genua.

EUROGATE Puts its Trust in genugate

EUROGATE operates a total of nine container terminals in Europe, and has a total workforce of 6,600. The largest terminal is Bremerhaven, while Hamburg has the most dynamic growth. As soon as a ship docks here, the huge container cranes start their work: they move busily back and forth, loading and unloading the huge ships at high speed. This speed is possible only thanks to perfect coordination. Software programs calculate all the processes and generate the optimum stowage plan. This ensures that no container is suddenly in the wrong place, or has to be moved several times.

Europe's largest container terminal operator safeguards IT and data communication with a firewall cluster that guarantees high availability.

Global trading today utilizes a universal form of packaging – the container. Regardless of whether textiles, television sets, raw steel, refrigerated fruit, or gasoline, there is room for everything in these standardized steel crates. Most of them will travel around the globe on container ships, and the number is steadily growing. Container transport is currently expanding, matched by a similar increase in the number and size of the ships used. The latest container ships can stack up to 15,500 TEUs (twenty-foot equivalent units, or standard containers). The advantages of the container become most apparent when it reaches its destination port. Instead of the goods having to be transferred individually, which would be a most laborious process, the entire container can simply be moved onto a train or truck for onward shipment. Careful coordination is required at this stage.

Computers calculate the optimum procedure, to ensure that all the containers end up promptly in the right place, while customers are kept constantly updated on the status of their delivery. Data ex-change must always be able to function in this environment, since breakdowns can mean longer wharf and shipment times, and thus higher costs as well. EUROGATE, the largest container terminal operator in Europe, uses a cluster with two-tier firewall systems to safeguard and ensure the high availability of its data connections at the LAN-Internet interface.

Project Description

The Customer:
EUROGATE, Europe's largest container terminal operator

The Task:
Secure communication for a shipping and logistics company

The Solution:
High availability operation of the genugate firewall with certification according to CC EAL 4+ and approval for classification levels German VS-NfD, NATO RESTRICTED, and RESTREINT UE/ EU RESTRICTED

Continuous Exchange of Data is Needed for Efficient Coordination

Data needs to be exchanged constantly in order to coordinate procedures: ship owners e-mail information on their cargoes, container deliveries, and onward transport. In turn, the terminal operator uses the "Infogate," to provide detailed information on the status of the unloading of ships, so that customers are at all times aware of where each of their containers is. EUROGATE is also in constant contact by data line with many business partners who provide additional logistics services, or who carry out maintenance work. If this flow of information were ever to break down, work on the long quays would quickly come to a standstill – and EUROGATE would incur substantial additional costs.

Stephan Krause, IT administrator at EUROGATE in Hamburg explains: "To ensure, for example, that a container from Beijing gets to the right consignee in Berlin on the agreed date, a lot of different processes need to mesh together perfectly. Reliable data exchange between all the parties involved is absolutely crucial to maintain this complex logistics exercise, so we place the highest priority on IT security and reliability." In its efforts to ensure that these standards are met, the terminal operator is assisted by the Hamburg-based IT consulting and services company secion GmbH.

To coordinate the EUROGATE logistics processes, data must be constantly and securely exchanged.

Critical Point: The Interface to the Internet Must be Secured

To ensure reliable data communication, it is essential to secure the gateway between the local EUROGATE network and the Internet. In this instance, the secion IT specialists recommended the use of two genugate-type firewalls that are combined to form a cluster. secion Managing Director Hellmuth Michaelis is convinced that the genugate firewall is the right solution for requirements such as these: "In a cluster, the system can be used with a high degree of availability, and, thanks to the two-tier system, it provides a high level of security that has been tested by the German Federal Office for Information Security (BSI), and certified to an extremely high level."

genugate is a security solution developed by German firewall company genua, which is based in Kirchheim, near Munich. The option of combining genugates in clusters is an important feature: the systems in the clusters share tasks and monitor one another. If one system breaks down, the other can take over the entire load at short notice. As a result, the firewalls act as an efficient protective wall, ensuring high availability between the Internet and the company network.

Secure: Demilitarized Zone for Online Services

The genugate firewalls also divide the internal area of EUROGATE into two separate networks: the demilitarized zone (DMZ), and the actual Local Area Network (LAN). The DMZ contains the systems that can be accessed from both the Internet and the LAN, e.g. the Infogate information system. The LAN itself, with the clients, is even more securely sealed off. No external access is possible here, except for expressly authorized connections.

"The neutral buffer zone between the Internet and the LAN is an intelligent solution," explains Stephan Krause. "It allows us to offer customers and external partners convenient online services without jeopardizing the security of our corporate network."

The two internal security zones can be set up very easily, since genugate provides two firewall systems in one solution: an application level gateway and a packet filter. Both systems are different types of firewall, and run on physically separated computers. The DMZ is protected from the Internet by the application level gateway, while the LAN enjoys two-fold protection thanks to the additionally installed packet filter.

"genugate has two coordinated firewalls whose control mechanisms complement one another at different levels, providing reliable protection for our network."

Stephan Krause, IT Administrator, EUROGATE

4

Secure Protection:
Two Firewall Systems in One Solution

Data from the Internet therefore has to get through two firewall systems before it reaches the EUROGATE LAN. However, its journey comes to an abrupt end at the first control point: the application level gateway blocks the data packets, and a direct connection is never permitted. The system checks the packets, analyzes the contents, and blocks out harmful data, such as viruses or active Web content.

Once its content has been carefully examined by the application level gateway, the data passes on to the second firewall system, the packet filter, immediately upstream of the LAN. The packet filter is designed to be even more restrictive. It generally allows through only data packets that have previously been requested by the LAN. Data packets are checked at network and transport level using the header information. Individual ports need to be expressly activated for other external connections.

Greylisting Helps Defeat Spammers

genugate also has an efficient method of dealing with annoying spam. Greylisting is based on a simple technique. Three pieces of information are queried for all incoming mail: the IP address of the dispatching mail server, the address of the sender, and that of the recipient. If this three-part data combination occurs for the first time, the e-mail is rejected, but the new set of information is stored. In these cases, professional mail servers will make a second attempt to deliver after a short period of time. Since the three-part set of information is already known, the mail is then allowed through to the recipient. Spammers, on the other hand, focus on sending volume in the shortest possible period, and do not waste time on repeat deliveries. For that reason, they are foiled by greylisting. "We receive around 30,000 e-mails per day, but, thanks to greylisting, only 5,000 are accepted. This method successfully mitigates the annoying problem of spam," explains Stephan Krause.

EUROGATE is using two genugates in a cluster that is regularly up-dated with new software from the manufacturer genua to combat any new risks. Stephan Krause summarizes the advantages of the system as follows: "genugate has two coordinated firewalls whose control mechanisms complement one another at different levels, providing reliable protection for our network. With the continuing success of EUROGATE, we are experiencing an increasing number of attempted attacks, but with this solution no security issues have ever arisen."
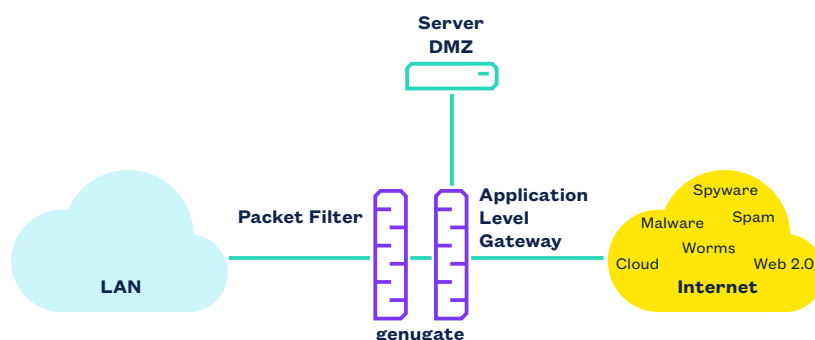
The two-tier firewall genugate combines two different firewall systems
– an application level gateway and a packet filter

genugate Firewall is Certified to the Highest Level

This appraisal has also been confirmed by the German Federal Office for Information Security (BSI). It has certified the two-tier solution in accordance with the international Common Criteria (CC) standard at the EAL 4+ security level. This is the highest level that can reasonably be applied to a complex security system such as a firewall. However, genugate can meet even higher standards when it comes to the important security criterion of "Self-protection against direct attacks." Here, it meets the criteria for EAL 7. This is a significant point: a firewall must be equipped to deal with all kinds of attacks or attempts to manipulate data if it is to provide reliable security for the network it is guarding. Because of this function, the firewall is also classified as "highly resistant" – the only firewall in the world to achieve this rating.

Certification and approval by the German Federal Office for Information Security

genugate is certified according to the Standard Common Criteria (CC) at the strict EAL 4+ level and approved for classification levels German VS-NfD, NATO RESTRICTED, and RESTREINT UE/EU RESTRICTED

Bundesamt
für Sicherheit in der
Informationstechnik

**Deutsches
IT-Sicherheitszertifikat**

BSI-DSZ-CC-1154-2021

EAL 4 mit Zusatz
Gültig bis: 21.06.2026

Common Criteria

0325-11-EN

About genua

genua GmbH secures sensitive IT networks in the public and enterprise sectors, at KRITIS organizations and in the classified industry with highly secure and scalable cyber security solutions. The company focuses on comprehensive network protection and internal network security for IT and OT. The range of solutions includes firewalls and gateways, VPNs, remote maintenance systems, internal network security, and cloud security through to remote access solutions for mobile working.

genua GmbH is a company of the Bundesdruckerei Group. With more than 400 employees, it develops and produces IT security solutions exclusively in Germany. Since the founding of the company in 1992, regular certifications and approvals from the German Federal Office for Information Security (BSI) provide proof of the high security and quality standards of the products. Customers include, among others, Arvato Systems, BMW, the German Armed Services, THW as well as the Würth Group.

genua GmbH | Domagkstrasse 7 | 85551 Kirchheim, Germany
+49 89 991950-0 | info@genua.eu | www.genua.eu