Arbit TRUST Gateway

Whitepaper

Release 2019-05-20

Arbit technical reference:
Rasmus Borch
rasmus.borch@arbit.dk

Hardware

The Arbit TRUST Gateway (ATG) is a more advanced type of data diode with release capability. It is able to verify data requested to pass through originates from an approved source system using digital signing technology.

The ATG is based on three separated networks connected by data diodes. The data diodes ensures that data is only able to be transmitted in one direction. This is done by using a single fiber optic cable to transmit the data with no return flow possible[1].

The two data diodes creates an isolated network with no interactive access from neither the sending nor the receiving net. This isolated network (called the VOID net) handles the verification of the data that is requested to pass through the ATG. Each approved source system allowed to transmit data through the ATG will sign the data to be released. The ATG then checks the signature on the VOID net. If the signature is correct the data may optionally be required to be released manually by a releasing officer before passing through. Otherwise the event is logged and possible counter measures may take effect.

The basic platform of the ATG consist of four units:

High Guard	(1U enclosure; Sending net)
VOID Proxy	(1U enclosure; VOID net)
VOID Guard	(1U enclosure; VOID net)
Low Proxy	(1U enclosure; Receiving net)

Technical specifications (complete platform)

Diode principle	Hardware based (one-way laser light)
Backflow	None (secured by the laws of physics)
Diode NIC	4x
Single fiber	2x
Diode NIC speed	Gigabit
Server type	4x Embedded computers (quad-core)
Server storage	Disk-less system (runs directly from 4 custom configured CDs created at the operation site)
Power supply	8x (universal; redundant power supplies for all units)
Server size	4x 1U
Weight	4x 15 kg
Network connectors	4x RJ45 (gigabit; 1x sending network; 2x VOID net; 1x receiving network)

Technical specifications (each unit: High Guard, VOID Proxy, VOID Guard, LOW Proxy)

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

Please refer to the Arbit Data Diode whitepaper for more information on the design of Arbit Data Diode technology.

Software

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

ATG software	Arbit TRUST Gateway software
OS	Debian Linux (minimal Ubuntu Server 64-bit v14.04)
Terminal access	OpenSSH Server (optional)
Open system	Yes (may be inspected and customized by customer)

Arbit TRUST Gateway software

The license includes the following software features:

Manual release from VOID net terminal	Yes (optional; otherwise automatic)
Automatic release (no manual check)	Yes (optional; otherwise manual)
Signature check of all data	Yes
Complete transaction log (including free-text search)	Yes (add-on)
External content verifiers	Yes (add-on; file type identification/filter provided by Arbit)
External content verifiers created by customer	Yes (uses open API)
Latency	<1 sec for transactions up to 10 MiB
Max transaction size	12 GB
Source system integration	Open Java API
Configuration and key generation	Stand-alone laptop
Running configuration changeable	No (new runnable CDs must be created on site)
Multiple approved source systems possible	Yes
Regular maintenance	None (the system runs unattended)

Data Integrity

The ATG 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.

3) Finally the ATG uses a redundancy algorithm which prevents almost all network transmission errors.