advenica

SecuriCDS® DD1000i
Recommended Security Management

Document version: 17954v1.1 SecuriCDS DD1000i - Recommended Security Management

TABLE OF CONTENTS

1. INTRODUCTION

SecuriCDS DD1000i is a Data Diode which means that it only allows information to flow in one direction.

The information in this document refers to the operational management of the DD1000i (see *Figure 1*). It specifies recommendations concerning usage, system configuration and environment.

Please note! *The DD1000i is designed to be used as a component of highly sensitive networks. The overall security provided 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 organisational policies.

Figure 1 - SecuriCDS DD1000i.

1.1 DESCRIPTION

The DD1000i system at its core provides a unidirectional diode functionality for establishing one-way connectivity between networks. In addition, the DD1000i includes two proxy computers, one before (upstream) and one after (downstream) the diode which together provide a set of communication services.

The DD1000i can be used in two main scenarios. The first is when you want to send data to a downstream network where **confidentiality** is the primary focus, i.e. it is essential that nobody can access information stored on the downstream network from the upstream network.

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

1.2 SECURITY FUNCTIONALITY

The security functionality of the DD1000i is its diode functionality, i.e. that the device only allows for information to flow in one direction. The diode provides a unidirectional connection. A Data Diode is said to have a direction. The direction of the diode is the direction that information is allowed to flow (see *Figure 2*).

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

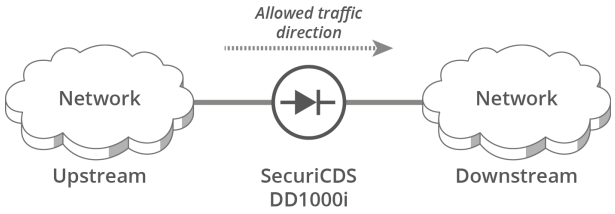

Figure 2 - DD1000i traffic direction.

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

In this document it is assumed that the Data Diode is connected at 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 at each side or a combination of a network and a computer or system.

This unidirection of the Data Diode is complete in that nothing, not even protocol acknowledgement, success and fail messaging or requests for re-sending is allowed in the direction opposite of the diode's. While this is the sought after attribute of a Data Diode it provides a challenge for many of the communication protocols normally used when providing services over a network.

The unidirection also protects the confidentiality of the information at the downstream network in that it cannot be extracted back through the Data Diode connection. Likewise, the unidirection protects the integrity of the information at the upstream network in that nothing can enter into the upstream network and risk its integrity. Normally, only one of the scenarios are required.

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 DD1000i ties together the functionality of a Data Diode with the platform and software necessary on each side to enable a set of transfer services.

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 four recommended roles:

- User
- Local System Operator
- Administrator
- Security Manager

2.1.1 USER

The **User** is anyone that uses the device to send information from the upstream to the downstream network. The User will interact with the service interface on each side of the DD1000i and in some cases the User will not even know that there is a Data Diode in the middle.

2.1.2 LOCAL SYSTEM OPERATOR

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

2.1.3 ADMINISTRATOR

The **Administrator** is someone who configures the services available, i.e. operates the device on a logical level. The Administrator does not necessarily have physical access to the device.

Both the Local System Operator and the Administrator are critical in that they can potentially circumvent the Data Diode functionality, either through rewiring or by feeding information from the outside onto the upstream proxy.

Please note! *The security model of the DD1000i assumes trusted Local System Operators and Administrators.*

Having two persons sharing both the Administrator and the Local System Operator role is a better approach than necessarily separating them since they then indirectly act as reviewers of each other. Having a single person carrying both roles may, however, be necessary, especially in smaller organisations.

2.1.4 SECURITY MANAGER

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

3. CONTROLS AND CONSIDERATIONS

3.1 INTEGRITY CHECKS AND REGULAR CONTROLS

It is recommended to have an agreement in place with the vendor of the DD1000i 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 - 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 shows no signs of tampering

4. CONFIGURATION

A Data Diode is at its core a very simple device but have one paramount configuration 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 upstream and downstream proxies, i.e. the **DATA IN** and **DATA OUT** interfaces on the device.

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.*

Before taking any DD1000i into operation or connecting the device to any live networks, the following should be performed:

1. Verify that the tamper seal on the front of the device as well as the device casing is intact, unbroken and shows no signs of tampering.
2. Run the installation for both proxies.
3. Change all pre-set passwords.
4. Verify the intended direction of the connection.

4.1 ADMINISTRATION

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 downstream and upstream network, i.e. information cannot flow to the upstream network through the 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 downstream and upstream network.*

To limit the risk of compromising this attribute of unidirectionality the two sides of the DD1000i should be kept separated in terms of administration as well. Each side of the device has its own administration interface (ADMIN Ethernet interfaces), i.e. it is important that these administration networks are separated. If you use the same administrative network you have created a potential attack vector for a route between the two sides.

Please note! *Each side of the DD1000i should be administered from separate networks.*

4.2 IPMI

The two proxy platforms, one on each side, come with an Intelligent Platform Management Interface (IPMI) functionality. IPMI is normally used to simplify the management of computers and servers in an environment.

However, at delivery IPMI is not accessible on the **ADMIN** interface or any other external interfaces, unless specifically requested by the customer.

Please note! *IPMI is configured to not listen to any external interfaces at delivery.*

Warning! *It is possible to re-enable the IPMI interfaces. It will not change the DD1000i functionality as such. It will, however, increase the attack surface of the device and is not recommended. Make sure you understand all security implications before enabling IPMI.*

4.3 PASSWORDS

There is a set of passwords used in the DD1000i solution. They are pre-set during installation and should all be changed before using the DD1000i in a production environment.

Please note! *All passwords should be changed before using the DD1000i in a production environment.*

4.4 BIOS SETTINGS

There are situations where a reset of the BIOS settings might occur, e.g. during updates of BIOS firmware. In such a situation the settings performed at production will be lost.

To reconfigure the recommended BIOS settings, perform the following steps:

1. Connect a display and a keyboard to the Upstream or Downstream proxy on the SecuriCDS DD1000i.
2. Press **DEL** while the Upstream or Downstream proxy is starting up to enter the **BIOS setup**.
3. Login using *northernp1ke* as password.

   Please note! *The default BIOS password (northernp1ke) should be changed before using the DD1000i in a production environment.*
4. Navigate to **Save&Exit/Restore Defaults** in the BIOS settings.
5. Select **YES** when prompted to **Load Optimized Defaults?**.
6. Follow the **recommended BIOS settings** that should be changed from their default values (see *Table 1* below).

Setting	*Value*	*Comment*
Advanced\Chipset Configuration\South Bridge\USB Configuration\USB Mass Storage Driver Support	Disabled	-
Advanced\Chipset Configuration/PCIe/PCI/PnP Configuration\Load Onboard LAN X OPROM	Disabled	There are four settings, LAN 1 to LAN 4.
Advanced\Serial Port Console Redirection\Console Redirection	Disabled	There are three settings with the same name. All should be Disabled.
Advanced\Boot Feature\WOL Support	Disabled	WOL (Wake On LAN)

Table 1 - Recommended BIOS settings.

Setting	Value	Comment
IPMI	Disabled	IPMI is configured to only listen on an internal interface making it unreachable from any external port. This setting is not made in BIOS.
Boot\Boot Option #1	Intel SSD	-
Boot\Boot Option #2 and #3	Disabled	-
Boot\Network Device BBS Priorities\Boot Option #X	Disabled	There are currently only one Boot option, #1 (future updates might include additional Boot options).
Security\Administrator Password	-	The password should be assigned by the System Administrator.

Table 1 - Recommended BIOS settings.

At production, the devices BIOS settings have been saved to the **User Default** slot. This can be used if a user have changed some settings of their own and want to get back to the settings made by Advenica. This is made through the **Restore User Defaults** alternative under the **Save & Exit tab**.

Please note! *The* ***Restore User Defaults*** *does not survive a firmware update of the BIOS. If BIOS has been updated, the above table should be used as guidance.*

5. OPERATIONAL ENVIRONMENT

The DD1000i provides a proxy platform for services tied to its core Data Diode functionality. The proxies of DD1000i are not designed to be bastion hosts, i.e. depending on the deployment situation its proxy computers should be protected accordingly.

Please note! *The DD1000i should be protected similarly to other devices on the network.*

From a physical point of view, the DD1000i assumes being deployed in a protected environment. It also needs to be protected during storage and transportation. The device is built to withstand light tampering attempts but a more advanced attacker will, given time and resources, most likely succeed.

The DD1000i is delivered with port lock panels that can be used together with two padlocks. When attached they block the access to the proxies USB and VGA interface as well as the ADMIN Ethernet port.

Please note! *The DD1000i must be operated in an environment where it is protected from unauthorized physical access.*

If required, it is possible to feed power to each side of the DD1000i from separate power supplies since the DD1000i is equipped with individual power connectors for the DATA IN and DATA OUT sections.

Please note! *Remember that all traffic is allowed to pass through the DD1000i in its allowed direction. Therefore, in most cases the device is placed in series with other devices that provide control of and protection against the traffic content as such.*

6. HANDLING SECURITY EQUIPMENT

Any device used for protection of networks needs to be handled accordingly. This is true for DD1000i as well. The device should be stored in a protected environment as well as being protected during transport.

6.1 LOG CONTROL

It is recommended practice to regularly check each proxy's system logs for signs of attacks or unwanted behaviour, preferably by configuring log events to be sent to monitored external Syslog servers.

6.2 REGULAR CONTROL

It is recommended to establish procedures for regular control of a DD1000i in operation (see *"Integrity checks and regular controls"* on page 9). At a minimum the following should be verified:

- Check that the tamper seal (see *Figure 3*) and casing are intact and not broken or tampered with.
- Check that DD1000i ports and connected cables have not been tampered with.

Figure 3 - Tamper seal.

Warning! *In case the tamper seal, casing, ports or cables have been broken or tampered with, the integrity of the DD1000i can no longer be trusted and it is recommended that it is disconnected immediately.*

6.3 SENDING A DEVICE FOR REPAIR AND MAINTENANCE

If the DD1000i has been used in a way where sensitive information has passed through it, the following is recommended before sending the product for repair or maintenance:

- Remove the two SSD drives from their slots at the rear of the device and store them securely.

If the problem is suspected to be related to the OS, software or SSD drives, please contact the product support before sending the driveless device since there might be questions that the support has that needs to be investigated and answered with the drives still in place.

7. EMERGENCIES AND INCIDENTS

7.1 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 unidirectional connection or, more likely, no connection at all.

7.2 SUSPECTED COMPROMISE

There should be a procedure established for the administrators 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.*

7.3 END OF LIFE AND DECOMMISSIONING

If the DD1000i has been used in a way where sensitive information has passed through it the following is recommended when the equipment reaches end of life:

1. Remove the two SSD drives from their slots at the rear of the device and process them (destroy, or render the information unrecoverable) according to organisational policy.
2. Remove the top cover and on each side remove the main circuit boards (service platform motherboard). Destroy them according to organisational policy.
3. On each side, remove the inner cover protecting the Data Diode board and remove the boards. Destroy them 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