

Application Note

Adapting current mGuard configuration files for the mGuard rs2000



mGuard rs2000

Innominate Security Technologies AG
Rudower Chaussee 13
12489 Berlin, Germany

Phone: +49 (0)30-921028 0
Fax: +49 (0)30-921028 020
contact@innominate.com
<http://www.innominate.com>

Table of Contents

1	Disclaimer	3
2	Introduction	4
3	Configuration Profile Adjustment	5
3.1	<i>VPN Connections</i>	5
3.2	<i>VPN Firewall</i>	6
3.3	<i>Other Variables</i>	6

1 Disclaimer

© Innominate Security Technologies AG

December 2011

"Innominate" and "mGuard" are registered trademarks of the Innominate Security Technologies AG. All other brand names or product names are trade names, service marks, trademarks, or registered trade marks of their respective owners.

mGuard technology is protected by the German patents #10138865 and #10305413. Further national and international patent applications are pending.

No part of this documentation may be reproduced or transmitted in any form, by any means without prior written permission of the publisher.

All information contained in this documentation is subject to change without previous notice.

Innominate offers no warranty for these documents. This also applies without limitation for the implicit assurance of scalability and suitability for specific purposes.

In addition, Innominate is neither liable for errors in this documentation nor for damage, accidental or otherwise, caused in connection with delivery, output or use of these documents.

This documentation may not be photocopied, duplicated or translated into another language, either in part or in whole, without the previous written permission of Innominate Security Technologies AG.

2 Introduction

The field line device mGuard rs2000 is optimized for being used in software-independent remote maintenance scenarios. The mGuard rs2000 can be used as a VPN client for up to two concurrent, IPsec-encrypted VPN tunnels and functions as a robust remote maintenance infrastructure for the secure connection of globally distributed machines and control units.

The functional range of the field line firmware is reduced to the essential, but is nevertheless compatible. Compared to the unlimited functionality of other mGuard products, the following features are not supported by the mGuard rs2000:

- Radius authentication
- User firewall
- Modem support
- DHCP server/DHCP relay for the external network
- Secondary external interface
- Firewall rules (only ´accept all outgoing/incoming connections´ or ´drop all outgoing/incoming connections´ is selectable)
- Advanced firewall settings (e.g. DoS Protection)

Due to the reduced functional range some configuration variables of an mGuard rs2000 configuration profile must have different values than contained in a configuration profile downloaded from another mGuard product. Therefore configuration profiles downloaded from other mGuard products (e.g. mGuard smart, mGuard industrial rs) must be adjusted before being imported and activated on an mGuard rs2000.

This document describes how to adjust a configuration profile for being activated on an mGuard rs2000, based on mGuard 7.4 configuration profiles.

3 Configuration Profile Adjustment

The following variables must be adjusted before importing and activating a configuration profile, which was downloaded from another mGuard product, on the mGuard rs2000. Any text editor supporting linefeeds in UNIX format can be used to edit the mGuard configuration profile (*.atv).

3.1 VPN Connections

The mGuard rs2000 can be used as a VPN client for up to two VPN tunnels. If the configuration profile, which should be activated, contains VPN connections, it has to be ensured that no more than two VPN tunnels are enabled. Note that more than two VPN tunnels can be configured but no more than two can be active.

The easiest way is to disable all VPN connections and to modify them afterwards through the mGuard web interface after uploading and activating the profile on the mGuard rs2000.

VPN connections have the following structure in the mGuard configuration profile:

```
VPN_CONNECTION = {
  {
    /* VPN Connection 1 */
  }
  {
    /* VPN Connection 2 */
  }
  {
    /* VPN Connection 3 */
  }
  {
    /* VPN Connection n */
  }
}
```

To disable VPN connections, set their parameter **VPN_ENABLED** to **no**.

```
VPN_CONNECTION = {
  {
    /* VPN Connection 1 */
    VPN_ENABLED = "yes"
  }
  {
    /* VPN Connection 2 */
    VPN_ENABLED = "yes"
  }
  {
    /* VPN Connection 3 */
    VPN_ENABLED = "yes"
  }
  {
    /* VPN Connection n */
    VPN_ENABLED = "yes"
  }
}
```

=>

```
VPN_CONNECTION = {
  {
    /* VPN Connection 1 */
    VPN_ENABLED = "no"
  }
  {
    /* VPN Connection 2 */
    VPN_ENABLED = "no"
  }
  {
    /* VPN Connection 3 */
    VPN_ENABLED = "no"
  }
  {
    /* VPN Connection n */
    VPN_ENABLED = "no"
  }
}
```

3.2 VPN Firewall

The variables **FW_INCOMING_GLOBAL** and **FW_OUTGOING_GLOBAL** of the VPN firewall must be adjusted as follows:

```
VPN_CONNECTION = {
  {
    /* VPN Connection 1 */
    FW_INCOMING_GLOBAL = "accept"          (or "drop")
    FW_OUTGOING_GLOBAL = "accept"         (or "drop")
  }
  {
    /* VPN Connection 2 */
    FW_INCOMING_GLOBAL = "accept"          (or "drop")
    FW_OUTGOING_GLOBAL = "accept"         (or "drop")
  }
}
```

3.3 Other Variables

The following variables must also be set to the values listed below:

```
ARP_LIMIT_EXT="10000"
ARP_LIMIT_INT="10000"
FW_ICMP="all"
FW_ICMP_EXT2="all"
FW_INCOMING_GLOBAL="accept"      (or "drop")
FW_OUTGOING_GLOBAL="accept"     (or "drop")
ICMP_LIMIT_EXT="10000"
ICMP_LIMIT_INT="10000"
IP_SYNFLLOOD_LIMIT_EXT="10000"
IP_SYNFLLOOD_LIMIT_INT="10000"
IP_UNCLEAN_MATCH="no"
```