Excellence in Digital Security.

genua.

Data Diode vs-diode

High-Performance One-Way Interface Solution
Approved for Black-Red Transitions

Technical Information

Table of Contents

1. Summary

vs-diode is a device for securing classified information and is a result of the continued development of genua's proven genugate data diode. This high security system transfers data in only one direction – from black to red networks – and is more comfortable and quicker to use than a so-called air-gap – manual transfer to a more secure network using storage media.

The secure data transfer and receipt confirmation provided by vs-diode means that is also more reliable than a glass fiber diode. Components within vs-diode run on physically separated hardware and are operationally separated by an L4 microkernel, meaning that the system provides considerably more security than a firewall. vs-diode is based on the highly-secure genugate firewall and is approved for the classification levels German SECRET ("GEHEIM"), UE SECRET/SECRET EU, and NATO SECRET by the German Federal Office for Information Security.

This brochure describes the vs-diode solution, its functions and fields of application.

2. vs-diode: Reliable Unidirectional Data Transfer across Red-Black Transitions

This brochure is intended for persons and institutions who work with information of different classification levels such as "Secret" or "Restricted" and who are responsible for security measures to protect this information.

It provides a compact overview of how the vs-diode can be used to allow secure and regulated unidirectional data transfer from black, unclassified or restricted networks into red, higher classified ones.

2.1. Challenge

Many networks require access to up-to-date data, which they obtain from other networks. While this exchange of data does not generally pose a problem, the direct physical coupling of networks with different security classification levels is unacceptable.

In this case, data transfer to an area with a higher classification level is therefore usually carried out manually, i.e. through the use of portable storage media such as DVD-ROMs or USB sticks. The information is first copied from the lower classified data source onto the portable medium, before then being copied from the medium to the higher classified network. Data transfer in the opposite direction is avoided through appropriate instruction of the staff responsible.

The difficulties with this method are that real-time transfers cannot take place, and that the use of portable data carriers for confidential information poses a serious security risk.

A better solution for the permanent coupling of differently classified networks is provided by the fully or partly automatic high security gateways described in the next section.

2.2. Solutions: Types of High Security Gateways

Packet diodes, red-black gateways, and data diodes all follow different approaches to solving this problem.

2.2.1. Packet Diodes

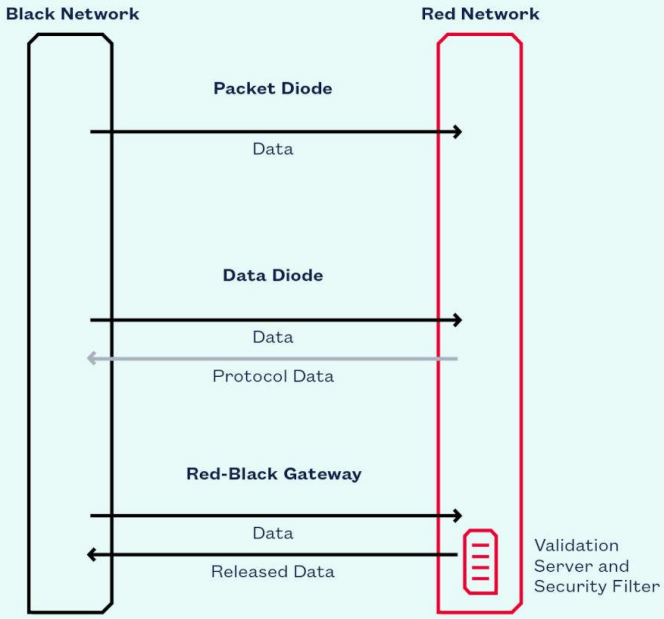
Packet diodes can only transfer IP packets in one direction – from black to red – and are prohibited from transferring in the reverse direction. This prevents all leakage of classified information. Packet diodes are often implemented using a fiber optics connection, in which the fiber for the return channel is not connected. Communication across this type of connection is exclusively via the user datagram protocol (UDP).

The use of this protocol has the disadvantage that reception of a packet is not verifiable, even when transmission is repeated. Data might not be received in full and may therefore be unusable. In addition, packets sent per UDP may not necessarily be received in the order in which they were sent, and may be received more than once. This, in turn, means that applications using UDP either have to be insensitive to lost and unsorted packets, or have to be equipped with suitable correction features. Transfers of larger quantities of continuous data are almost impossible, as confirmation of individual packet reception cannot be returned and therefore the sender never knows whether the data has been fully received.

2.2.2. Red-Black Gateways

A red-black gateway allows inspection and regulation of data flow content between differently classified networks in both directions – from black to red and from red to black. A range of security components is used to achieve this: one method being a two-stage procedure using a validation server and a security filter. Here, content control can be carried out both automatically and manually.

Automatic procedures are carried out by a parser, checking data whose contents are embedded in a strictly defined format. However, files containing arbitrary text or graphics are manually checked using a viewer. If no confidential information is detected, the data will be digitally signed before release for transfer to the black network. The validation server will then check the validity of the signature and associated owner certificate. Unlike the packet and data diode approaches, this solution also transfers exactly defined “black” information from the red to the black network.



Overview: Packet diode, data diode, and red-black gateway

2.2.3. Data Diodes

Data diodes use the Transmission Control Protocol (TCP) and allow data transfer from black to red networks. However, the protocol requires that packet exchanges take place in both directions simultaneously. The TCP control packets ensure secure and regulated data transfer – in contrast to the packet diode approach – and transmission errors and lost or duplicate packets are avoided.

However, all return packets other than those carrying protocol data essential for communication must be “normalized” at the network border – they must not contain any hidden information. This approach aims to ensure both the highest possible levels of data security and file transfer reliability. The key feature of a data diode is the achievement of these two requirements.

3. Security of Classified Information

3.1. Classified Information Requirements and Red-Black Coupling

The instructions for handling classified material issued by the German Federal Ministry of the Interior basically require that the confidentiality, availability and integrity of such data is guaranteed. This means that particular scrutiny has to be given to the security-related issues resulting from the coupling of different security do-

mains in organizations handling this type of material. Suitable precautions are to be implemented at the transitions between domains.

3.2. Confidentiality Presents Special System Challenges

As already mentioned, a return stream of log data is necessary if the interface solution is to allow any regulated transfer of data into a red network per TCP. In this situation, a suitable system architecture is required to counter the security risk presented by bi-directional communication.

This means that particular requirements must be met by the interface solutions between differently classified networks: on the one hand, possibly malicious programs must be prevented from entering the red network from a less secure black network, and on the other hand stop any data transfer from high security networks to low security ones.

4. Detailed Requirements

In the following section we describe the fundamental requirements that a data diode has to fulfill at a red-black transition in more detail.

4.1. Fuctional Requirements

4.1.1. Data Transfer from the Black to the Red Network

Data communication between two devices in different networks requires an IP-based system that can carry out secure data transfers.

4.1.2. Reliability

A suitable data transfer protocol should be used to prevent data loss. A status signal indicating success or failure of data transfer is necessary.

4.1.3. High Data Transfer Rates

The system performance requirements may increase, depending on the intended use and utilization level: Transfer speeds (line speed) of several Gbit/s and the processing of large data quantities in a bulk transfer should be possible.

4.1.4. Automatic Operation

Operator intervention should not be necessary during normal operation. Data transfer will take place via the standard protocols: SMTP (mail), FTP (file transfer) and TCP stream or UDP datagram.

4.2. Security Requirements

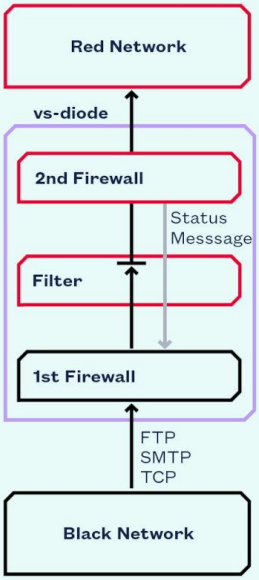
Information transfer from the red to the black network must be prevented. In addition, the system has to enable SMTP filtering for viruses and malware and provisions should be made for protection against covert channel attacks.

5. The Solution: vs-diode

genua has used this list of requirements to develop a complete high security system based on the highly-secure genugate firewall and the L4 microkernel. vs-diode is a three-stage system consisting of a packet filter positioned between two Application Level Gateways.

5.1. Architecture with Three Separate Filter Systems

The vs-diode architecture is made up of three sub-systems arranged in series which data has to pass on its way through the diode: Application Level Gateway (ALG) – one-way filter – Application Level Gateway.

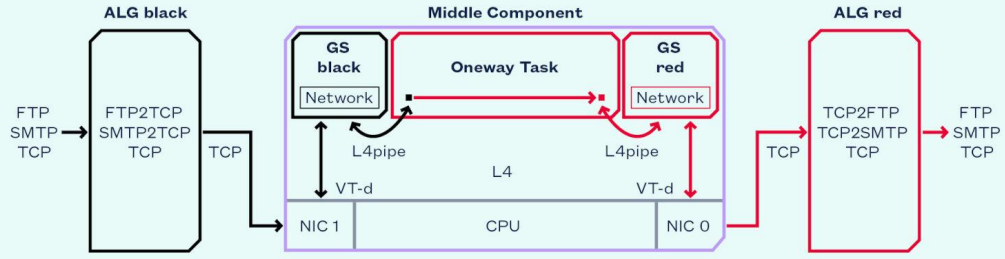


The vs-diode, consisting of a one-way filter and two firewalls

The three separate components that complete the vs-diode function together much like a canal lock – albeit a lock with two channels – a wide and a narrow one: data is received from the black network and transferred to the red network via a new connection. Only status information is allowed to pass in the opposite direction.

5.2. The vs-diode Components and Their Functions

Security of vs-diode is based on the principle of different technologies being applied one after the other. This can be seen in the hardware, which is made up of three parts, each with their own function.



Overview: The communication process

The following sections provide a more detailed insight into the workings of the individual components and processes of vs-diode, ordered in line with the diagram above.

5.2.1. The Application Level Gateways (ALGs)

Both ALGs are responsible for transforming complex Internet protocols into easy-to-check one-way data streams. These complex protocols currently include FTP, FTPS, SMTP, TCP, UDP as well as Syslog and Lumberjack. With vs-diode, for example, files and e-mails can be transferred and log entries can be aggregated in Elasticsearch. The data is accepted on the black side and delivered with the same protocol on the red side. The ALGs used are identical to those of the high resistance firewall genugate. Proven and highly secure technology for content and protocol analysis is used here.

Communication over the middle component of vs-diode (the one-way filter) uses TCP with connections only being able to be made from black to red. The data flow from the ALGs and from the one-way filter is restricted to a single direction. A feedback channel can be opened for each connection and an error signaled by a TCP protocol “reset packet”. A TCP reset packet is also sent when the recipient cannot accept the data.

5.2.2. The One-Way Filter

In order to avoid information being transferred from red to black in the TCP control packets, each connection is terminated, modified and then reopened in the one-way filter. As TCP is a complex protocol this procedure is further divided up in the one-way filter.

Using one of the L4 family of microkernels, the one-way-filter hardware is divided into three compartments – that is strictly separated areas. Each of these compart-

ments has its own function: receiving the TCP connection, examining the data flow and establishing a new TCP connection.

A genuscreen firewall system runs in each of the two compartments that handle the TCP. Although we trust this product, we have paravirtualised the kernel as an L4-Task and restricted it to its own CPU core and a part of the main memory. We use Intel's VT-d virtualization technology so that we can couple the network hardware to this compartment. The two black and red designated interfaces are so closely coupled to the corresponding red and black genuscreen interfaces that even errors in the firmware of the network cards or in the drivers would make breaking out of the compartments impossible.

5.2.3. The One-Way Task

There is a one-way task between the two genuscreens, which is also decoupled from the rest of the system by the L4 microkernel. The one-way task has the sole purpose of copying data from black to red and allowing a success message to be sent in the opposite direction. As this task is relatively simple, it is straightforward to keep a track of its implementation. This avoids errors in these critical components and means that loss or tampering with data is not possible at this level.

5.2.4. System Security

A look at the nested system structure inevitably brings up the question, “Which components are critical for security?” The three machines that make up vs-diode: ALG – one-way filter – ALG are connected in series and designed so that the data payload only flows in one direction. The three compartments which the middle machine in the vs-diode is divided into: genuscreen – one-way task – genuscreen, all perform a security function as well. Only the one-way task and the L4 separation have to remain uncompromised to ensure secure functioning of the diode.

With only some 1,300 lines of code, the one-way-task is very manageable. With less than 100,000 lines, the L4 microkernel is considerably larger but also manageable, particularly when compared with the usual operating systems with several millions of lines of code. This is partly due to the hardware drivers and network stack being encapsulated in the genuscreen compartments and no longer belonging to the trusted code base.

The L4 microkernel and the one-way task would prohibit an insider from transferring data via the diode from red to black, even in the unlikely event of the genugate ALG, the genuscreen kernel or the network card firmware being compromised.

5.2.5. Native Use of TCP and UDP Datagrams

When transferring TCP streams or UDP datagrams from the black to the red network, the TCP client in the black network is given information about the success/failure of the transfer. That is why the TCP protocol offers a high degree of transfer reliability; whereas UDP, even with repeated transfer, does not offer a guarantee

that the packets that have been sent out will be received, due to the protocol being limited to sending data in only one direction.

5.2.6. Data Transmission via Protocol Converters

The ALGs of vs-diode have appropriate protocol converters, so-called relays, for processing FTP, SMTP, Lumberjack and other possible complex protocols.

The ALG receives for example all the FTP and SMTP commands and data in the black network. The SMTP relay in the black ALG can check particular MIME types and file extensions and filter them if required. Integration of a virus scanner is also possible here. Files are forwarded to a FTP2TCP relay after being examined.

This relay uses a separate TCP connection to forward each command over the one-way filter to the corresponding partner process – the TCP2FTP relay on the red ALG. Here the data is transferred by TCP stream, only success or failure is signaled in the opposite direction.

The FTP command and data will then be restored in the red area from the data provided by this connection. The command is subsequently forwarded by the red TCP2FTP relay to the FTP server. This server returns a status message, which the TCP2FTP relay will then check for success or failure of the transfer.

5.3. The vs-diode Security Features – a Summary

The transmission process within the vs-diode features numerous security features.

5.3.1. Separation of the TCP Data Stream at Both ALGs

The TCP data stream is interrupted at both ALGs and the information stored temporarily: data packets are not forwarded. All control information is reinserted in the TCP packet headers when a new connection is opened. This means that the packet headers only receive the information necessary for communication and are free of any content. Unintentional flow of information from the red network to the black, as well as timing and covert channel attacks are thereby ruled out.

5.3.2. Filtering of SMTP and FTP Content

vs-diode provides several content filtering options, depending on the protocol being used: The SMTP relay on the black ALG is able to examine parameters of incoming mails such as the authorization of the sender, MIME types, file extensions, script languages and active content according to specified rules and, if necessary, to refuse delivery of the mail. The FTP relay on the black ALG can check particular query methods and filter them if required.

5.3.3. Anti-Virus Scanning

A virus scanner on the black ALG can reliably protect the sensitive red network from malicious code.

The genuscan software option is provided for this purpose: incoming data is processed in a so-called cage, a secure area in the file system of the ALG. There, the data is prepared for the virus scanner by uncompressing it (unpacking the individual files from the archives). This can be carried out recursively if required.

If the scanner should detect a virus, genuscan will trigger appropriate alarm messages. The genuscan system retains any e-mails infected with a virus in a secure area for further analysis. It only forwards data in which no viruses have been found.

genuscan works optionally with ICAP or with the additional package for the virus scanner Antivir Professional.

5.3.4. Highly Secure Diode Function of the One-Way Filter

The complex testing routines of the two ALGs are supplemented by a one-way filter. The separate appliance provides the middle section and contains the essential safety component of vs-diode. The one-way filter allows information transfer only from black to red. The actual diode function is implemented on a minimalist microkernel system. It is of low complexity and easy to analyze. Its complete code can be checked to eliminate errors in this crucial component. The high-security diode function is the key feature of vs-diode and guarantees absolutely reliable one-way data transfers.

5.3.5. Highly Secure Boot Process of the One-Way Filter

The one-way filter is booted using a specially developed coreboot implementation. As a minimal BIOS, it initializes only permitted hardware components. An extension to the UEFI Secure Boot functionality allows only the loading of software signed by genua. Third-party software or a modified operating system cannot be loaded.

5.3.6. External Access to the Boot Medium Impossible

The boot medium of the one-way filter is a static configuration DVD-ROM. This follows the security by design approach: the information transfer through the one-way filter only from black to red cannot be changed on purpose or through configuration errors. Permitted changes such as updates or upgrades require physical access to the device. As a result, the security of the system is significantly increased.

5.3.7. Hardening the ALGs

The OpenBSD operating system used on the ALGs is already hardened against attack and therefore already optimized for use in a data diode.

5.4. Performance

A single vs-diode system can achieve a data throughput of up to 3 GBit/s, which can be extended as required by building a load-sharing cluster.

5.4.1. Hardware

At the moment we offer vs-diode in our medium sized hardware. As genua is continuously adapting the different models to current technological developments (e.g. the CPU type), their specifications may change at short notice. The current technical details may be found online in our hardware data sheet:

https://www.genua.eu/vs-diode

5.4.2. High Availability Clusters

Uninterrupted availability of the security systems is an absolute necessity for many organizations. For this reason genua offers cluster solutions consisting of a number of vs-diodes.

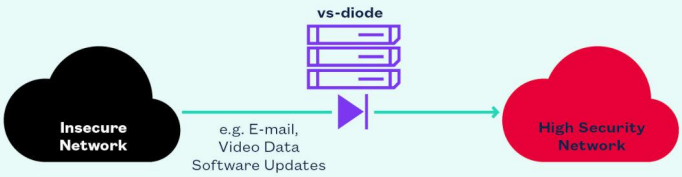
This solution has the following advantages:

- All systems included in a high availability cluster share tasks during normal operation.
- An immediate manual intervention in the event of a system failure is not necessary.
- The cluster is fully scalable and can be extended as required in order to meet higher bandwidth requirements.

6. Use Cases

One obvious application for vs-diode can be derived from the regulations for public authorities mentioned in Section 2; another is in the field of national defense communication. Securing networks connected with research laboratories, development departments and other sensitive areas in the private sector can be allowed by competent authorities.

Particularly strict security regulations apply to classified information in the military sector, with national defense being one of the key interests of a country. Such data is to be processed exclusively in the specially protected red networks and under no circumstances may this information be transferred to black networks.



Data transfer into a classified network

It should, however, be possible to transfer data that is freely available or subject to lower classification levels from black to red networks.

All data from red networks therefore needs to be secured against threats from outside, so that confidential information does not fall into unauthorized hands. Data transfers in the opposite direction should be allowed – from black to red networks – but protected of viruses and malware.

The vs-diode has been conceived for exactly this purpose: in addition to a comprehensive examination of the data being transferred, it provides fully automatic, real time unidirectional information transfer in 24/7 operation. Further, it meets the high requirements demanded in military use – both in stationary applications and, for example, on ships.

Real-life applications in the public as well as in the private sectors are geo-information systems (GIS), enterprise resource planning systems (ERP) and the control networks of large technical plants – such as power plants or railway interlocking systems – that for security reasons are located in a red network but at the same time are dependent on ongoing data synchronization.

Support of syslog and the Lumberjack protocol allows the aggregation, analysis, visualization, and subsequent processing of data in isolated networks using Elasticsearch applications. To this end data can be transferred from a number of sources to a central store via vs-diode and secured from outside. Use of the vs-diode between several stores allows a hierarchical architecture of highly secure data processing instances.

The vs-diode's FTP support with TLS encryption as an option means that it is also suitable for synchronizing larger amounts of data while the SMTP relay allows receiving e-mail even in separated networks.

The system can be flexibly adapted to custom environments. For example, additional protection mechanisms can be implemented against malware or active content.

7. Approval

Approval procedures are reserved solely for IT security products that are used within federal and state governments for the processing and transmission of confidential and classified official information, or by companies working within the framework of contracts for the federal and state governments.

vs-diode is approved for the classification levels German SECRET ("GEHEIM"), UE SECRET/SECRET EU, and NATO SECRET. Please feel free to contact us for further information about approval. We will be pleased to offer you more comprehensive information.

8. Support

8.1. Installation Service

If required, genua and our specialized partners will support you during the installation, configuration and commissioning of your vs-diode. In this process, your administrators will be extensively instructed in product use and maintenance. If requested, we will first outline a detailed plan for a secure network coupling. Personal security clearances up to “secret” are available.

8.2. Training

genua provides a range of training courses and workshops specially tailored to your needs. Please feel free to ask for further information. We will be pleased to help.

8.3. Software Support for Operational Systems

Update Service: genua’s solutions are continuously being developed further. New versions incorporating current developments and useful new functions are released regularly. Intermediate versions may also be released if necessary. You will also receive security fixes with our update service. Additional intermediate versions may also be released if necessary.

Hotline: Our qualified staff provide e-mail and telephone support (up to the German security clearance level “Secret”) in addition to our update service. You can use our hotline for any questions related to your solution. If required, we can provide telephone hotline support 24 hours a day, 7 days a week. This means you can rely on getting support straight from the manufacturer of your vs-diode.

genua GmbH, Domagkstrasse 7, 85551 Kirchheim/Munich

P +49 89 991950-0, F +49 89 991950-999, E info@genua.eu, www.genua.eu