

Comdasy FAQ: Internet
Connection for the MC
Controller

Comdasy AG
Rüdesheimer Str. 7
D-80686 München

Tel.: +49.89.5484333-0
Fax: +49.89.5484333-29

support@comdasy.com

<http://www.comdasy.com>

Disclaimer

We have taken all possible care to ensure that this manual contains correct, accurate information. However, the manufacturer cannot assume liability for any possible errors. In addition, the manufacturer cannot guarantee that the hardware will meet the purpose you require.

Comdasys reserves the right to make changes according to technical progress at any time. Brand names may be registered trademarks and must be treated as such.

© Copyright 2005-2009
Comdasys AG
80686 München, Germany

All rights reserved. No part of this manual may be reproduced, processed or distributed in any form (print, photocopy, microfilm or any other process) or processed by an electronic system without prior written permission from the manufacturer.

Content

1. Synopsis.....	4
2. Direct Connection.....	4
3. Indirect Scenarios.....	5
3.1. With intermediary DMZ.....	5
3.2. Behind a Firewall with NAT and Port Forwarding.....	6
3.3. With a SIP-aware Firewall or Session Border Controller (SBC).....	7
4. Last Words.....	7

1. Synopsis

This document describes the various possibilities of connecting the Comdasys MC Controller to the internet. Although it is generally possible to run the MC Solution, which consists of the MC Controller as a server component, and the MC Clients as its deployed client components, without an internet connection, some services rely on a proper internet setup. These services include:

- **WLAN over internet**

If the MC Controller is connected to the internet, all MC Clients within the local area network (LAN) of the MC Controller and outside of it will be able to offer services in WiFi to their users. These services include: Voice-over-IP calls and MC Client software and configuration deployments.

- **VoIP over 3G**

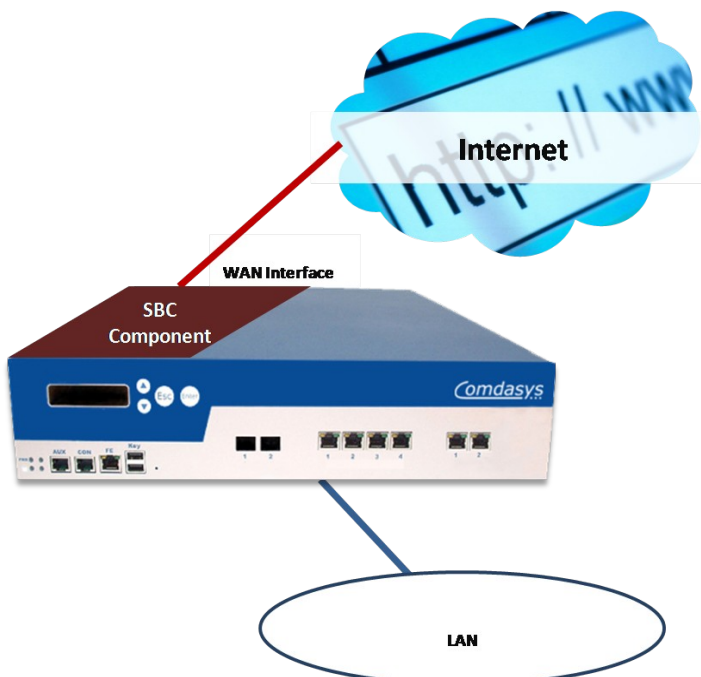
A user can take advantage of 3G connections for calls if the MC Controller is connected to the internet. This also makes all other features, like least-cost routing (LCR), Callback and MC Client software and configuration deployments possible.

Please consult the administrator manual for your MC Controller version for details about the menus that you have to configure to put your scenario into effect. All manuals can be found here:

http://ftp.comdasys.com/pub/documentation/FMC_series/

2. Direct Connection

The MC Controller provides a fully featured firewall and runs on a hardened Linux operating system (OS). This makes it possible to connect it directly to the internet without any risky exposure of your internal network. The MC Controller also has a built-SBC component which provides even more protection.



TODO: To set up the direct internet connection, configure the WAN interface of your MC Controller accordingly.

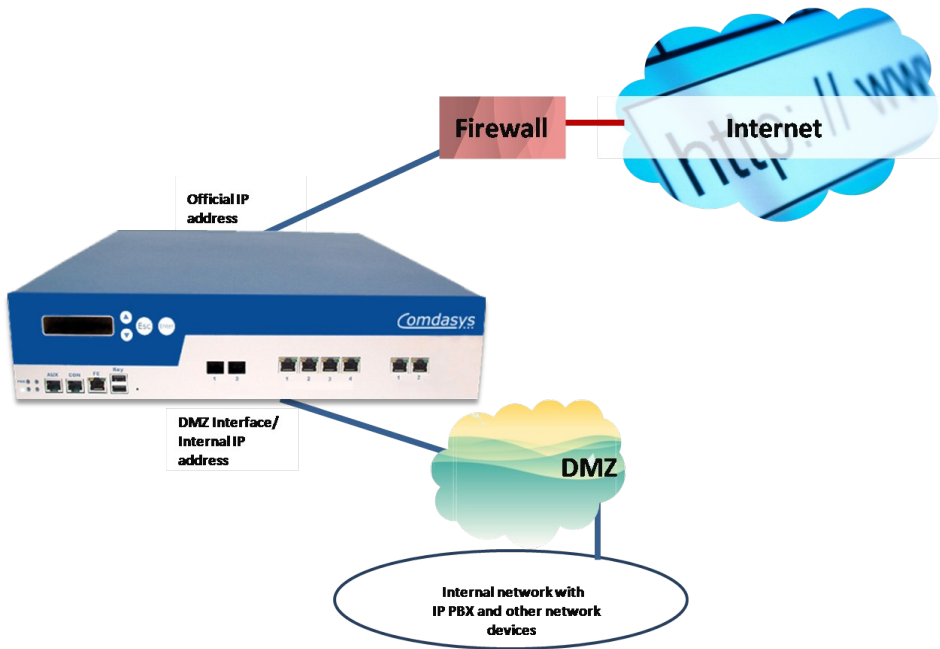
The built in SBC component listens on **port 5062 by default**, there is **no activation needed**. However, you have to make sure that the MC Client's requests are actually forwarded to port 5062 when crossing the firewall.

3. Indirect Scenarios


There are some possible indirect setups for connecting the MC Controller to the internet. Choose the one that most suits your system properties and/or requirements.

3.1. With intermediary DMZ

A demilitarized zone (DMZ) can be used to ensure higher protection of your internal system (and its information). "DMZ" describes a secure network area, which is separate from the internet and the local network. Normally, this is used for servers that have to be reachable from both the internal network and the internet (e.g. mail server, web server, etc.). In most cases a DMZ will have official IP addresses.

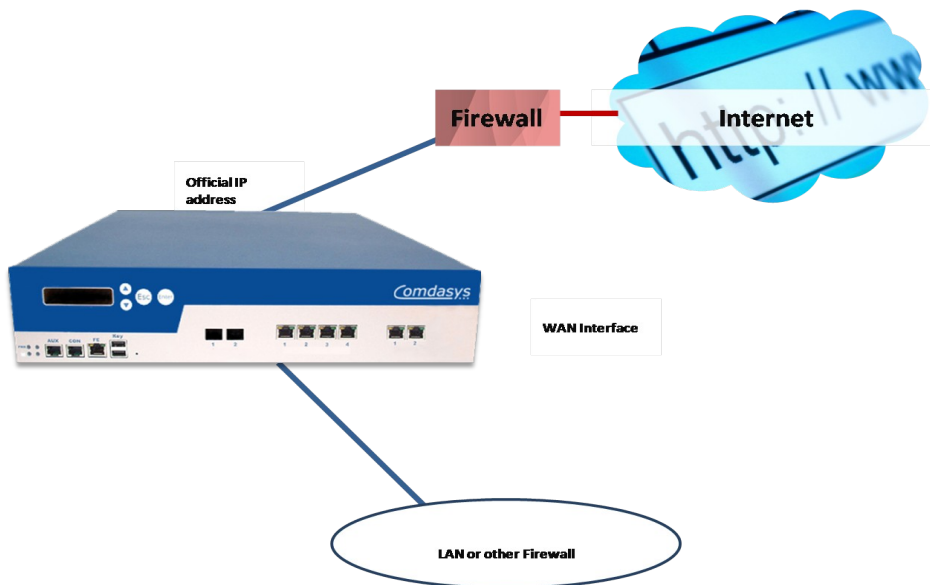


TODO: Configure the DMZ Interface of your MC Controller and connect it to the services in the DMZ.

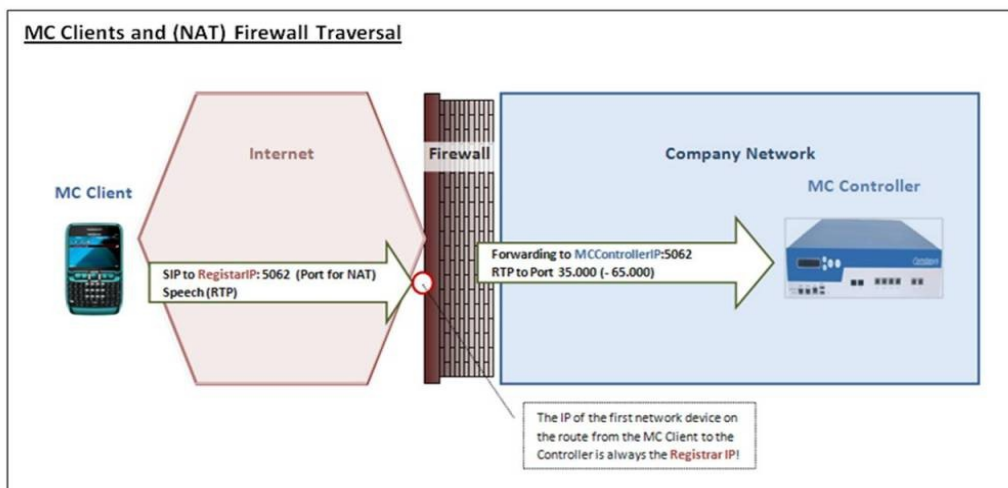
 Port Forwarding rather than a DMZ is needed for providing services to the internet while having servers with private IP addresses. Please refer to the next section for more information about Port Forwarding.

3.2. Behind a Firewall with NAT and Port Forwarding

If the DMZ scenario is not an option, try Port Forwarding and NAT behind a firewall (see simplified picture below). Of course a firewall can also be the one provided by the MC Controller itself.



TODO: Configure Port Forwarding rules (in the MC Controller menu of the same name). All you have to do to enable NAT handling is to set the “External IP for NAT” (Global Settings) on the MC Controller and to use the target port 5062 on the MC Clients. The picture and description below provide more details about this.



1. MC Client:

The Registrar IP has to be set to the IP of the first network device on the way from the internet to the internal enterprise network (the firewall); the port has to be set to 5062. Example: <IP Address>:5062

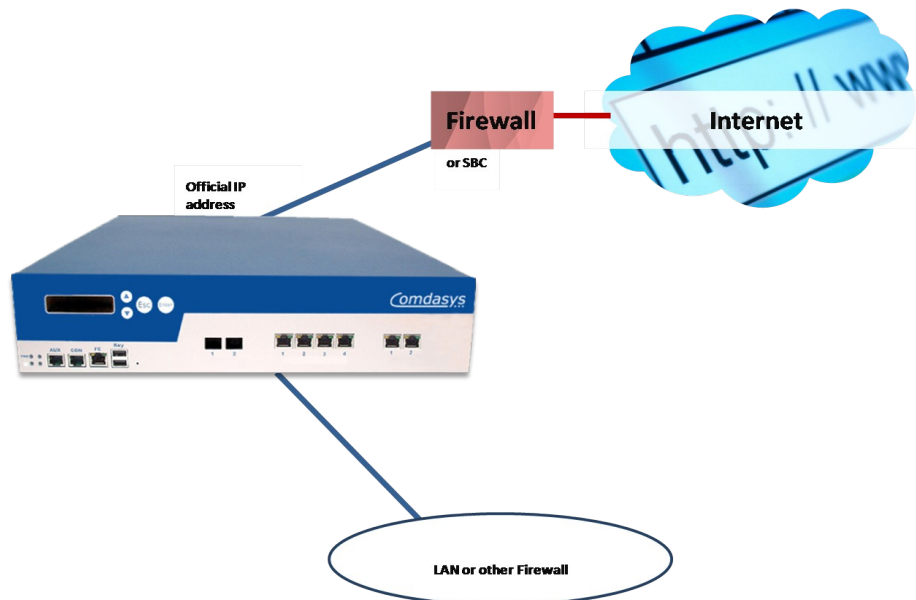
2. Firewall Device:

Make sure that the port forwarding rule for this scenario is set to the IP address of the MC Controller in your network and that the port for SIP kept at 5062. Please keep in mind that the

port range for RTP (speech) is 35.000 - 65.000!
The default port 5062 (SBC component) can of course be changed on the MC Controller (Port Settings). If this is the case in your corporate network, please set the port forwarding rule accordingly!

3.3. With a SIP-aware Firewall or Session Border Controller (SBC)

Another option is to use a SIP-aware firewall or a Session Border Controller (SBC). You can use the built-in SBC-component of your MC Controller to accomplish this:



There are certain configurations that have to be made if a firewall is located between the MC Client and the MC Controller. The following section provides all necessary details.

In most cases, this scenario requires a larger setup.

4. Last Words

Of course there are numerous other possibilities to connect your MC Controller to the internet. This document can only outline the most common scenarios. However, with the above noted options, it should be possible to find an apt configuration for all typical corporate networks.