advenica

SecuriCDS® DD1000A & DD1G

Recommended Security Management

Document version: 17113v1.3 SecuriCDS DD1000A & DD1G - Recommended Security Management

TABLE OF CONTENTS

1. INTRODUCTION

This document provides information that refers to the operational management of the SecuriCDS Data Diode DD1000A (see *Figure 1*) and DD1G (see *Figure 2-4*). It specifies recommendations concerning usage, system configuration and environment. DD1000A and DD1G are Data Diodes, meaning that they only allow information to flow in one direction.

Please note! *The DD1000A and DD1G devices are designed to be used as components of highly sensitive networks. The overall security offered by the system is depending on correct use.*

The specified rules and regulations in this document can be used as is or modified according to your own organisational policies.

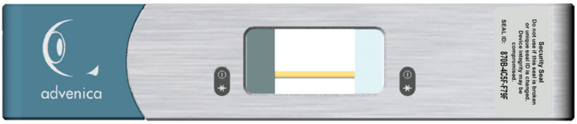
advenica
Security Seal
Do not use if this seal is broken or unique seal ID is changed. Device integrity may be compromised.
SEAL ID: 870B-4C5F-F79F

Figure 1 - SecuriCDS Data Diode DD1000A.

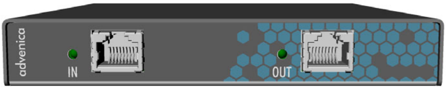

Figure 2 - SecuriCDS Data Diode DD1G-S.

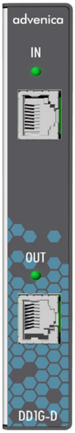

Figure 3 - SecuriCDS Data Diode DD1G-D.

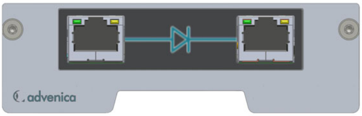

Figure 4 - SecuriCDS Data Diode DD1G Gen 2.

1.1 DESCRIPTION

The Data Diode system at its core provides a unidirectional diode functionality for establishing one-way connectivity between networks.

The Data Diode can be used in two main scenarios. The first is when you want to send data to a destination network where **confidentiality** is the primary focus, i.e., it is essential that nobody can access information stored on the destination network from the source network.

The second scenario is when you want to send data from the source network where **integrity** is the primary focus, i.e. that nobody can modify the resources located in the source network from the destination network.

1.2 SECURITY FUNCTIONALITY

The security functionality of the Data Diode is its diode functionality, i.e. that the device only allows for information to flow in one direction. A Data Diode is said to have a direction. The direction of the Data Diode is the direction that information is allowed to flow (see *Figure 5*).

To represent the Data Diode functionality the symbol for a semiconductor diode is used.

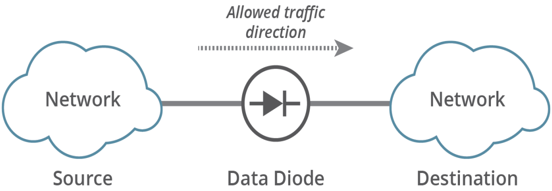

Figure 5 - Data Diode traffic direction.

The information will be allowed to flow from left to right in the picture, i.e. from the source network to the destination network.

In this document it is assumed that the Data Diode is connected on both sides to networks of some kind. However, either side could be replaced by a single node, e.g. a computer. You could use a Data Diode and connect to a standalone computer or system on each side or a combination of a network and a computer or system.

Please note! *A Data Diode does not add any cryptographic confidentiality and integrity protection to the information sent through it.*

1.3 DEVICE FUNCTIONALITY

The DD1000A and DD1G Data Diodes operate on layer 2 and carry only diode functionality. In many cases you will need some kind of proxy service on each side to handle the "non-response" and lack of acknowledgement messaging.

2. SECURITY OPERATIONS

The device should be controlled by, and available to, authorised personnel only. Personnel appointed to access and handle the device should be trained, cleared and authorised.

Please note!

- All personnel that handle network security equipment should have appropriate training both on the device and on network configuration in general.
- All personnel that handle network security equipment should be authorised for their job.
- All personnel that handle network security equipment should be trusted.

2.1 ROLES

For the use of the product there are three recommended roles:

- User
- Local System Operator
- Security Manager

2.1.1 USER

The **User** is anyone that uses the device, in many cases indirectly, to send information from the source to the destination network. In some cases the User will not even know that their data flows through a Data Diode.

2.1.2 LOCAL SYSTEM OPERATOR

Local System Operator is someone who handles the installation, network connection and maintenance on the system as a physical device.

Local System Operators are critical, from a security point of view, in that they can potentially circumvent the diode functionality by not connecting the device at all.

⚠ ***Please note!*** *The security model of the Data Diode assumes trusted Local System Operators.*

2.1.3 SECURITY MANAGER

The **Security Manager** is a role to whom incidents and suspected incidents concerning the device are reported.

3. CONTROLS AND CONSIDERATIONS

A Data Diode is at its core a very simple device but have one paramount choice to be concerned with. A Data Diode is always used in a network solution with an intended direction in mind. Before connecting the device to the network, the Local System Operator must be fully aware of the intention and have clear instructions on what network needs to connect to each of the source and destination sides, i.e. the **DATA IN** and **DATA OUT** interfaces on the Data Diode.

It is highly recommended to work with marked cables to avoid mistakes in the physical installation.

Warning! *Connecting the DATA IN and DATA OUT Ethernet interfaces can, if made incorrectly, risk compromising the networks. The device itself does not know the intended data flow direction.*

3.1 INTEGRITY CHECKS AND REGULAR CONTROLS

It is recommended to have an agreement in place with Advenica on how the device integrity will be protected during transportation and how it can be verified at delivery.

Some integrity protection can be handled through the packaging. There are also a couple of features of the device itself that can be part of such verifications:

1. The part number - Verify the part number on the label at the bottom of the device case.
2. The PID serial number - Verify the PID serial number on the label at the bottom of the device case.
3. The tamper seal - Inspect that the tamper seal is intact, unbroken and shows no signs of tampering.
4. The device exterior - Inspect that the device casing is intact, unbroken and shows no signs of tampering.
5. The fiber inspection window (*DD1000A only*) - Inspect that nothing out of the ordinary can be seen through the fiber inspection window.

The thoroughness of an integrity check can vary a lot depending on the time spent. It is important to provide the person performing the inspection with facts beforehand on what should be expected, e.g. lists of the expected part and PID serial numbers.

Depending on the sensitivity of the network and your organisational policy you may want to prepare photos of each device's tamper seal and casing to provide the inspector with something to compare with at the time of inspection.

It is recommended that procedures for the following is defined within your organisation:

- Checks to be made before putting device in operation
- Regular integrity checks of devices in operation

The checks may be performed by the Local System Operator(s) or it may be assigned to a separate role.

The checks to be made before putting a device in operation should include:

1. Verification of the intended direction of the connection
2. Application and verification of markings to the cables to be connected to the device
3. Integrity checks of the device as presented above

The regular integrity checks of devices in operation should include:

1. Integrity checks of the device as presented above
2. Checks that the ports of the device and the connected cables show no signs of tampering

3.2 NETWORK CONFIGURATION

The reason a Data Diode is used is to only allow communication between networks in one direction. This attribute is dependent on that no other routing exist between the destination and source network, i.e. information cannot flow to the source network through the Data Diode and it cannot flow any other way either.

Please note! *No other network connections must exist that creates a less restrictive reverse route between the destination and source network.*

4. OPERATIONAL ENVIRONMENT

⚠ ***Please note!*** *The Data Diode should be protected similarly to other devices on the network.*

The Data Diode is built to withstand physical tampering attempts through the use and inspection of the tamper seal. However, a more advanced attacker will, given time and resources, be able to circumvent this. Therefore it is essential that, from a physical point of view, the device is deployed in a protected environment. It also needs to be protected during storage and transportation.

⚠ ***Please note!*** *The Data Diode must be operated in an environment where it is protected from unauthorized physical access.*

The DC current carried over the DD1000A power extension cable to the secondary power connector on the destination side is filtered. If required, the DD1000A provides the possibility of feeding each side of the diode from separate power supplies by disconnecting the power extension cable and feeding the secondary power connector from a separate power supply.

The DD1G models will become operational when connecting a single power supply to any side of the diode. Power redundancy can be achieved by connecting a second power supply to the side not already connected.

When designing and configuring the network layout close to the Data Diode, increased security can be achieved by careful routing and configuration of the surrounding devices. E.g. even though no traffic will be able to pass through the Data Diode against its direction there is no reason to allow traffic to be routed towards the diode’s out port in the first place.

⚠ ***Please note!*** *Remember that all traffic is allowed to pass through the Data Diode in its allowed direction. Therefore, in most cases the Data Diode is placed in series with other devices that provide control of and protection against the traffic content as such.*

5. HANDLING SECURITY EQUIPMENT

Any device used for protection of networks needs to be handled accordingly. This is true for Data Diode as well. The device should be stored in a protected environment as well as being protected during transport.

5.1 REGULAR CONTROL

It is recommended to establish procedures for regular control of diodes in operation (see *"Integrity checks and regular controls"* on page 10). At a minimum the following should be verified:

- Check that the tamper seal (see *Figure 6*) and casing are intact and not broken or tampered with.
- Check that Data Diode ports and connected cables have not been tampered with.

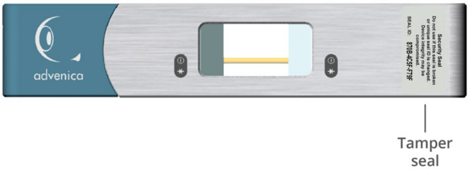

Figure 6 - Tamper seal, DD1000A example.

Warning! *In case the tamper seal, casing, ports or cables have been broken or tampered with, the integrity of the Data Diode can no longer be trusted and it is recommended that it is disconnected immediately.*

5.2 SENDING A DEVICE FOR REPAIR AND MAINTENANCE

The traffic sent through the diode does not touch any non-volatile memory on its way through the Data Diode. After leaving the device powered off for 20 minutes at room temperature the device should carry no remanence of any data.

6. EMERGENCIES AND INCIDENTS

6.1 FAIL-CLOSED DESIGN

The device is designed and built to fail in a closed state. This means that if it loses power or if parts of it break or fail, the result will still be a uni-directional connection or, more likely, no connection at all.

6.2 SUSPECTED COMPROMISE

There should be a procedure established for the Local System Operators to follow if they suspect any compromise of the device. They should report the suspected incident to the Security Manager. The recommendation is also to stop using the device until the suspected compromise has been investigated.

⚠ ***Please note!*** *Suspected compromise of the device should be reported to the Security Manager and the device should no longer be used until the suspicion has been cleared.*

6.3 END-OF-LIFE AND DECOMMISSIONING

User data does not touch any non-volatile memory on its way through the Data Diode. After leaving the device powered off for 20 minutes at room temperature the device should carry no remanence of any data.

Your organisational policy may have strict rules on safe disposal. If so, the procedure for disposal of the Data Diode includes destroying the inner circuitry. Perform the following steps:

1. Remove the top cover.
2. On each side, remove the inner cover protecting the diode board and remove the boards. Destroy the boards according to organisational policy.

advenica

Roskildevägen 1
SE-211 47 Malmö, SWEDEN

Phone +46 40 60 80 401

E-mail helpdesk@advenica.com
URL www.advenica.com