

Time Sensitive Information!

**These Configuration Changes Must Be
Applied Ten Days Prior to Norcom Solutions
Group Cut-Over**



Edgewater Router Configuration for Norcom Solutions Group Cloud Phone System

Document Version 1.3

March 17th, 2017

Table of Contents

1. [Introduction](#)
2. [Firewall Checklist](#)
3. [NAT](#)
4. [Traffic Shaper](#)
 - a. [Classes of Service](#)
 - b. [Classification Rules](#)

Introduction

This document is targeted towards IT administrators and illustrates configuration changes required on Edgewater firewall & router appliances to support Norcom Solutions Group's cloud communications telecommunications platform. This document assumes a basic network deployment consisting of one internal LAN network containing the IP phones and one WAN network connected to the Internet. While we strongly recommend a dedicated network for VoIP traffic, the instructions below can be used for a "converged" network whereby both VoIP and non-VoIP traffic share one physical WAN network. With basic modifications (such as adding access rules for additional interfaces), this configuration can be extrapolated for other network layouts. The screenshots below may vary slightly from what is displayed while configuring the device depending on model and software version. Setting values not mentioned may be left at default or changed as required for specific purposes.

Please call Norcom Solutions Group Support at 877-667-2661 if you need any further information.

Screenshots and instructions are based on Edgewater 4550 – EdgeMarc 2 running Version.11.6.13.....

Firewall Checklist

After applying the GUI configurations in this document, please take the appropriate screen shots to provide the firewall “verification” to Norcom Solutions Group.

Screen Shot #:	Configuration:	Completed:
1	NAT → Enable Dynamic NAT (checked)	
2	Traffic Shaper → General	
3	Traffic Shaper → Advanced → Classes of Service	
4	Traffic Shaper → Advanced → Classification Rules	

NAT

Note: default log in to Edgewater devices is:

UN: root

PW: default

NAT

NAT[Help](#)

This page supports only IPv4 addressing.

Dynamic Nat

Dynamic NAT allows a device with a private address to access resources on a public network. Requests from the device are remapped to use the public IP address of the system. A different public IP address other than the system IP address can be specified.

Enable Dynamic NAT: ☒

Public IP Addresses:

Primary WLR Interface:

Secondary WLR Interface:

- Check to Enable Dynamic NAT
- Click Submit or Apply Later

Traffic Shaper

[Help](#)

Traffic Shaper

Enable Traffic Shaping: ☒

PRIMARY WAN Downstream Bandwidth (Kbps):

SECONDARY WAN Downstream Bandwidth (Kbps):

PRIMARY WAN Upstream Bandwidth (Kbps):

SECONDARY WAN Upstream Bandwidth (Kbps):

Differentiated Services Code Point (DSCP)

☒ Expedited Forwarding (default)

☐ IP Precedence

☐ Assured Forwarding

☐ Custom Value (1-63)

IPv4 only.

Enable TOS based routing: ☐

Enable TOS Byte Stripping: ☒

Enable Call Admission Control: ☐

Maximum calls allowed on Primary WAN:

Maximum calls allowed on Secondary WAN:

Note: See the [Help](#) page for help determining how many calls your WAN link can support.

Enable SIP Inactivity Monitor: ☒

SIP Inactivity Timeout (min):

- Check to Enable Traffic Shaping
- Enter the Download and Upload bandwidth of your internet connection
 - Note: Please use contracted speeds not speed test results that may show bursting.
- Differentiated Services Code Point (DSCP)
 - Choose EF – Expedited Forwarding
- Check Enable TOS Byte Stripping

Traffic Shaper → Advanced → Classes of Service

[Help](#)

Advanced Traffic Shaping

[Classes of Service](#)
[Classification Rules](#)

Classes of Service			
Select: All None			Delete
	Name	Priority Class	Bandwidth %
<input type="checkbox"/>	priority	EF / IP5	90
<input type="checkbox"/>	best_effort	Best Effort	10

Create a new Class

Name:

Priority Class: AF1x / IP1 ▼

Bandwidth Percentage (%):

Add
Reset

- Configure the Classes of Service to show as above.
 - Priority – EF – 90%
 - Best Effort – 10%
- Remove any other classes

Traffic Shaper → Advanced → Classification Rules

[Help](#)

Advanced Traffic Shaping

[Classes of Service](#)
[Classification Rules](#)

Classification Rules						
Select: All None						Delete
	Direction	IP Address	Source Port	Destination Port	Protocol	DSCP
<input type="checkbox"/>	both	184.178.213.1-254	any	any	any	EF

Create a new Classification Rule

Traffic can be classified by a single or a range of IP addresses and/or ports.
For example: 192.168.1.100-105, 1000-1005.

IPv4 only.

IP Address:

Direction: both

Protocol: any

Source Port:

Destination Port:

Differentiated Services Code Point:

☒ Expedited Forwarding
☐ IP Precedence
☐ Assured Forwarding
☐ Custom Value (1-63)

1
AF11

[Add](#)
[Reset](#)

- Added Classification rule
 - IP address: 184.178.213.1-254
 - Direction: Both
 - Protocol: Any
 - Source: Any (leave blank the system will automatically fill)
 - Destination: Any (leave blank the system will automatically fill)
 - DSCP: Expedited Forwarding
- Apply settings.

Document Revision History

Version	Reason for Change	Date
1.0 Draft	Initial Draft Document	November 21, 2013
1.3	Firewall Checklist added	March 17 th , 2017