General Intelligence and
Security Service
Ministry of the Interior and
Kingdom Relations

Deployment Advisory

BSPA Assessment of MagiCtwin Diode

Version: 2.1
Date: December 16, 2024

Colophon

Our reference number	:	9d7d3716-or1-1.0
	:	T +31 (0)70 320 44 00
	:	F +31 (0)70 320 07 33
	:	P.O. Box 20010 2500 EA The Hague The Netherlands

Copy number	:	
Author(s)	:	NLNCSA
Number of enclosures	:	0

1 Table of contents

2 Statement of Conformity

Hereby is stated that evaluation has demonstrated that the product:

MagiCtwin Diode

from

COMPUMATICA SECURE NETWORKS BV

address
Oude Udenseweg 29, 5405 PD, Uden
The Netherlands

is in conformity to:
BSPA Security Evaluation Target MagiCtwin Diode, Version 0.6, 2024-11-18

as demonstrated by:
SGS Brightsight BV located in Delft, Netherlands

Applying:
NL Scheme for Baseline Product Assessment, February 13, 2018

This Statement of Conformity (SoC) is part of the Deployment Advisory (DA) and is only valid if the recommendations and obligations in the DA are being followed.

The DA determines the conformity of the product with its SET and the effectiveness of the security features offered by the product.

This SoC relates only to a specific version of a product. If the product is changed, this SoC is not applicable any more. Newer versions of the products need to undergo the BSPA process anew to obtain a new Statement of Conformity.

Issuance of a SoC is no guarantee that the product is free from security vulnerabilities. Also, a SoC is not an endorsement of the IT product by NLNCSA and no warranty of the IT product by NLNCSA or by any other organisation, is either expressed or implied.

Issue date: 16 December 2024

F. van Tongeren

Head of the National Communications Security Agency of
the General Intelligence and Security Service

3 Introduction

3.1 Scope

Product name	MagiCtwin Diode
Product version	**Hardware** ICS MagiC family (housing) **Software** Version 7.50.1-5
Product category	Network Security
Evaluation criteria and version	NL Scheme for Baseline Product Assessment Date: February 13, 2018
Vendor	COMPUMATICA SECURE NETWORKS BV Compumatica secure networks BV Oude Udenseweg 29, 5405 PD, Uden The Netherlands https://www.compumatica.com
Overseer	General Intelligence and Security Service Ministry of the Interior and Kingdom Relations Netherlands National Communications Security Agency (NLNCSA) P.O. Box 20010 2500 EA The Hague The Netherlands
Evaluation facility	SGS BRIGHTSIGHT Brassersplein 2 2612 CT, Delft The Netherlands

The goal of this Deployment Advisory is to inform consumers on:

- the specific use case for which the product has been tested,
- the manner in which the product has been tested and the limitations of this test process,
- the level of security provided by the product when used according to the prescribed use case,
- the residual risks of the product when used according to the prescribed use case.

This Deployment Advisory also gives guidance to users and/or administrators on how to securely use and configure the product.

3.2 Disclaimer

This advisory and associated Statement of Conformity applies only to the specific version of the product in its evaluated configuration (see section 4.1).

The Statement of Conformity is not a guarantee that the product is free from security vulnerabilities. Neither is it a guarantee that the product protects against adversaries with a high attack potential like (for example) intelligence organizations, organized (cyber-) crime organizations, terrorist organizations and capable security researchers.

Exploitable vulnerabilities may be discovered after issuance of the Statement of Conformity. The organization or individual using the product should check regularly if security vulnerabilities have been discovered and whether updates are provided by the vendor. Installation of updates must be compliant with the risk management policy[1] and risk appetite of the organization or individual using the product. Updates should only be installed if there is sufficient trust or assurance that they improve the security of the product.

This advisory is supplementary to the instructions and documentation of the vendor. It is still necessary to consult these before installing and using the product.

All product or company names used in this report are for identification purposes only and may be trademarks of their respective owners.

3.3 Certification scheme

The Dutch *Baseline Security Product Assessment* evaluates the security features of hardware and software security products for use in the "internal but unclassified" domain. The main goals of the evaluation are:

- Establishing that the product conforms to the security specification in the Security Evaluation Target,
- Establishing the effectiveness of the security features offered by the product,
- Establishing that the product has a limited impact on the security of the host system.

A positive Statement of Compliance and Deployment Advisory enables a government organization to make a better substantiated decision if these products are applicable in an ICT-infrastructure at the BBN1 or BBN2[1] level of the Government Baseline for Information Security (Baseline Informatiebeveiliging Overheid, BIO, Versie 1).

BSPA is intended for "internal but unclassified" information where there is no need for the product to be resistant against adversaries with a high attack potential[2], like intelligence organisations, organised (cyber-) crime organisations, terrorist organisations and capable security researchers

Documentation and procedures of the Baseline Security Product Assessment scheme are available at the following Internet site: www.aivd.nl search for "BSPA".

1
To attain the BIO BBN2 level, a government organization will at least need:
- additional measures for detection of cyber-attacks by adversaries with high attack potential (BIO 12.4.1.3 and BIO 13.1.2.1),
- an additional and deeper assessment of the cryptography of the product (BIO 8.3.1.2 and BIO 13.1.2.3).

2
BSPA is not designed and intended for the BIO BBN3 level (and higher classifications and threat levels). For the assessment security products for the BIO BBN3 level a national evaluation scheme exists, with different characteristics

3.4 Copyright information

3.5 Contact information

All correspondence regarding this deployment advisory should be addressed to:

General Intelligence and Security Service
Ministry of the Interior and Kingdom Relations
NLNCSA
P.O. Box 20010
2500 EA The Hague
The Netherlands
bspa@nlncsa.nl

4 Product overview

4.1 Product version

This deployment advisory is limited to version 7.50.1-5.

4.2 Product identification

The current version is specified on the 3rd page of the SET.

After installation the product version can be found in Web UI page.

4.3 Security functions

The evaluated security functions of TOE are:

- Uni-directional communication channel (diode) from TX to RX.
- Proxies: SFTP/SCP, SMTP.
- NTP, TX Heartbeat, Port Mirroring, and OPC UA.
- UDP Relay.
- Authentication on configuration interfaces: WebUI over HTTPS, SSH.

Security functions that are not evaluated are:

- MASC
- VPNs (OpenVPN and IPSEC).
- HA and AIDE.
- Diode protocols: FTP and FTPS.
- Proxies and relays: HTTP, FTP, Telnet, NNTP, POP3, NET8, MGNT, and the TCP relay.
- SCADA proxies.
- CLI tools such as ping and netcat.
- Sending of system alerts per email to the administrator.
- Sending of system logs to a remote syslog server.

4.4 Product description

The Compumatica MagiCtwin Diode is a network appliance that enforces through hardware one-way data transfer between networks. Its hardware is designed to allow data to flow in one direction only, while preventing any data from flowing back in the opposite direction. Each CompuWall in the MagiCtwin Data Diode has specific diode proxies corresponding to their side. Management (web and SSH) of the TX and RX side of the diode is done independently of each other. There is no possibility to manage the RX over the TX side or vice versa.

4.5 Product category

- ☑ 01 – Network security
- 02 – Network filtering, detection and response
- 03 – Secure messaging
- 04 – Media and file security
- 05 – Identity and access management
- 06 – Secure OS execution environment
- 07 – Hardware and embedded software

4.6 Product configuration

The following configuration options are the most suitable given the typical use case of the TOE:

Uni-directional communication channel (diode) from TX to RX.
Proxies: SFTP/SCP, SMTP.
NTP, TX Heartbeat, Port Mirroring, and OPC UA.
UDP Relay.
Authentication on configuration interfaces: WebUI over HTTPS, SSH.

All other configuration options are not within scope of the evaluation.

5 The evaluated use-case for the product

The TOE provides one-way data transfer between networks, and requires network connectivity between MagiCtwin Diode proxies to function. The optical fiber is an internal connection between two individual systems, one of which transmits the data (TX), and the other one receives the data (RX), all of which happens within the same 1U server hardware.

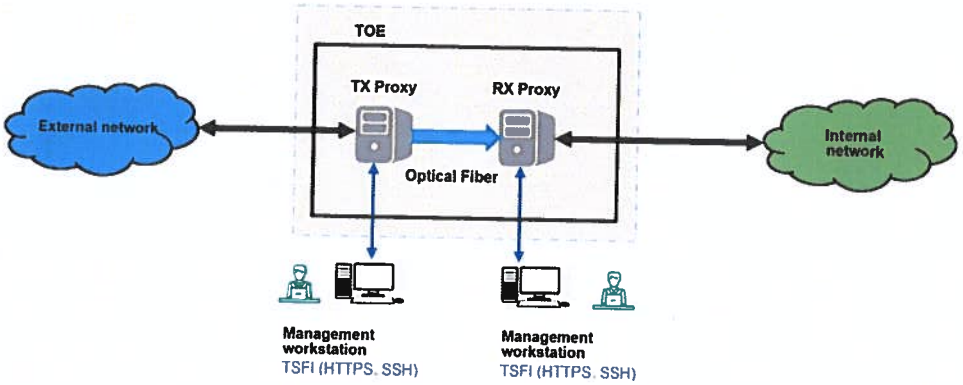

Figure 1 TOE Configuration

The TOE must be stored in a physically secured environment that can only be accessed by authorized personnel, as it has no protection against physical attacks.

The TOE' s initial configuration may be done locally. A user can connect to the TOE' s display interface and perform configuration this way. Alternatively, a client configured as SSH / Web Management which is reachable over any of the TOEs management network interfaces (TX or RX) can be used to execute configuration commands. No (public) internet connectivity is needed at any time.

The TX and RX sides must be configured on different networks, and no other physical communication line should be available between TX and RX, apart from the fiber connection.

Explicitly:

- The TX side management workstation must not be connected to the internal network
- The RX side management workstation must not be connected to the external network.
- The TX and RX management workstations must not be connected to the same network.

The following configuration options are the most suitable given the typical use case of the:

- Uni-directional communication channel (diode) from TX to RX.
- Proxies: SFTP/SCP, SMTP.
- NTP, TX Heartbeat, Port Mirroring, and OPC UA.
- UDP Relay.
- Authentication on configuration interfaces: WebUI over HTTPS, SSH.

The product has **not been evaluated** for any other use cases.

6 Scope and limitations of the evaluation

6.1 Evaluation facility

The security test has been performed by
SGS BRIGHTSIGHT
Brassersplein 2,
2612 CT, Delft,
The Netherlands,
www.brightsight.com

6.2 Test duration and time used

The vulnerability analysis and the security tests have been performed between July 2024 and November 2024.

6.3 Evaluation process and scope

The following time-boxed evaluation process was employed:

analysis of the MagiCtwin Diode v7.50.1-5,
analysis of assets and assumptions,
desk study of a multi-functional "black box" built as data diode including management interfaces,
definition of the attacker model for the specific use case,
vulnerability analysis based on the results of the protocol desk study
testing based on the results of vulnerability analysis.

6.4 Product procurement, installation and configuration for evaluation

The default installation steps were used and installed by the developer on site.

Special configuration was necessary, as described in the Secure Baseline Configuration MagiCtwin Diode v7.50.1-5 document.

7 Recommendations for the administrator/user

Only administrator can configure the TOE. The administrator must follow the guidance when installing and configuring the TOE.

7.1 Procurement of the product

The product can be ordered at Compumatica.

7.2 Installation of the product

Consult the most recent (security-) instructions and documentation of the vendor before installing and configuring the product. Consult any additional material when relevant.

7.3 Configuration of the product

The following configuration options must be set:

Uni-directional communication channel (diode) from TX to RX.
Proxies: SFTP/SCP, SMTP.
NTP, TX Heartbeat, Port Mirroring, and OPC UA.
UDP Relay.
Authentication on configuration interfaces: WebUI over HTTPS, SSH.

All other configuration options were not within scope of the evaluation.

7.4 Security risks and countermeasures

The administrator must be aware that the TOE does not provide authentication (brute-force) protection on management interfaces. If such protections are required to protect the assets, additional measures must be taken, in addition to deploying the TOE.

The administrator must be aware to follow the Secure Baseline Configuration MagiCtwin Diode v7.50.1-5 guidance steps. In order to be protected against brute-force attacks, the guidance instructions are to configure a proper password length, and additional security measures.

Additional security measures include configuring the access to the management interfaces (HTTPS, SSH) only on trusted networks, on specific IP addresses and network interfaces from which administrative activities could be performed.

The administrator must be aware that the FTP protocol is taken out of scope. If configured, the credentials could be sent in plain text over an insecure channel. This could impact the SFTP user credentials as well, given the fact that the same user credentials are used for different protocols.

The administrator must be aware that application layer protocol (i.e. SSH) based encryption rules perform filtering based solely on the source and destination ports contained in the transport layer protocol's header. Custom rules may be created for arbitrary port numbers, and this should be done if encryption is desired for a protocol which is used with a non-standard port.

7.5 Availability risks and countermeasures

None

7.6 Do's

Follow the configuration as described in the SET and in the Secure Baseline Configuration MagiCtwin Diode v7.50.1-5.

Configure the access to the management interfaces (HTTPS, SSH) on trusted networks, only on the IP address and network interface where it will be used for administration activities.

The administrator should carefully consider the filtering rules for un-encrypted protocols to prevent the hypothetical situation that one of the unencrypted protocols could be used to manipulate the data that is encrypted in another protocol.

7.7 Don't s

Do not rely on generic protocol names, but verify the actual port numbers that the protocol uses before applying the configuration.

Do not rely on the TOE for protection against brute – force attacks.

Do not physically connect the TX network with the RX network.

* * *