Arbit Data Diode

Whitepaper

Release 2021-10-27

Arbit technical reference:
Rasmus Borch
rb@arbitcds.com

Concept

The Arbit Data Diode solutions consist of two enclosures (called Pitcher and Catcher respectively) connected by a single fiber-optic cable. The Pitcher connects to the sending network and the Catcher connects to the receiving network.

The unidirectional communication is Common Criteria certified by BSI (see below) to EAL 7+.

The Arbit Data Diode is designed to function in three different configurations:

<table>
<tr><th>Configuration</th><th>Feature</th></tr>
<tr><td>Stateless</td><td>The Pitcher and Catcher work as simple UDP-forwarding devices and offer no further functionality.</td></tr>
<tr><td>Stateful</td><td>The Pitcher and Catcher offer the following protocols for transporting data:
<table>
<tr><th>Protocol</th><th>Can be used for (not a complete list)</th></tr>
<tr><td>UDP</td><td>Video/audio streaming, SPLUNK integration, syslog</td></tr>
<tr><td>TCP</td><td>System integration using TCP (one way)</td></tr>
<tr><td>NTP</td><td>Time synchronization</td></tr>
</table></td></tr>
<tr><td>Stateful with proxy servers</td><td>The same as Stateful, but supported by at least two proxy servers (one on each side) which adds support for the following additional protocols:
<table>
<tr><th>Protocol</th><th>Can be used for (not a complete list)</th></tr>
<tr><td>SMTP</td><td>Mail transfer</td></tr>
<tr><td>FTP</td><td>File transfer, Centos/Ubuntu offline repository, WSUS</td></tr>
<tr><td>SFTP</td><td>File transfer, Centos/Ubuntu offline repository, WSUS</td></tr>
<tr><td>SMB Move</td><td>File transfer</td></tr>
<tr><td>SMB Copy</td><td>File mirroring, WSUS</td></tr>
<tr><td>NFS Move</td><td>File transfer</td></tr>
<tr><td>NFS Copy</td><td>File mirroring</td></tr>
<tr><td>HTTP/HTTPS</td><td>NiFi, REST API forwarding</td></tr>
<tr><td>OPSWAT Vault</td><td>OPSWAT Kiosk-to-Vault and Vault-to-Vault</td></tr>
</table>
Additionally, it provides the possibility to verify all file-based traffic by applying filters like OPSWAT MetaDefender.
Please refer to the section “Proxy Servers” for minimum requirements and recommendations.</td></tr>
</table>

Technical specifications (describes a single physical unit corresponding to either one PITCHER or one CATCHER; two units are required for one Arbit Data Diode).

The Arbit Data Diode is available in two form factors:

- Industrial network appliance (10 GbE)
- Ruggedized network appliance (1 GbE)

Industrial:
Two hardware units are required for creating one diode: 1 Pitcher Unit and 1 Catcher Unit. The following specifications describe one unit (same specs for Pitcher and Catcher).

Specification	**Value**
Diode principle	Hardware based (optical)
Backflow	None (secured by the laws of physics)
Certification	Common Criteria EAL 7+
Certifying body	Bundesamt für Sicherheit in der Informationstechnik (BSI), Germany
NICs	2x 10GBASE-T; 2x 10GBASE-LR (LC); 1x 1000BASE-T IPMI; 1x diode 10 GbE diode single LC
Fiber technology	Single mode 1310 nm
Diode NIC speed	10 Gigabit
Embedded server	Intel XEON, 128 GB RAM
Boot media	Custom read-only SSD disk
Configuration	Smartcard based
Front panel	On/off switch, Boot media tray, Smartcard slot, LED indicators: Power status, PSU1, PSU2, Alarm, Status, Disk activity
Back panel	All network connectors, VGA, USB, Power 1, Power 2, LED indicators: LINK/Activity for each NIC
Configurator	Arbit Configurator (configures smartcards and read-only boot media)
IPMI	Yes
IPMI Interface	1000BASE-T
Server storage	Diskless system (runs directly from a custom configured read-only boot media generated by Arbit Configurator)
Cooling type	Active
Cooling air flow	Front to back
Server size	1x 1U, 19”/2 (two units required for a complete diode: 1 pitcher and 1 catcher)
Weight	6 kg
KVM connectors	1x VGA, 1x USB (2.0)
Operating temperature	0 to 40ºC
Storage temperature	-10 to 70ºC
Humidity	90% RH
Regulatory conformance	CE, RoHS, WEEE
Power supply	2x 100-240 VAC 50/60 Hz (Redundant power supply)
Dimensions (W x H x D)	19”/2 x 1U x 800 mm

Ruggedized:
Please refer to separate product information document.

Proxy Servers

In case the configuration “Stateful with proxy servers” is selected, the servers must fulfill the following minimum requirements:

Feature	**Minimum requirement**
CPU	4 (not counting hyper-threading)
CPU architecture	x86 64 bit (AMD or Intel)

RAM	32 GB
Disk type	SSD Mixed Use
Disk configuration	RAID10
RAID controller	Linux OS compatible
Disk space	*<daily amount of traffic>* multiplied by *<days to store traffic for retransmission>* multiplied by 2
Network interfaces	2 (one of which must be either: 1000BASE-T, 10GBASE-T or 10GBASE-LR)

Recommended server brands are Dell, HPE and Lenovo. The servers can be virtualized.

Software

The Arbit Data Diode software has the following features:

Feature	**Value**
Network speed	1 GbE or 10 GbE (determined by license and hardware)
Supported protocols	Depends on configuration. Please refer to section "Concept".
Custom protocols/services	Yes, either developed by Arbit, end customer or third party.
Transmission error detection	Yes
Automatic error correction	Yes, on all services except raw UDP steaming.
MTBF	< 3,75 *10-10 packets
Maximum file size	Half free disk space on proxy server (or 2^{64}-1 bytes)
Management interface	Web interface
Retransmission of failed transmissions	Manual by web-interface on Pitcher
Traffic overload protection	Back pressure and safe points on Pitcher
Data channels	64
Data channel priority	Yes, transaction based
Regular maintenance	None (the system runs unattended)
Operating System (Pitcher/Catcher)	Custom Linux
Operating System (proxy servers)	Red Hat 7 or Red Hat 8 (alternatively Ubuntu Server 18.04)
Firewall (Pitcher/Catcher)	FirewallD using the "public" zone
Firewall (proxy servers)	FirewallD using the "public" zone (only on Red Hat)

Filtering

The Arbit Data Diode software running on the proxy servers on the Catcher side supports filtering. Each file-based data channel (not streaming channels) can be configured to have zero or more external filters.

These filters are presented each file which is passing through the specified data channel. Each filter can reject files, which forces the diode software to deliver it to a different target system than originally specified for the data channel. All defined filters must accept a file for it to be delivered to the originally specified target system.

Data Integrity

The Arbit Data Diode utilizes several layers of data integrity:

1. The unidirectional 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 packets, which ensures that all packages are processed in the correct order.

3. When transporting files and supporting TCP-like streams, the data diode uses a forward error correction algorithm which prevents almost all network transmission errors.

4. All files are verified by checksum after arrival on the Catcher.

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