

**Comdasy** FAQ: VoIP Branch  
Connectivity with VPN Tunnels

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 2005-2008  
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.

# Inhaltsverzeichnis

1. VoIP survivability mode through VPN tunnels.....	4
1.1. Introduction.....	4
1.2. Custom firewall rules.....	4
1.3. Summary.....	5

# 1. VoIP survivability mode through VPN tunnels

## 1.1. Introduction

Several Convergence products support VoIP proxying in the so-called survivability mode. This document describes the necessary steps to enable survivability through a VPN tunnel.

Because of security concerns Convergences do not allow to send traffic from the Convergence through the VPN tunnel. They only forward traffic from other computers. Since in survivability mode a service on the Convergence (the VoIP proxy) needs to send and receive traffic through the tunnel we need to tell the firewall to allow this specific traffic.

The following document is leading you step-by-step through the creation of the necessary custom firewall rules (stored in `/etc/sysconfig/firewall.custom`). It assumes that the traffic should go through an IPsec tunnel, which has the interface name `ipsec0`. If you are using OpenVPN you must exchange `ipsec0` for the appropriate tun interface (you could use `tun+` for all OpenVPN interfaces).

## 1.2. Custom firewall rules

First, we need to allow ICMP packets and UDP packets for port 5060 (SIP) to be sent into the tunnel. The rules necessary look like this:

```
iptables -A OUTPUT -p icmp --icmp-type any -o ipsec0 -j ACCEPT
iptables -A OUTPUT -p udp --destination-port 5060 -o ipsec0 -j ACCEPT
```

But we also need to mark those packets because we later need to NAT them. This is because otherwise the packets sent through the tunnel would have the WAN interface address as sender IP address.

```
iptables -t mangle -A OUTPUT -p icmp --icmp-type any -o ipsec0 -j MARK --set-mark 0x5EC
iptables -t mangle -A OUTPUT -p udp --destination-port 5060 -o ipsec0 -j MARK --set-mark 0x5EC
```

You can choose another value than `0x5EC` but be careful to use the same value you've chosen in the NAT rule below.

Of course we also need to allow packages coming through the tunnel sent to us. We allow all packets which the firewall knows a belonging to a "session" and additionally packets to the UDP port 5060.

```
iptables -A INPUT -m state --state ESTABLISHED,RELATED -i ipsec0 -j ACCEPT
iptables -A INPUT -p udp --destination-port 5060 -i ipsec0 -j ACCEPT
```

The only thing left to do is NAT. As mentioned before, the problem is that the Convergence wants to send packets with the address of the WAN interface as sender address, but the receiver will not know this address. So we need to modify the source address so that the receiver will see our LAN address as sender address. If we assume that our LAN1 port has the address `192.168.255.160` then the rule would be:

```
iptables -t nat -A POSTROUTING -o ipsec0 -m mark --mark 0x5EC -j SNAT --to-source 192.168.255.160
```

If you've chosen another value than 0x5EC in the marking rules you need to use that value here instead of 0x5EC. Otherwise the NAT rule won't translate your packets.

### 1.3. Summary

Here is the complete `/etc/sysconfig/firewall.custom`, assuming an IPsec connection (ipsec0 interface), a LAN1 address of 192.168.255.160 and using a mark of 0x5EC.

```
iptables -A OUTPUT -p icmp --icmp-type any -o ipsec0 -j ACCEPT
iptables -A OUTPUT -p udp --destination-port 5060 -o ipsec0 -j ACCEPT

iptables -t mangle -A OUTPUT -p icmp --icmp-type any -o ipsec0 -j MARK --set-mark 0x5EC
iptables -t mangle -A OUTPUT -p udp --destination-port 5060 -o ipsec0 -j MARK --set-mark 0x5EC

iptables -A INPUT -m state --state ESTABLISHED,RELATED -i ipsec0 -j ACCEPT
iptables -A INPUT -p udp --destination-port 5060 -i ipsec0 -j ACCEPT

iptables -t nat -A POSTROUTING -o ipsec0 -m mark --mark 0x5EC -j SNAT --to-source 192.168.255.160
```

Note that you have to call `applyfirewall.sh` after you've written these rules into `/etc/sysconfig/firewall.custom`.