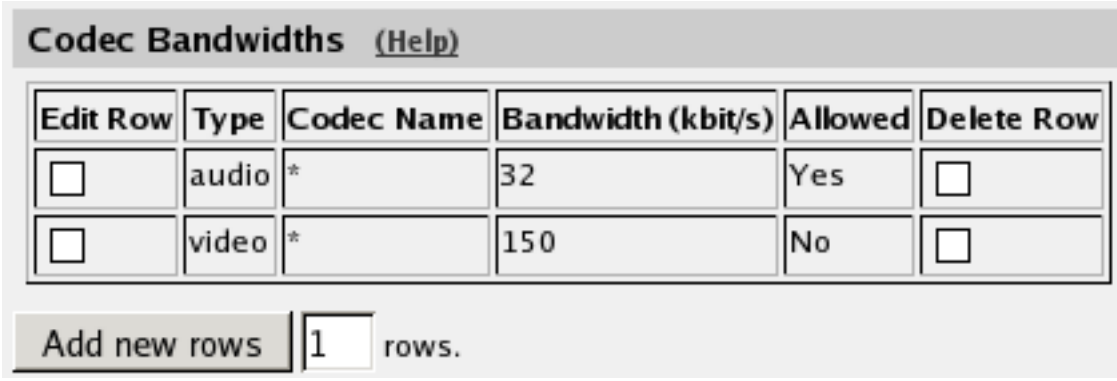
For each interface where Call admission control should be used, enter bandwidth limits for media streams.

Bandwidths For SIP Media (Help)

Interface	Outgoing (kbit/s)		Incoming (kbit/s)	
	Allowed for Media (kbit/s)	Allowed for Emergency (kbit/s)	Allowed for Media (kbit/s)	Allowed for Emergency (kbit/s)
Internal (eth0)	1000		1000	
External (eth1)	600	200	700	
External2 (eth2)				
DHCP clients (eth3)	1500		1500	
SIP-1 (eth4)				
SIP-2 (eth5)				

For the Firewall/SIParator to know when to reject calls, it needs to know how much bandwidth an audio or video stream will consume. The bandwidth largely depends on which codecs are used.

Enter bandwidths used for the variouis codecs. There is also a generic bandwidth for each codec type, which is used by the Firewall/SIParator when a specific codec can't be found in the table.

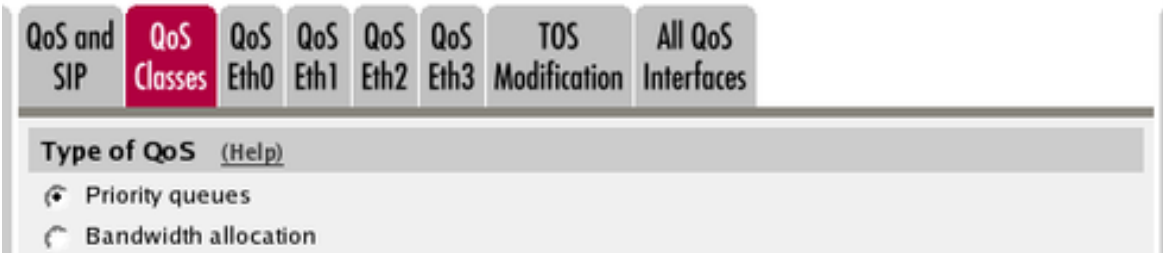


When a new call request is received by the Firewall/SIParator, it calculates the bandwidth still free and which media streams the new call asks for. If there is enough bandwidth left for all media streams, the call is allowed. If there is not bandwidth enough, the call will be denied. The response 486 (Busy Here) will be sent to the call requestor.

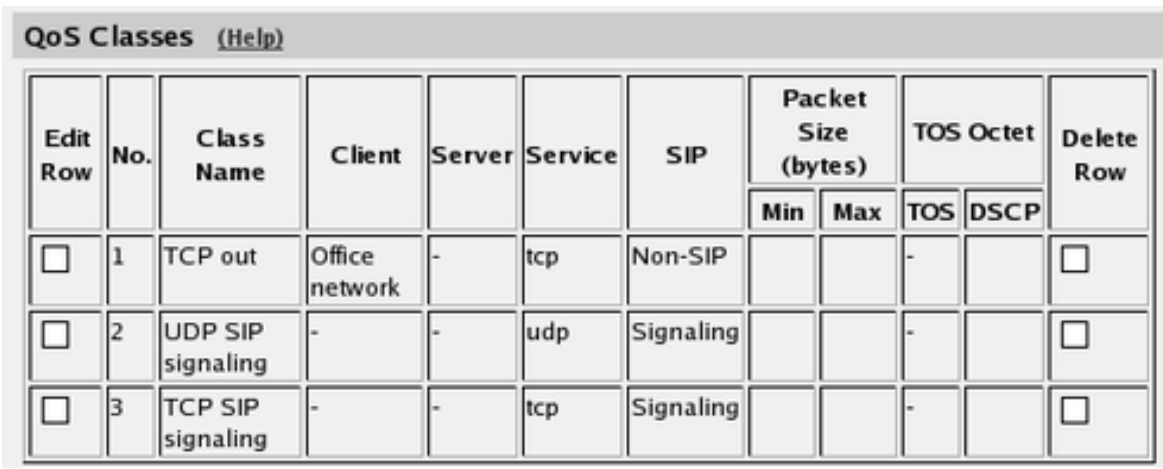
The settings hitherto explained will ensure that SIP media is allowed a certain bandwidth, and also limit it to that bandwidth. If you want to control SIP signaling too, more settings are needed.

First, select to control traffic through prioritization (different types of traffic are assigned different priorities), or bandwidth limitation (different types of traffic are assigned bandwidth limits).

In this example, traffic prioritization is used.



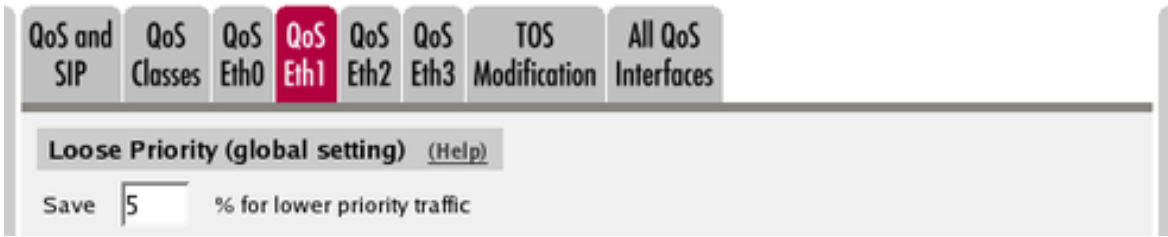
Then, create **QoS Classes** for the types of traffic you want to prioritize. There is no need to create a class for SIP media; as soon as priorities are made for other traffic, the Firewall/SIParator will automatically give SIP media traffic the highest priority.



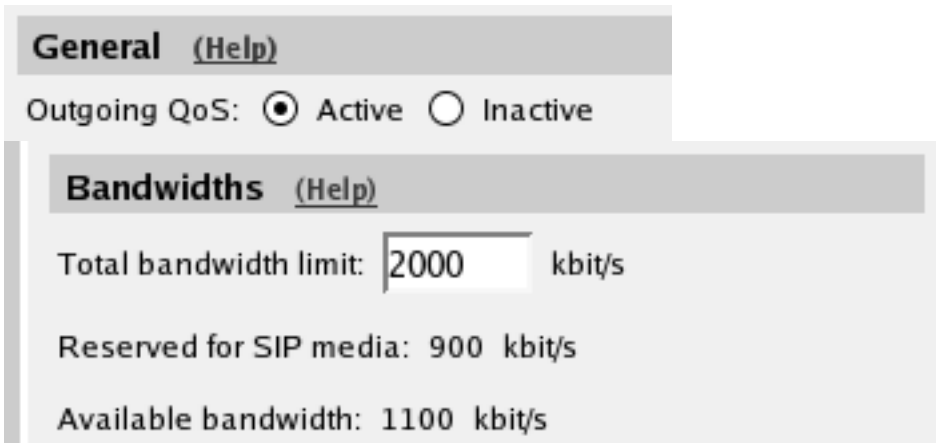
For every interface where QoS should be used, you need to define how much bandwidth can be used for different types of traffic. You do that on the **QoS Interfaces** pages.

As prioritization is used here, there is a setting called **Loose Priority**. With this setting, you control if a higher priority traffic can use the entire bandwidth, or if some lower priority traffic should be allowed even if there is high priority traffic enough to fill the bandwidth.

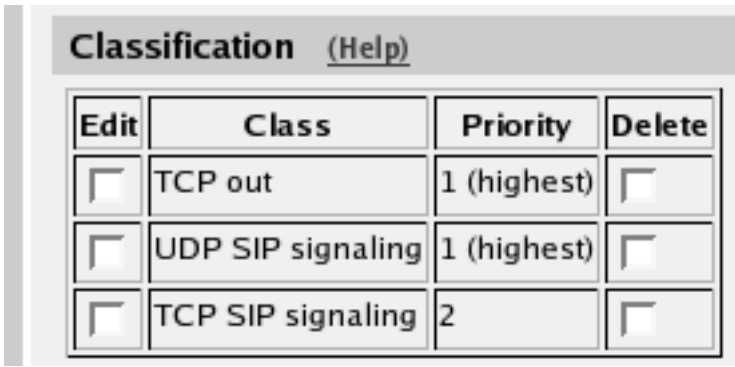
Here, we select to allow 5 % of lower priority traffic.



Turn **Egress QoS** on and enter a **Total bandwidth** for the interface. Due to the configuration previously made on the **QoS and SIP** page, some bandwidth is already reserved for SIP media.



Assign priorities for the traffic classes you created. We want SIP signaling to have a high priority.



You also need to assign a priority for traffic that is not defined in the **Classification** table.

Finally, go to the **Save/Load Configuration** page under **Administration** and apply the new settings by pressing **Apply configuration**.