Development of unidirectional data diode system in the secure environment

A. G. Vorontsov
Information Technology
FSUE VNIIA
Moscow, Russia
voroncov-ag@narod.ru

S. A. Petunin
Information Technology
FSUE VNIIA
Moscow, Russia
S.A.Petunin@gmail.com

The paper describes features of the development of unidirectional network (DataDiode devices) in the secure environment (the development of the unidirectional data transfer from the wide area network (WAN) to the secured enterprise network). A brief overview of the existing devices is given and their characteristics are described. The method to address limitation issues, such as lack of feedback channel related to the implementation and integration of one-way channel is described.

The main part of the research is focused on enhancing accessing process to the restricted network. The model of the unidirectional data transfer system, including DataDiode device, has been introduced.

The paper reflects:

- *General principles of unidirectional data transfer;*
- *Topological features of the unidirectional data transfer model;*
- *Interaction with information security system;*
- *Providing load balancing and interactivity under high-load conditions.*

Keywords: data diode; unidirectional; security; highload; fiber; one-way gateway

I. INTRODUCTION

A unidirectional gateway is a network appliance allowing data to be transferred only in one direction [1]. It doesn't allow data to pass in the opposite direction and connects different segments of the network with various privacy levels of the data processing and storage [2]. In the subject area under consideration, such one-way network solution must ensure no data transmission capacity in the opposite direction at the hardware level to preclude reconfiguration of security policy or firewall rules.

The class of such devices that provides isolation of network segments to prevent unauthorized access to the network information assets is referred to as Data Diode. Thus, it ensures the required data input to the closed network, and at the same time, it prevents unauthorized outputting of restricted information or any other external accessing to the closed network [3].

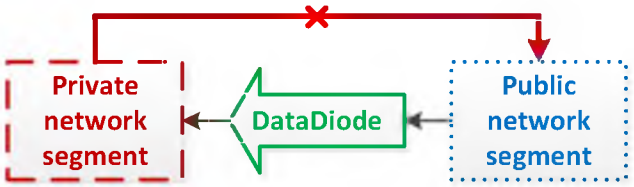
Currently, the Data Diode devices may be topologically different unidirectional data gateway. Some types of such systems are discussed below.

We introduce the notion of a private network segment and public network segment. The private network segment is a protected automated network system. The public network is an unsecured wide area network.

Schematic [4] of the unidirectional data gateway is shown in Fig. 1.

Figure 1. Data transmission to the downstream network

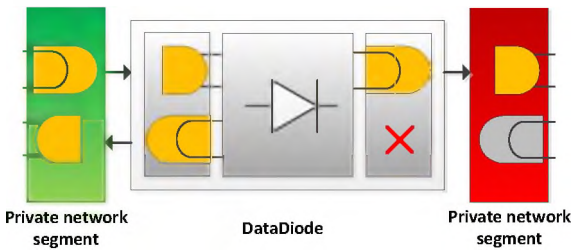
This Data Diode system is based on physically isolated fiber-optic communication and data feedback principle (no



network autonegotiation). The functional diagram of the system kernel is shown in Fig. 2, which demonstrates the absence of a data feedback.

Figure 2. Functional diagram of transmitting system kernel

The devices based on the given functional diagrams have a



number of advantages and disadvantages. Using Data Diodes allows resolving the problem of open data input to the downstream network, and implementing asynchronous management (without data feedback) of services within downstream network by means of control commands sent from the public network segment. It allows moving away from the previously used input methods (e.g. specialized input points where all the data is controlled by an operator) and to partially automating data input process.

However, the absence of data feedback brings forth a number of possible technical challenges. Implementation of the unidirectional channel causes the problem of transferred data verification which in the most cases is critical for data integrity:

- TCP/IP protocol requires handshaking;
- Data feedback is required for determination and adjustment of the communication rate;
- It is impossible to run application software since it requires a data feedback or data received acknowledgement.
- Most of web-services are not functional.

There are different approaches to resolve such problems [5]. For instance, the USA patent No. 5703562 Method for transferring data from an unsecured computer to a secured computer proposes a verification mechanism that uses a warning device coupled to a secured computer and emits a warning signal if an error was introduced during data transmission. The patent suggests using a single long duration tone [6]. It is obvious that the suggestion doesn't allow transmitting the checksum calculations from a Send Node to a Receive Node to allow the latter match the results, and thus define received data integrity.

Also, there are simplified approaches that deploy commercially-available hardware devices for establishment of a topologically adjusted network, configured only to one-way data transmission. However, these methods and approaches don't provide the sufficient protection level and it doesn't protect from attacks aimed to reverse data channel flow.

Out of the existing and functional devices, the most interesting configurations are built on the basis of the diagram shown in Fig. 2.

A. Unidirectional gateways with two module and repository

It consists of two components – the transmitter of the public network and the receiver of the private network coupled without any real data feedback. Every module contains an SSD drive with XFS file system. Both components are controlled by OS Linux special build.

The following operation algorithm is used [7]:

1. The public network data flows to the receiver, and then is written to an SSD drive.
2. As data transmission to the receiver is over, the data is synchronized with the private network receiver's SSD drive via UDP protocol that doesn't require acknowledgement, thus partially eliminates the necessity of data feedback. During synchronization process, the transmitted data is splitting into data packets, where each packet entered the checksum.
3. The data stored on the receiver, becomes available to a recipient, while the data on the public network SSD drive receiver is automatically deleted after synchronization is over.

Schematic diagram of two-module unidirectional gateways is shown in Fig. 3.

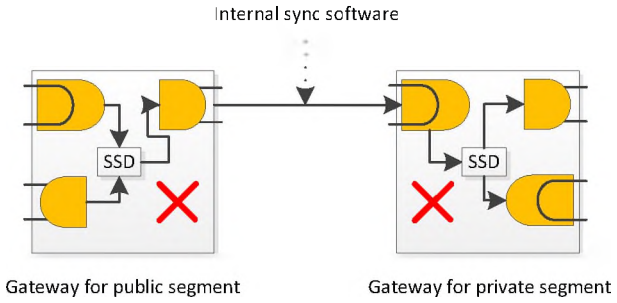


Figure 3. Functional diagram for two-module unidirectional gateways

Such implementation allows for one-way data transfer without data feedback required to confirm the integrity of the transmitted data and dynamic bandwidth adjustment of transfer rate. The data integrity is confirmed by the internal software. As the channel bandwidth and specification for the transmitter and the receiver is beforehand known, this provides an opportunity to determine synchronization speed in advance between SSDs drives.

The transmission speed has a great relevance because if the asynchronous behavior occurs, the receiver would not be able to keep up handling the input data stream, and the sender (the upstream network transmitter) would not know about it. This situation may lead to transmission failure.

The implementation disadvantages:

- XFS file system instability;
- Poor performance (about 30 Mb/s)
- The limited number of users is supported (100 users in total, 20 active users)
- The volume of SSD drives within the system is limited.

The most important measures of the device performance entered as the parameters listed in Table 1.

TABLE I. DATA TRANSFER RESULTS

Quantity*volume / Measures	1x8000 Mb	3x8000 Mb	1030x7 Mb	3030x10 Mb
Average send speed, Mb/s	20	20	15	14
Average sync speed, Mb/s	30	30	25	25
Average receive speed, Mb/s	25	25	23	22
Average transmit time, min	18	53	20	82
Average number of transmission errors	0	0	15	43
Average number of sync errors	0	0	20	1315
Number of transmissions	5	5	5	5

B. End-to-end unidirectional gateway with one module

Unlike the previously two-module architecture, it is a single device. It is also a transmission device based on the same principles as the two-module unidirectional gateways but it doesn't have any internal storage and embedded software to perform data synchronization.

Operating principle is also build on the transmitting system kernel as the two-module device, though it has its specific differences [8]:

- Absence of the internal storage;
- Supports large number of active users (511);
- High performance (up to 90 Mb/sec).

Since there is no need to store the data within the device and no sync role – the given architecture is more fault tolerant and much better to implement. The software which responsible for data receiving and transmitting is located within the device on separate servers. The diagram of the device is shown in Fig. 4.

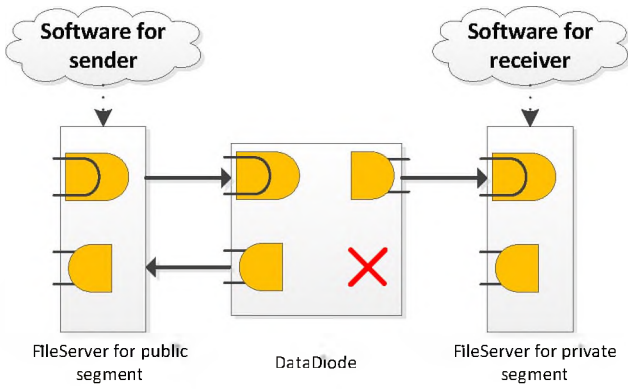


Figure 4. Scheme of the end-to-end unidirectional gateway

The most important measures of the device performance entered as the parameters listed in Table 2.

TABLE II. DATA TRANSFER RESULTS

Quantity * volume / Measures	1x8000 Mb	3x8000 Mb	1030x 7 Mb	3030x 10 Mb
Average send speed, Mb/s	87	92	52	50
Average receive speed, Mb/s	87	92	52	50
Average transmit time, min	95	265	140	610
Average number of sync errors	0	0	7	0
Average number of redundancy data packets	1	1	1	2
Number of transmissions	5	5	5	5

II. UNIDIRECTIONALDATA TRANSFERSYSTEM REQUIREMENTS

Necessity of development methods and a number of means to implement the automated unidirectional network ensure:

- guaranteed unidirectional data transfer;
- absence of transmitted data loss;
- communication channel performance (no less than one Gb/s);
- dynamic load balancing between output points from the public network;
- dynamic load balancing between input point to the private network;
- compatibility with information protection software;
- private network topology hiding;
- integration with network domain structure.

The proposed methods and means are automated, integrated with public and private network and has centralized management. The necessary condition to be able to interact with private network is the appropriate certification of Data Diode device.

III. SYSTEM MODEL

To develop the system model, it is necessary to define the objects.

Objects of the public network:

- A transmitting file server;
- Domain controller;
- User workstations.

Objects of the private network:

- A receiving file server;
- General file server;
- Domain controller;
- Network firewall;
- Data Diode;
- User workstations.

The proposed model implements network firewall in compliance with different network classes interaction requirements.

The functional diagram is shown in Fig. 5.

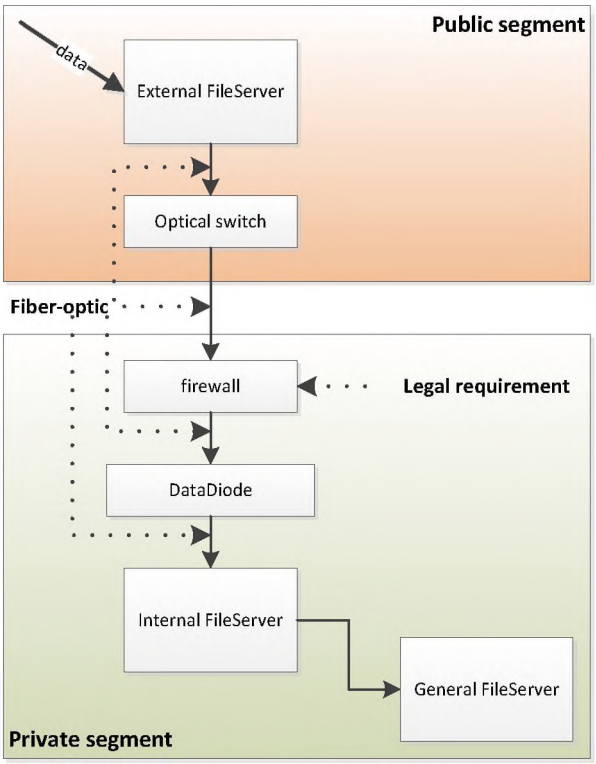


Figure 5. Example of a figure caption. *(figure caption)*

IV. STRUCTURAL IMPLEMENTATION METHODS

Architecture of the proposed solution is shownabove. Besides customizing of communication equipment and sync software for the transmitting and receiving file servers, a number of problems need to be solved, such as:

- The incoming file queue problem;
- Overload of the devices that may become a reason of out of sync behavior;
- Interaction with information security system;
- Load balance;
- Interactive management and automation of the research system.

The problem of the incoming file queue is the selection of file processing priority. Before transmitting the current file in queue, the analysis of the whole ready-to-transmit queue is required, arranged by the file size, for example. Then, it is necessary to rebuild transmitting queue. This action solves such problems as large packet transmission and concentration of a great number of small-sized files in file queue. A queue manager is implemented into the proposed model. If the large-sized file is being in the transmitting process while the system has only one unidirectional channel, it is necessary to wait until the file transfer is over. To resolve this problem file queue manager should compress large-sized files into equally sized archive volumes as part of the file transfer preparation procedure. It will enhance opportunities for queue management.

As it was mentioned above, absence of data feedback and transmission error that may occur due to asynchronous behavior of data transfer speed has two potential options:

- Application of sync software;
- Application of additional control facility for received files.

For the purpose of reduction such risk it is necessary to have identical technical characteristics for transmitting and receiving servers, and also contain high-performance disk subsystems, which preferably should be based on SSD drives.

The above mentioned method for file integrity check (uses application responsible for data transfer) needs optimization. While using this method, a possible problem may occur when it comes to huge number of files transfer that becomes more complicated regarding to inability to know the size, quantity and list of transmitted files due to a lack of data feedback.

The additional check method involves full data compressing and creation of archive volumes. It guarantees visual check for complete transfer of every archive file. If error occurs, the archive would not be upload to the receiving file server, thus a user would have to retransmit the archive volume.

Interaction with information protection system when end-to-end unidirectional gateway is used becomes a trivial task, aimed to ensure integration of transmitting and receiving file servers into the existing systems [9]. The main task is to provide error-free interaction with synchronizing software without any delay of network protocol or files reading and writing operations.

In case of using one unidirectional gateway device load balance is applied if exceeding or insufficient computational resources. To resolve such problem the scaling method is applied. It involves increasing the number of transmitting and receiving file servers and unidirectional channels. It is also necessary to apply balancing gateway that redirects the user to one of the receiving servers of the public network [10]. This architecture is shown in Fig. 6.

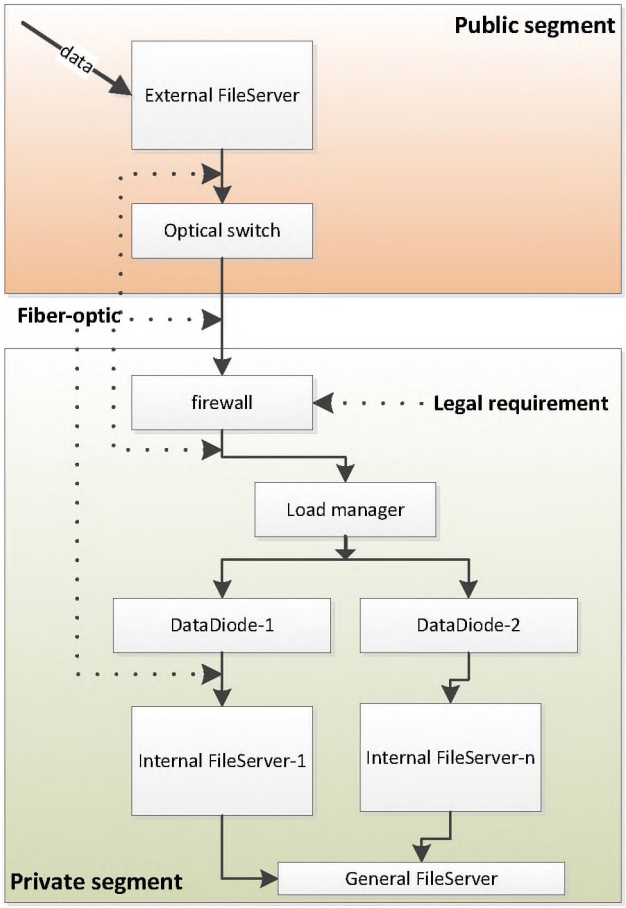


Figure 6. Example of a figure caption. *(figure caption)*

Development of a general control structure to ensure interactive control of the system is also required.

It provides:

- Addition of new network users;
- Automated control for transferred and received files that include archiving, transmission preparation, priority queuing, receiving files allocation.

The structure functions in cooperation with synchronizing software of the unidirectional gateway within public and private network. The conditions of no data feedback are observed.

Work algorithm of control structure and internal synchronization software within public network is shown in Fig. 7.

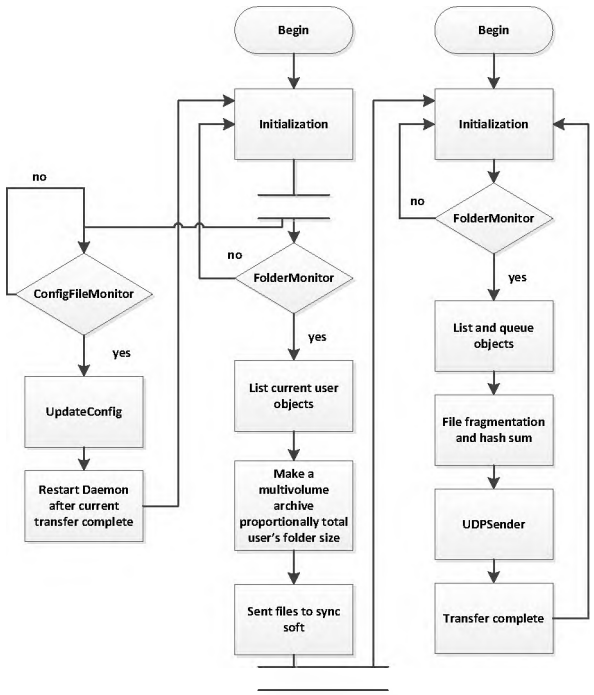


Figure 7. Sync software and control structure of the upstream network flowchart

Work algorithm of receiving data within private network is shown in Fig. 8.

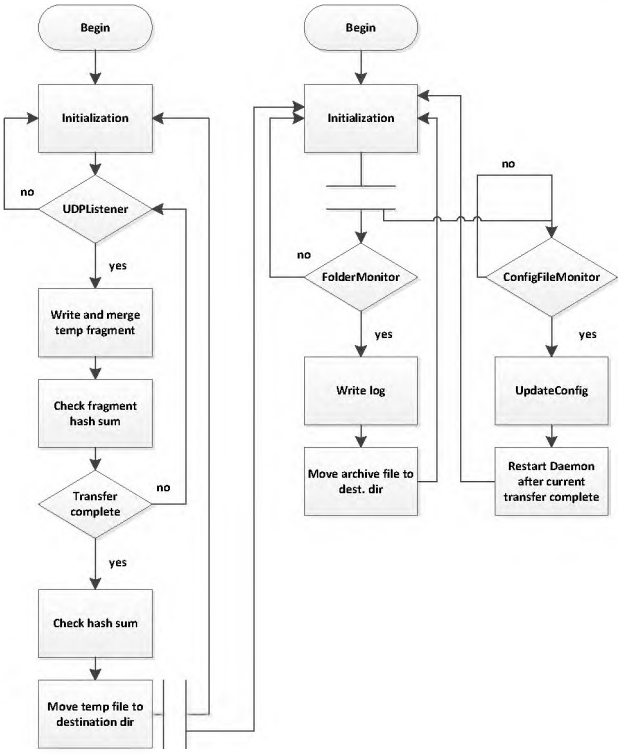


Figure 8. Sync software and control structure of the private network flowchart

V. CONCLUSION

This paper introduces and describes the development of hardware and software solutions for unidirectional gateway implementation in the conditions of secured environment. The actual implementation provided a unidirectional data flow from Wide Area Network to Local Area Network under the given conditions.

A primary result of this paper is theoretical development and implementation of unidirectional network system integrated into corporative network ensuring interaction with security systems. The developed control structure permits to scale the system considering basic load factors such as transmitted data volume and the number of users in system.

REFERENCES

[1] Unidirectionalnetwork: https://en.wikipedia.org/wiki/Unidirectional_network

[2] Australian Government Information Management Office 2003, Securing systems with Starlight, Department of Finance and Administration http://www.agimo.gov.au/archive/publications_noie/2003/06/transform/defence.html

[3] "CanSec" company – "What is unidirectional gateway": http://cansec.ru/21/unidirectional-gateway.html

[4] AMT Group – "InfoDiode - Unidirectional gateway system": http://www.amt.ru/rubr.aspx?rubr_id=237&art_id=1154

[5] Douglas W. Jones and Tom C. Bowersox "Secure Data Export and Auditing using Data Diodes" // 2006 USENIX/ACCURATE Electronic Voting Technology Workshop, 1 August 2006, Vancouver, https://www.usenix.org/legacy/events/evt06/tech/full_papers/jones/jones_html/

[6] OKB SAPR – "Organization of a unidirectional data transmission channel on the basis of a protected service information carrier": http://www.okbsapr.ru/lydin_tezisy2013_1.html

[7] "CanSec" company – "Integrated file and mail unidirectional gateway Strom-File": http://cansec.ru/products/strom_file.html

[8] "CanSec" company – "High speed unidirectional gateway Strom-1000": http://cansec.ru/products/strom-1000.html

[9] Vorontsov A. G., Petunin S. A., Konyshev A. V. "Empowering information security systems in the conditions of domain environment" // Workshop on computer science and information technologies CSIT'2015, Rome, Italy, 2015.

[10] Somerdata – "AROW Data Diode": http://somerdata.com/?page_id=176