

Comdasy FAQ: Firewall

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. Deactivating the Firewall.....	4
2. Firewall Marking.....	4
2.1. Introduction.....	4
2.2. Setup.....	4
2.3. Marking IPSEC Packes.....	5
3. Natting inside an IPSEC Tunnel.....	5
4. Qos Tagging (DSCP/TOS).....	6
4.1. Introduction.....	6
4.2. Setup.....	6

1. Deactivating the Firewall

In some configurations, it is necessary to completely deactivate the firewall. This could be necessary if complete forwarding between all interfaces is wished, which might be necessary in some routing configurations. New variables were added to the configuration environment in release r686 and later.

To deactivate the firewall it is necessary to set all activated interface to be "open". This is done by setting the following variables in the `/etc/config/baseconfig` file:

```
fw_lana_all_open=1
fw_lanb_all_open=1
wan_all_open=1
wan_as_lan=1
```

If you have a Convergence 2600, the additional line `fw_dmz_all_open=1` may be necessary as well.

Afterwards the firewall rules must be regenerated, which is done with the following two commands:

```
# applyconfig.sh firewall
# applyfirewall.sh
```

(Please don't type the hash symbols (#), they just symbolize your command prompt.)

The firewall will now only contain rules for the loopback interface, custom rules given via the web GUI and custom rules from the `/etc/sysconfig/firewall.custom` file. The default policy is set to accept all packages (contrary to the normally setting of the firewall which is to reject all packages that are not explicitly allowed).

2. Firewall Marking

2.1. Introduction

The Convergence Products all support the marking of network packets. This feature is frequently being used in conjunction with the Bandwidth Management. Sometimes it is easier to define a firewall rule for marking packets that are to be handled by the traffic shaper, than using the filters of the traffic shaping.

2.2. Setup

The setup is done via the `/etc/sysconfig/firewall.custom` config file. In order to appropriately mark packets, the following line needs to be inserted.

```
iptables -A POSTROUTING -t mangle -p udp -m dscp --dscp 34
-j MARK --set-mark 5
```

This marks all UDP packets flowing through the box and having the DSCP tag 34 set. DSCP stands for Diffserv Control Point. Similarly, the TOS bit can also be adjusted if that should be

necessary. All parameters shown here are of course only examples chosen for demonstration purposes. These values can of course be adjusted arbitrarily. After entering the line apply it by typing `applyconfig.sh` or reapply the configuration via WebGUI.

2.3. Marking IPSEC Packets

Sometimes you will want to mark the payload packets of an IPSEC tunnel for performing e.g. traffic shaping. What we describe here will mark the IPSEC AH and ESP packets coming from a Convergence box. You can then use this mark to perform logging or restrict the bandwidth the VPN payload traffic may take on a link. You can also use it to prioritize this traffic.

This can be accomplished by adding a single line to `/etc/sysconfig/firewall.custom` file:

```
iptables -A OUTPUT -t mangle -p esp -j \
MARK --set-mark 0xAFFE
iptables -A OUTPUT -t mangle -p ah -j \
MARK --set-mark 0xAFFE
```

If you are using NAT traversal please use the following rule:

```
iptables -A OUTPUT -t mangle -o ipsec0 -j \
MARK --set-mark 0xAFFE
```

To activate this simply use `applyfirewall.sh`.

3. Natting inside an IPSEC Tunnel

Sometimes you will want a VPN tunnel without having a flat routing scheme across the VPN tunnel. This means that you have a private IP address range at the branch office and the official IP address is terminated on the Convergence box. Official in this sense means a valid IP address that can be routed on the other side of the VPN tunnel. It can of course also be a private IP address. This can easily be accomplished by adding a few firewall rules.

In order to achieve this, add the following lines in `/etc/sysconfig/firewall.custom` file:

```
iptables -t mangle -A OUTPUT \
-o ipsec0 -j MARK --set-mark 0x5EC
iptables -t mangle -A FORWARD \
-o ipsec0 -j MARK --set-mark 0x5EC
iptables -t nat -A POSTROUTING -o ipsec0 \
-m mark --mark 0x5EC -j SNAT \
--to-source 10.10.157.1
iptables -t nat -A PREROUTING -i ipsec0 \
-m state --state NEW -j DNAT
--to-destination 192.168.1.1
```

This example assumes that the data center end can handle the 10.10.157.1 IP address, but is unaware of the 192.168.x.x address. The data center IP is terminated on the Convergence. All internal equipment on the branch side works with the 192.168.x.x . If you are using TLS VPN tunnels, simply replace `ipsec0` with the corresponding tun device.

To activate this simply use `applyfirewall.sh`.

4. Qos Tagging (DSCP/TOS)

4.1. Introduction

The Convergence Products all support the tagging of network packets. This feature is frequently being used in conjunction with Diffserv.

4.2. Setup

The setup is done via the `/etc/sysconfig/firewall.custom` config file. In order to appropriately tag packets, the following line needs to be inserted.

```
iptables -I POSTROUTING -t mangle -p udp -m udp  
--source-port 5060 -j DSCP --set-dscp 34
```

This marks all UDP packets flowing out via eth0 and Port 5060 with the Diffserv Tag 34. DSCP stands for Diffserv Control Point. Similarly, the TOS bit can also be adjusted if that should be necessary. All parameters shown here are of course only examples chosen for demonstration purposes. These values can of course be adjusted arbitrarily. After entering the line apply it by typing `applyconfig.sh` or reapply the configuration via WebGUI.