
iSecure-ils Administration

Booklet

SCOPE  NetSecure LLC

iSecure-ils Administration

Author: Thomas Soysal (English Version)
Version: 1.0
Date: May 06, 2002
Filename: iSecure-ils Administration (Engl.).doc

The contents of this document is the property of SCOPE NetSecure LLC. Without a permission in written form from SCOPE NetSecure it may not be copied – neither partially nor entirely. Also it may not be handed over to a third party nor be published by any means.

© Copyright SCOPE NetSecure LLC.

All rights reserved.

Editor:

SCOPE NetSecure LLC
2013 Utah Ave. South
55461 Minneapolis / MN

This document was created with Microsoft Word for Windows and printed on Tektronix Phaser 740 Plus or HP Laserjet 5 N. SCOPE is a Registered Trademark of SCOPE NetSecure LLC. Microsoft and Windows are Registered Trademarks or Trademarks of the Microsoft Corporation.

Table of Contents

1 Overview _____ 1

2 iSecure Management System _____ 2

2.1 Global Management Module 3

2.2 Local Management Module 4

2.3 Web Page 5

Table of Figures

Figure 1 Scheme Administration of iSecure	2
Figure 2 Components of GMM.....	3
Figure 3 LMM Scheme.....	4
Figure 4 Home page of iSecure Administration	5
Figure 5 Example of black list configuration	6
Figure 6 Example of diagram showing DDoS attacks.....	6

Summary of Changes

Version	Date	Notes	Changed Pages	Author
1.1	05/21/2002	first final issue		

1 Overview

iSecure-ils (iSecure) is a „black box“ system (combined hardware/software solution) which recognises – in real-time – (distributed) Denial of Service attacks “(d)DoS” and effectively protects a company’s network behind the black box from those (d)DoS attacks. iSecure is transparent within the company’s network, which means, that iSecure is invisible from the company’s view and also from the view of potential hackers. This protects iSecure itself from being attacked or hacked.

All TCP traffic, which is part of (d)DoS attacks from outside the company’s network is rejected by iSecure. Proper messages are passing the iSecure box without limitations and almost without latency. Additional security functionalities are adjustable via the administration graphical user interface (GUI).

Within the pre-set standard configuration all UDP messages from outside to the inside of a company’s network are rejected, except for the communication data which are relevant for the Domain Name Service (DNS).

As mentioned before it is possible to change the pre-set standard configuration via the administration GUI. It is e.g. recommended to limit the DNS traffic for communication between tightly connected DNS servers. In addition it is possible with this method to activate further company specific UDP connections between tightly defined external and internal components.

The pre-set standard configuration also rejects all ICMP traffic. Valid pings and traceroute commands are however allowed to pass iSecure under secured conditions (only if a request has been passed from inside to outside, the reply from outside will be accepted). In addition it is possible to activate determined ICMP message types via the administration GUI.

Fragmented packets are also rejected in the pre-set standard configuration. But via the administration GUI it is possible to activate specific network areas as well as the maximum amount of valid fragmented packets. E.g. it is possible to prevent fragmented ICMP traffic but as an exception simultaneously to allow fragmented TCP traffic between two specific (and trusted) networks.

The configuration of the iSecure black box is only possible via its secure serial interface. The following settings can be done respective can be queried:

- UDP,
specify external DNS-Server , specify trusted host or network relations for additional UDP traffic (WhiteList)
- Blacklist TCP,
specify unwanted Hosts or Networks, delete / change the automated by iSecure added Host- or Networks
- ICMP,
specify the maximum accepted size of ICMP packets, specify the accepted ICMP requests and ICMP responses separately, (the status “NO” for fragmented ICMP traffic is recommended and should be not changed)
- Fragmented packets,
specify the accepted size of fragmented packets, specify trusted host or networks for fragmented TCP-Traffic
- Status (only query). ,
get statistical information out of iSecure (attacks, network traffic, availability)

2 iSecure Management System

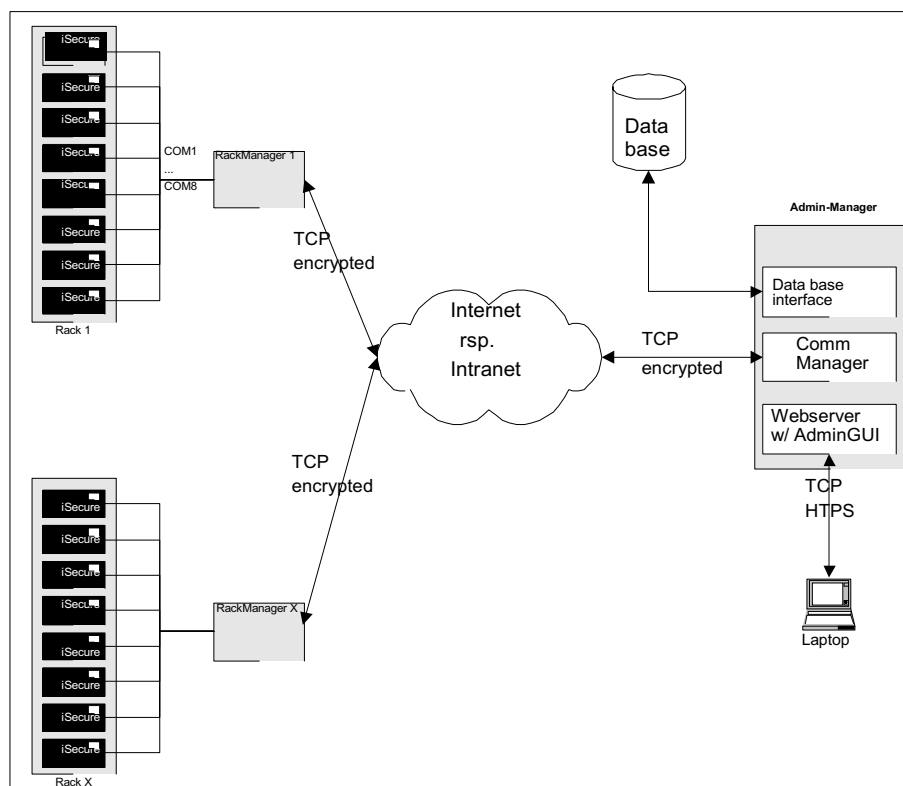
The iSecure Management System allows the administration, configuration and monitoring of up to 4096 iSecure boxes.

To ease the administration at each case up to 16 iSecure boxes are housed in one rack. A Local Management Module (LMM) communicates with the iSecure boxes via the corresponding serial interfaces and establishes the encrypted connection to the central Global Management Module (GMM) via the intranet.

Main task of the LMM is the monitoring of the attached iSecure boxes, as well as the exchange of configuration data. The status information of the iSecure boxes can be queried in configurable intervals, collected and saved in a file. If there is an alarm (e.g. in case of a dDoS attack) an event message is generated immediately and sent to the management console, also the saved file will be transferred in the background immediately to the central GMM. In other cases the saved status information are transferred to the GMM within configurable intervals. If no status information are to be collected the value Null should be adjusted.

The administration manager GMM is able to administer up to 256 LMMs. The GMM is the initiator of the encrypted communication with the LMMs, the transfer of the configuration data and the transfer of the status information (no polling).

Figure 1 Scheme Administration of iSecure



The configuration takes place with a web browser via the intranet. It is recommended to use Netscape 6 or Mozilla as a web browser. The use of Microsoft Internet Explorer is possible, but this can lead to minor differences in the graphical appearance.

2.1 Global Management Module

The central administration manager GMM consists of the following components:

- CommMgr for the encrypted communication with the LMMs,
- web server,
- PHP interface for output to the administration GUI, creation of tasks, queries of status and alarm messages,
- data base interface for processing of messages, alarm messages, configuration data and status messages.

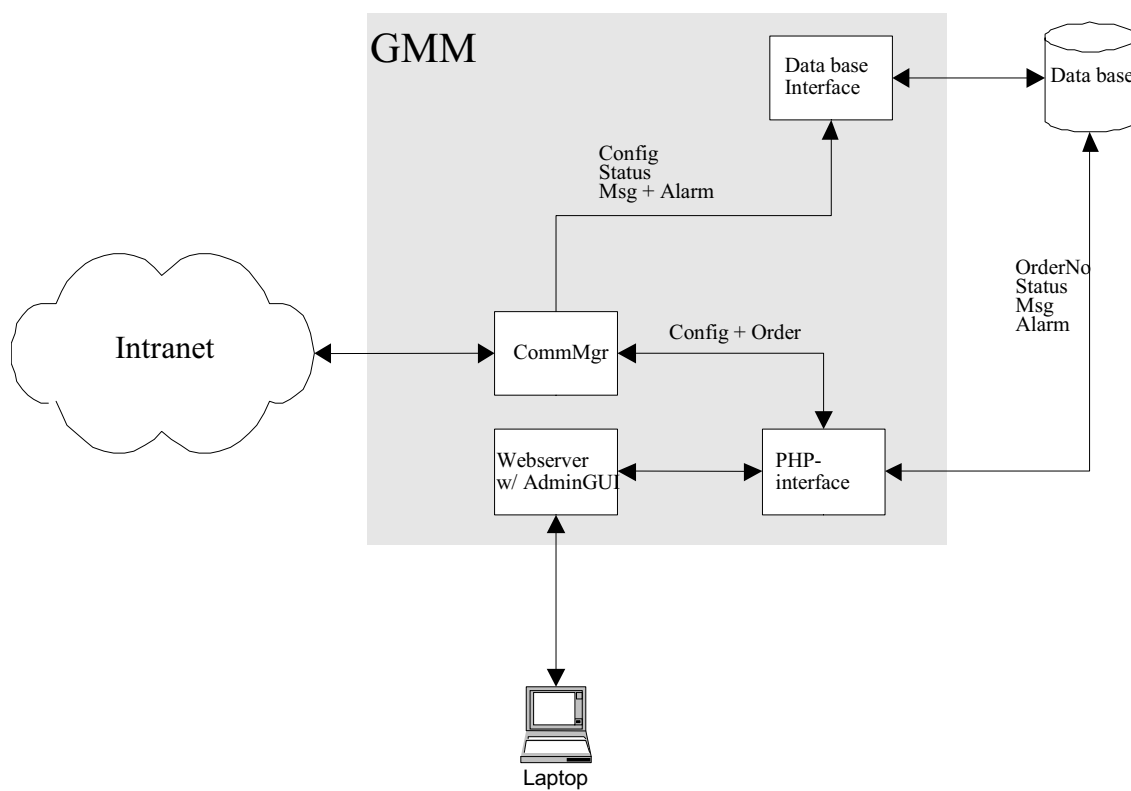


Figure 2 Components of the Global Management Module

2.2 Local Management Module

The local manager LMM consists of the following modules:

- SerialComm for encrypted communication with the GMM,
- FileProcessor for monitoring status information and buffering, as well as alarm handling.

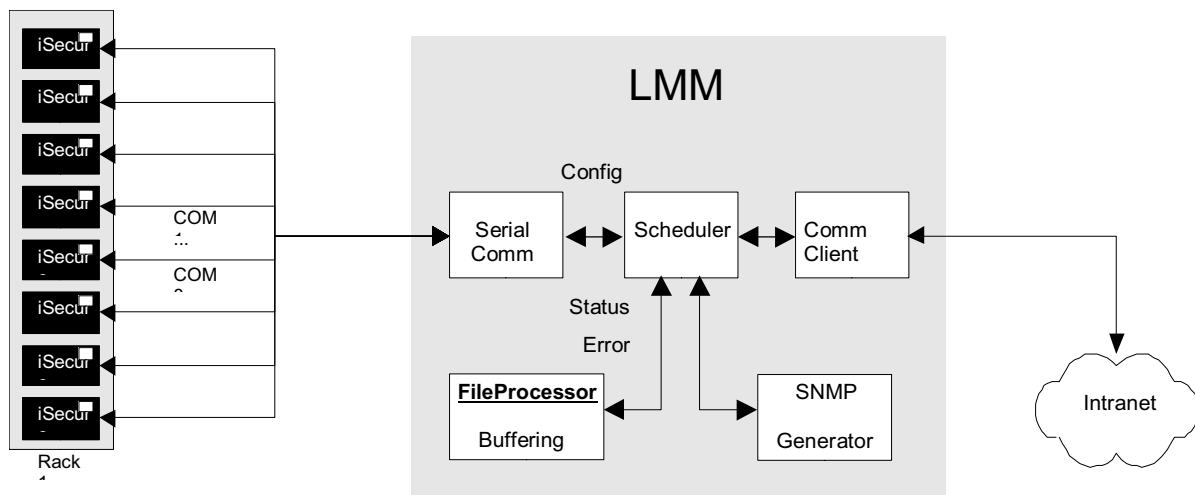


Figure 3 Scheme Local Management Module

The LMM is able to create SNMP traps which are posted to a SNMP management system. Threshold values and time intervals can be configured. SNMP traps are created for example in case of malfunctions or possible dDoS attacks. Intervals and threshold are adjustable in the LMM by management GUI. Because of security reasons it is not possible to configure the rack manager via SNMP.

2.3 Web Page

The following figures show the web pages with which the administrator is able to direct, configure and display the previously mentioned information.



Figure 4 Home page of iSecure Administration

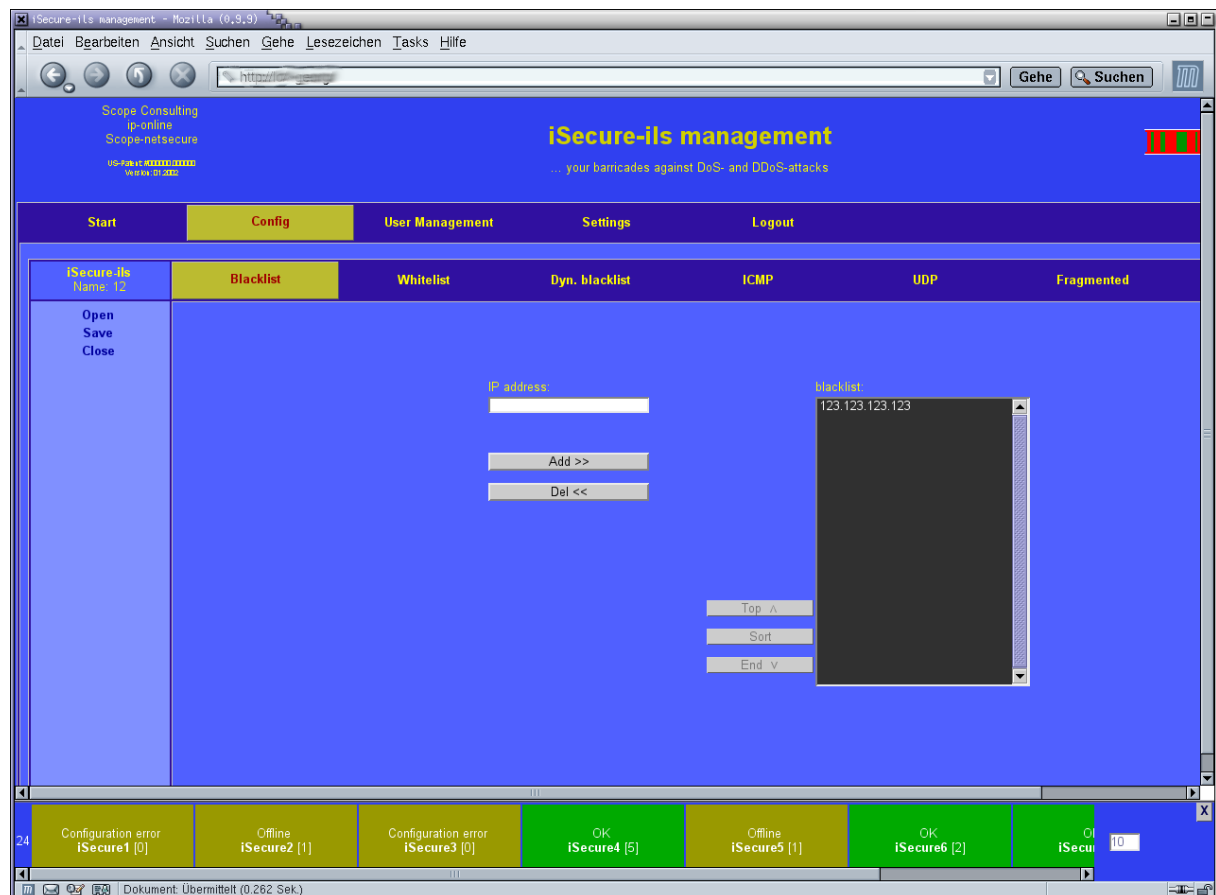


Figure 5 Example of black list configuration

It is possible to switch the language of the web pages from German to English or vice versa. Traffic and dDoS attacks are displayed as diagrams. See the example below:

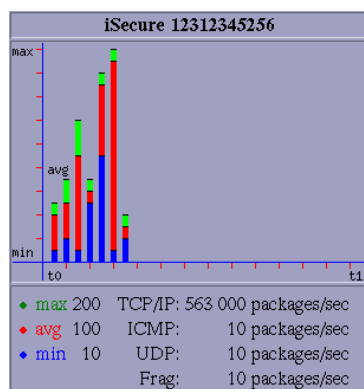


Figure 6 Example of diagram showing dDoS attacks