



GeNUGate Data Diode

Reliable Unidirectional Data Transfer at Red-Black Transitions

Connections between networks with different classifications – so-called red-black transitions – are difficult: Here, it is imperative to ensure that no confidential information from the red network with the higher classification reaches the black area, since unauthorized persons also have access to this area. This applies even when the unidirectional data transfer is set up so as to flow only from the black network to the red network. This is because, for a rapid and reliable transfer

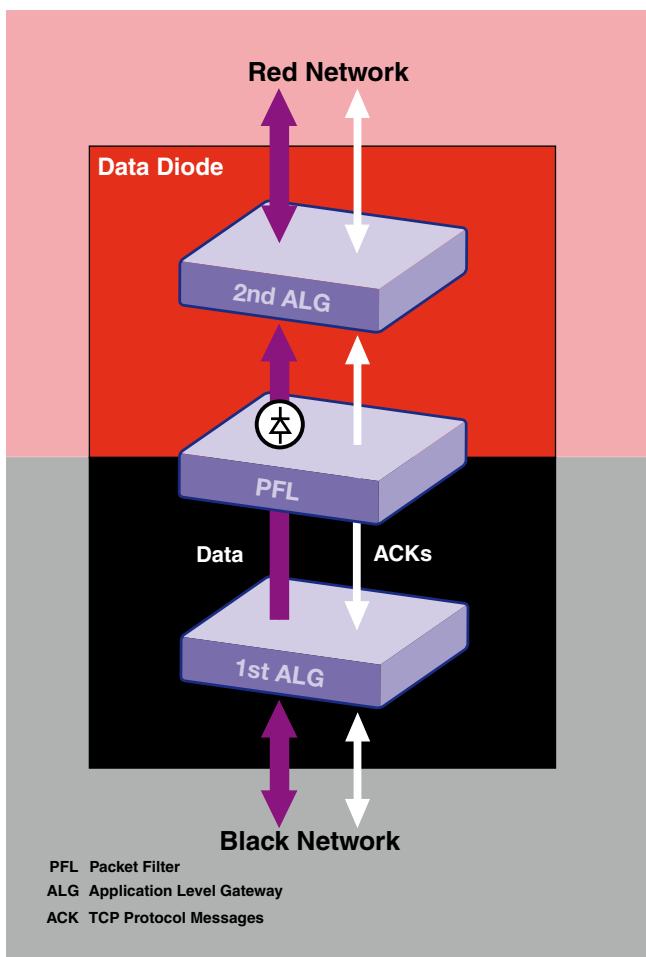
into the red network, a feedback connection in the opposite direction is required, by means of which the black sender is notified that all data packets have arrived properly. The common protocols TCP (for data) and SMTP (for e-mails) work in this manner. By contrast, procedures without a feedback channel are significantly slower and constantly lose packets, so that the transferred files are unusable.

The Feedback Channel must be Secure

Important applications and the transfer of larger quantities of data therefore necessitate protocols with a feedback channel. The technical challenge here is that only the protocol messages (ACKs) required for the data exchange flow from red to black – but never confidential information.

GeNUGate Data Diode as a Security Gate

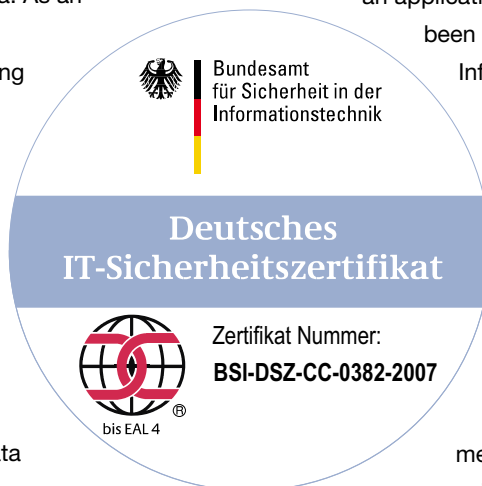
For this task, we designed the GeNUGate data diode. This solution is made up of three series-connected security systems – an application level gateway, a packet filter, and a second application level gateway (A-P-A structure). These three components together act like a sluice, with a wide channel and a narrower channel: data from the black network is accepted and transferred via a new connection to the red area, while in the opposite direction, by contrast, only protocol information that has been reduced to that which is absolutely necessary can pass through.





The Transfer Process

The black TCP or SMTP data arrives at the first application level gateway of the diode. Here, it is accepted, and the connection is then broken – an application level gateway does not allow a continuous flow of data. As an additional security measure, this diode component provides the option of filtering the accepted e-mails for viruses and malware in order to protect the red network. The new connection to the second application level gateway is now opened. The interposed packet filter allows this data to pass, but controls traffic in the opposite direction very carefully: only protocol messages that are sent back by the second application level gateway for data transfer to the first application level gateway, and that have been reduced to the absolutely essential information, are allowed through. All other content is removed, and packets from other senders are efficiently blocked. Finally, the second application level gateway establishes a new connection to the recipient and transfers the data to the red network. Together with the diode function of the packet filter, this twofold interruption of the data flow by the application level gateways ensures optimal security for red-black transitions. Detailed covert channel analysis testify to the high level of protection.



Setting up Important Applications with a High Level of Security

The GeNUGate data diode makes it possible to set up the data transfer from black to red for important applications with ease, and with a high level of security. Some examples are:

- Mirroring of databases for geographic information systems (GIS)
- File transfers
- Linking of e-mail systems

Certified by the German Federal Office for Information Security

The data diode is based on the proven GeNUGate firewall system by GeNUA. This two-tier firewall, consisting of an application level gateway and a packet filter, has been certified by the German Federal Office for Information Security (BSI) in accordance with CC EAL 4+ and, additionally, classified as Highly Resistant, since the EAL 6 level was attained for the important self-protection security criterion. GeNUGate is the only Highly Resistant Firewall in the world. For the three-tier data diode, an additional application level gateway was added to this highly efficient security solution. Depending on the performance requirements, we provide the GeNUGate data diode on various hardware systems in which all of the important components are redundantly designed. The most powerful individual system achieves a data throughput of 600 Mbit/s, and any additional requirements are satisfied with our highly available clusters.

Service to Satisfy any Customer Requirements

We provide service that is tailored to your exact requirements. On request, our system management will take over the continuous monitoring and complete administration of the security systems via heavily encrypted Internet connections. We also offer a 24/7 hotline service that can be accessed via telephone or e-mail, as well as a regular update service so that your solution is always state-of-the-art.

About GeNUA

GeNUA, Gesellschaft für Netzwerk- und Unix-Administration, is a German company specializing in IT security. Since the company's establishment in 1992, we have been involved in securing networks and developing sophisticated solutions. Our products and services include firewall systems with BSI certification, high-security gateways for red-black transitions, VPN and remote maintenance solutions, data optimization for satellite communications, and an extensive range of servicing options. Many companies and security-conscious agencies rely on GeNUA solutions to protect their IT systems.