19.4. Diodes

Objective

19.4.1. Networks connected to one-way (uni-directional) gateways implement diodes in order to protect the higher classified system.

Context

Scope

19.4.2. This section covers information relating to filtering requirements for one-way gateways used to facilitate data transfers. Additional information that also applies to topics covered in the section can be found in:

- Chapter 12 – Product Security which provides advice on selecting evaluated products.
- Section 20.1 – Data Transfers; and
- Section 20.2 – Data Import and Export;

References

19.4.3. Further information on the Evaluated Products List can be found at:

Reference	Title	Publisher	Source
	Evaluated Products List (EPL)	AISEP	https://www.cyber.gov.au/acsc/view-all-content/epl-products

Rationale & Controls

Diode assurance levels

19.4.4.R.01. **Rationale**

A diode enforces one-way flow of network traffic thus requiring separate paths for incoming and outgoing data. As such, it is much more difficult for an attacker to use the same path to both launch an attack and release the information. Using diodes of higher assurance levels for higher classified networks provides an appropriate level of assurance to agencies that the specified security functionality of the product will operate as claimed.

19.4.4.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4015]

Agencies MUST use devices as shown in the following table for controlling the data flow of one-way gateways between networks of different classifications.

High network	Low network	You require
RESTRICTED	UNCLASSIFIED	EAL2 or PP diode
	RESTRICTED	EAL2 or PP diode
CONFIDENTIAL	UNCLASSIFIED	high assurance diode
	RESTRICTED	high assurance diode
	CONFIDENTIAL	high assurance diode
SECRET	UNCLASSIFIED	high assurance diode
	RESTRICTED	high assurance diode
	CONFIDENTIAL	high assurance diode
	SECRET	high assurance diode
TOP SECRET	UNCLASSIFIED	high assurance diode
	RESTRICTED	high assurance diode
	CONFIDENTIAL	high assurance diode
	SECRET	high assurance diode
	TOP SECRET	high assurance diode

Diode assurance levels for NZEO networks

19.4.5.R.01. **Rationale**

As NZEO networks are particularly sensitive additional security measures are necessary when connecting them to other networks.

19.4.5.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4028]

Agencies MUST use a diode of at least an EAL4 assurance level between an NZEO network and a foreign network in addition to the minimum assurance levels for diodes between networks of different classifications.

19.4.5.C.02. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4030]

In all other circumstances the table at 19.4.4.C.01 MUST apply.

19.4.5.C.03. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:4032]

Agencies SHOULD use a diode of at least an EAL2 assurance level or a Protection Profile between an NZEO network and another New Zealand controlled network within a single security domain.

Volume Checking

19.4.6.R.01. **Rationale**

Monitoring the volume of data being transferred across a diode will ensure that it conforms to expectations. It can also alert the agency to potential malicious activity if the volume of data suddenly changes from the norm.

19.4.6.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:4039]

Agencies deploying a diode to control data flow within one-way gateways SHOULD monitor the volume of the data being transferred.