

# **Configuration Aid To Ingate Firewall/SIParator - SIP Call Admission Control**

**Lisa Hallingström**  
Ingate Systems AB



# Table of Contents

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

Ingate Firewall/SIParator version: 4.6.2

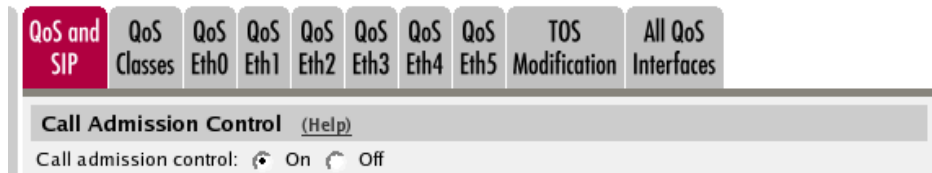
Document version: 1.1

## How To Use Ingate Call Admission Control

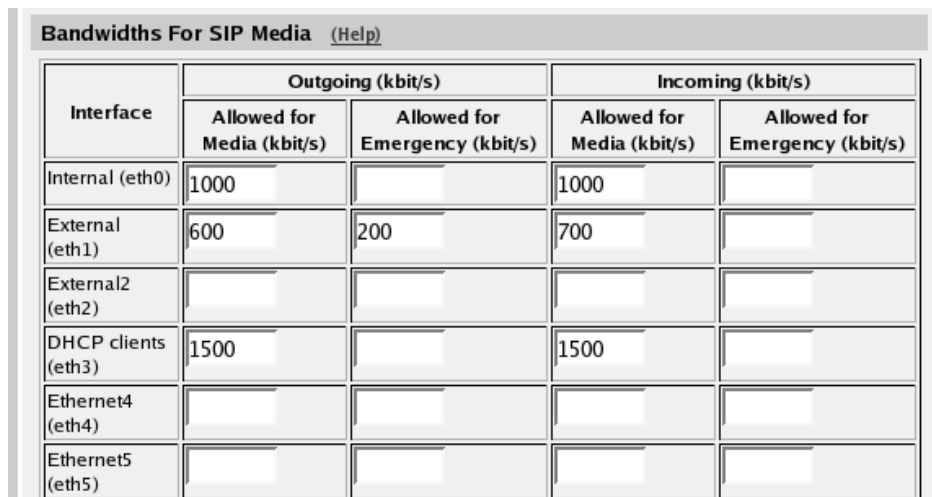
This is how to configure your firewall/SIParator to keep track of SIP calls through it and to reject new calls when there is not enough bandwidth for the new media.

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.



The screenshot shows the 'Bandwidths For SIP Media' configuration table. The table has columns for 'Interface', 'Outgoing (kbit/s)', and 'Incoming (kbit/s)'. Each of the last three columns is further divided into 'Allowed for Media (kbit/s)' and 'Allowed for Emergency (kbit/s)'. The table is populated with values for several interfaces.

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	
Ethernet4 (eth4)				
Ethernet5 (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 various 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.

Codec Bandwidths <a href="#">(Help)</a>					
Edit	Type	Codec Name	Bandwidth (kbit/s)	This Codec Is Allowed	Delete
<input type="checkbox"/>	audio	g723	40	On	<input type="checkbox"/>
<input type="checkbox"/>	audio	g726-16	16	On	<input type="checkbox"/>
<input type="checkbox"/>	audio	g726-24	24	On	<input type="checkbox"/>
<input type="checkbox"/>	audio	g726-32	32	On	<input type="checkbox"/>
<input type="checkbox"/>	audio	g726-40	40	On	<input type="checkbox"/>
<input type="checkbox"/>	audio	g729	8	On	<input type="checkbox"/>
<input type="checkbox"/>	audio	g729a	8	On	<input type="checkbox"/>
<input type="checkbox"/>	audio	gsm	13	On	<input type="checkbox"/>
<input type="checkbox"/>	audio	ilbc	16	On	<input type="checkbox"/>
<input type="checkbox"/>	audio	pcma	64	On	<input type="checkbox"/>
<input type="checkbox"/>	audio	pcmu	64	On	<input type="checkbox"/>
<input type="checkbox"/>	audio	speex	44	On	<input type="checkbox"/>
<input type="checkbox"/>	audio	*		Off	<input type="checkbox"/>
<input type="checkbox"/>	video	*		Off	<input type="checkbox"/>

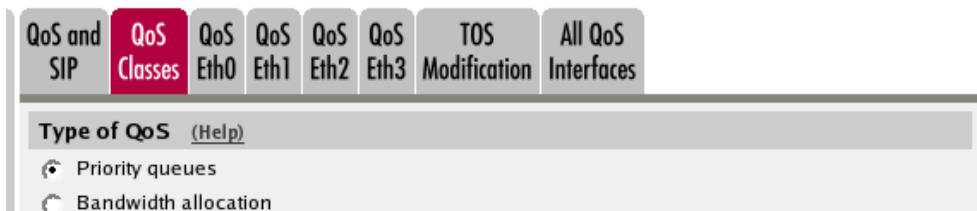
Add new rows  rows.

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.

QoS Classes <a href="#">(Help)</a>											
Edit	No.	Class Name	Client	Server	Service	SIP	Packet Size (bytes)		TOS Octet		Delete
							Min	Max	TOS	DSCP	
<input type="checkbox"/>	1	TCP out	Office network	-	tcp	Non-SIP			-		<input type="checkbox"/>
<input type="checkbox"/>	2	UDP SIP signaling	-	-	udp	Signaling			-		<input type="checkbox"/>
<input type="checkbox"/>	3	TCP SIP signaling	-	-	tcp	Signaling			-		<input type="checkbox"/>

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.

QoS and SIP | QoS Classes | QoS Eth0 | **QoS Eth1** | QoS Eth2 | QoS Eth3 | TOS Modification | All QoS Interfaces

**Loose Priority (global setting)** [\(Help\)](#)

Save  % for 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.

**General** [\(Help\)](#)

Outgoing QoS:  Active  Inactive

**Bandwidths** [\(Help\)](#)

Total bandwidth limit:  kbit/s

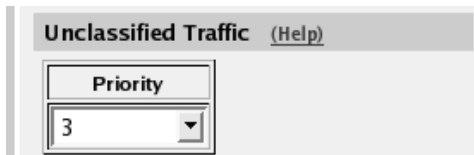
Reserved for SIP media: 900 kbit/s

Available bandwidth: 1100 kbit/s

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

Classification <a href="#">(Help)</a>			
Edit	Class	Priority	Delete
<input type="checkbox"/>	TCP out	1 (highest)	<input type="checkbox"/>
<input type="checkbox"/>	UDP SIP signaling	1 (highest)	<input type="checkbox"/>
<input type="checkbox"/>	TCP SIP signaling	2	<input type="checkbox"/>

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

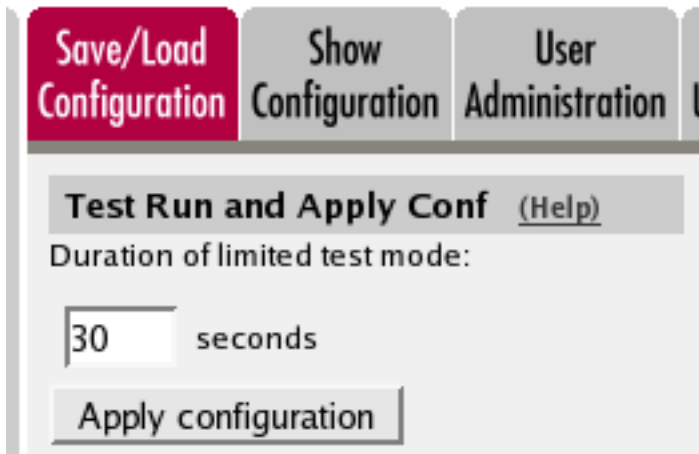


Unclassified Traffic [\(Help\)](#)

Priority

3

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



Save/Load Configuration Show Configuration User Administration U

Test Run and Apply Conf [\(Help\)](#)

Duration of limited test mode:

30 seconds

Apply configuration