Arbit Data Diode

Whitepaper

Release 2019-05-20

Arbit technical reference:
Rasmus Borch
rb@arbitsecurity.com

Hardware

There are three options on hardware for the Arbit Data Diode:

1. Arbit Data Diode Devices (two non-server enclosures supported by two proxy servers)
2. Arbit Data Diode Units (two server enclosures + optionally two proxy servers)

All Arbit Data Diode solutions consist of two enclosures (PITCHER and CATCHER) connected by a single fiber-optic cable. The PITCHER connects to the LOW side network and the CATCHER connects to the HIGH side network.

The Arbit Data Diode has two basic configurations available, which has different capabilities.

Option 1: Arbit Data Diode Device solution

This data diode consists of two simple enclosures (Pitcher Device and CATCHER Device) connected by a single fiber-optic cable. The Devices handles all the uni-directional network traffic properties of the data diode, but contains not software or configuration. Two additional servers (one LOW side and one HIGH side) must be added to this solution in order to make a fully functional data diode. The servers can be designed for the specific use-case required. Servers from DELL, HP and Lenovo are supported.

Certified Common Criteria EAL 5+

Option 2: Arbit Data Diode Unit solution

This data diode consists of two advanced enclosures (Pitcher Unit and Catcher Unit) connected by a single fiber-optic cable. The Units handles all the time critical processing required by the diode software in addition to all the uni-directional network traffic properties of the data diode. The Units support NTP and TCP/UDP streaming without any additional servers required. In order to handle file, mail or HTTPS transport two additional servers must be added. They can be virtual servers. However, in order to utilize the complete bandwidth of the diode, physical servers are recommended. Servers from DELL, HP and Lenovo are supported.

Certified Common Criteria EAL 5+

Option 1: Arbit Data Diode Devices

The solution consists of the following four items:

Item	Common name	Description	Function	Certification
Proxy Server	Pitcher Server	A transmitting proxy server	Transforms higher level protocols to UDP	
PD-162	Pitcher Device	A transmitting device without server	Handles two-way to one-way link	CC EAL 5+
CD-162	Catcher Device	A receiving device without server	Handles one-way to two-way link	CC EAL 5+
Proxy Server	Catcher Server	A receiving proxy server	Recreate higher level protocols from UDP	

The two Proxy Servers must fulfill these minimum requirements:

Feature	Requirement
CPU cores	4 or more cores (not counting hyper-threading)
CPU architecture	X86 64 bit
RAM	16 GB or more
Disk/RAID controller	Ubuntu Server 16.04 compatible
Disk space	<daily amount of traffic> times <days to store traffic for retransmission> times 2
Disk type	SSD mixed use RAID 10
Network interfaces	2 or more (if fiber is used, it must be 850 nm multimode fiber which is compatible with the fiber-versions of the Device)

Recommended server brands are Dell, HP and Lenovo.

Technical specifications of each Device (Pitcher Device PD-162 and Catcher Device CD-162):

Feature	Implementation
Diode principle	Common Criteria certified one-way component (PCB) with a single ROSA and a single TOSA. The light is passed through a single fiber to and from the CC component.
Back-flow	None
Diode transmission speed	690 mbit/s (more than 7 TB / 24 hours)
Network connectors	1x Diode interface: Simplex 1000Base-SX (LC) 1x Two-.way network interface: 1000Base-T (RJ45) or 1000Base-SX (SC)
Wave length	850 nm
Cooling type	Active
Cooling air flow	Front to back
Power supply	2x 100-240 VAC 50/60 Hz (Redundant power supply)
Power consumption	40 W
Dimensions (W x H x D)	19” x 1U x 340 mm
Weight	6 kg
Operating temperature	0 to 40ºC
Storage temperature	-10 to 70ºC
Humidity	90% RH
Regulatory conformance	CE, RoHS, WEEE

Option 2: Arbit Data Diode Units

The solution consists of the following four items:

Item	Common name	Description	Function	Certification
Proxy Server	Pitcher Server	A transmitting proxy server	Handles transmission of data	
PU-162	Pitcher Unit	A transmitting device including server	Handles proxy and two-way to one-way link	CC EAL 5+
CU-162	Catcher Unit	A receiving device including server	Handles proxy and one-way to two-way link	CC EAL 5+
Proxy Server	Catcher Server	A receiving proxy server	Handles reception of data	

The two Proxy Servers must fulfill these minimum requirements:

Feature	Requirement
CPU cores	4 or more cores (not counting hyper-threading)
CPU architecture	X86 64 bit
RAM	16 GB or more
Disk/RAID controller	Ubuntu Server 16.04 compatible
Disk space	<daily amount of traffic> times <days to store traffic for retransmission> times 2
Disk type	SSD mixed use RAID 10
Network interfaces	2 or more (if fiber is used, it must be 850 nm multimode fiber which is compatible with the fiber-versions of the Device)
Can be virtual	Yes, both

Recommended server brands are Dell, HP and Lenovo.

Technical specifications of each Unit (Pitcher Unit PU-162 and Catcher Unit CU-162):

Feature	Implementation
Diode principle	Common Criteria certified one-way component (PCB) with a single ROSA and a single TOSA. The light is passed through a single fiber to and from the CC component.
Back-flow	None
Diode transmission speed	690 mbit/s (more than 7 TB / 24 hours)
Network connectors	1x Diode interface: Simplex 1000Base-SX (LC) 1x Two-.way network interface: 1000Base-T (RJ45) or 1000Base-SX (SC)
Wave length	850 nm
Server type	Xeon CPU, 16 GB RAM
Server storage	Boots from CD-ROM or HDD: 2x 750 GB HDD(RAID1)
Cooling type	Active
Cooling air flow	Front to back
Power supply	2x 100-240 VAC 50/60 Hz (Redundant power supply)
Dimensions (W x H x D)	19” x 1U x 500 mm
Weight	9 kg
KVM connectors	1x VGA, 2x USB (2.0)
Operating temperature	0 to 40ºC
Storage temperature	-10 to 70ºC
Humidity	90% RH
Regulatory conformance	CE, RoHS, WEEE

Software

No matter which hardware solution is selected, the software is always the same.

The following main software products are installed on both pitcher and catcher:

Diode software	Arbit Data Diode software
OS	Debian Linux (Ubuntu Server 64-bit v16.04)
Mail-server (notification mails)	Postfix
Web-server (web interface)	Apache HTTP Server
Terminal access	OpenSSH Server
Open system	Yes (may be inspected and customized by customer)

The license includes both pitcher and catcher software. The license to use the software is not time limited.

Native forwarding services	FTP server, FTP client, SFTP server, SFTP client, SMTP, NTP, SMB, HTTPS, HTTP
Extendable with new services	Yes (provided by Arbit Security or developed by the customer)
Transaction control	Yes
Status and error notification	Yes (using email on the closed network catcher side)
Retransmission of failed transactions	Yes (using web interface on pitcher)
MTBF	< 3,75 *10^{-10} packets
Software limit on maximum file size	None (only limited by free disk space on catcher)
Configurable length of retransmission archive on pitcher	Yes (only limited by free disk space on pitcher)
Monitoring of free disk space	Yes (on pitcher and catcher)
Data traffic amount	Unlimited
Traffic overload protection	Back pressure and safe points on pitcher
Data channel priority	Yes (transaction based)
Remote status	Yes (using web interface on pitcher and catcher)
Streaming	Generic UDP/TCP streaming (video, audio etc.)
Regular maintenance	None (the system runs unattended)

Network

The pitcher offers the following network services on the lower classified net:

HTTPS	443	Manual retransmission is controlled through secure web access
HTTP	80	
FTP	21	Restricted FTP access for one or more users / computers
MAIL	25	Restricted MAIL access for one or more users / computers
SSH/SFTP	22	Secure Shell administration access and SFTP

All services are optional.

The catcher offers the following network services on the higher classified net:

HTTPS	443	Transaction status is gained through secure web access
SSH	22	Secure Shell administration access

All services are optional.

Data Integrity

The Arbit Data Diode utilizes several layers of data integrity:

1) The transport is based on UDP which includes a checksum ensuring that the individual packages are not corrupted.

2) On top of the UDP transport the data diode maintains strict transaction control which is able to detect any lost packages and which ensures that all packages are processed in the correct order. The strength of this transport control is equal to regular TCP/IP communication.

3) Finally the data diode uses a forward error correction algorithm which prevents almost all network transmission errors.

4) A retransmit cache on the pitcher ensures that any transmission errors due to hardware or power failures can be retransmitted manually.