High Resistance Firewall
genugate
Robust Security for Networks
Your degree of IT security is largely defined by what happens at the interface between the Internet and your local network. All external access, and all outbound data must pass through this point. The more reliably traffic is screened here, the higher the degree of protection will be for your entire network. IT security at this critical interface should therefore be given the highest priority. A central security component here is content analysis: content is only allowed to enter your network after thorough inspection, as well as reliable identification and removal of any dangerous elements.

A Customizable Comprehensive Solution
The genugate is a high resistance firewall developed by the German manufacturer genua as a solution for critical interfaces. genugate is a complete solution comprising hardware, operating system, and firewall software. The product’s unique factor: Two different firewall systems – an application level gateway and a packet filter – are combined to a compact solution. All components are perfectly coordinated and specifically designed for maximum security. The OpenBSD operating system ensures high security standards, and the two firewall systems run on physically separated computers. Both firewalls, however, are operated through a single interface, simplifying administration and reducing support costs. The genugate stands out by its two-tier protection, and guarantees you robust protection at critical interfaces.

Application Level Gateway Screens Content
At the heart of the genugate solution is the application level gateway. This advanced security system checks all data stream content. The first step in this process is termination of the incoming data packets – the application level gateway never permits a direct connection between the Internet and your local network. This feature significantly increases security: network level attacks are no longer possible, eliminating many potential weaknesses, such as those involving extended IPv6 headers. Then, much like a puzzle, the packets are re-assembled, as content checks can be carried out only on complete data records. The application level gateway can now filter the data and block out unwanted material: active content, viruses, or spam, depending on how you have configured your system. Data will be forwarded over a new connection only after all checks have been performed. The application level gateway can also secure cloud usage, e.g. by only allowing encrypted uploads to external services. The comprehensive content analysis provided by the application level gateway means genugate provides a significantly higher level of security than so-called "next generation" firewalls. These mostly use deep packet inspection or pattern matching, and only check a random sample of the data contents.

Teamwork with Packet Filter
genugate also has an additional packet filter, operating on the inside (local network side). The packet filter checks data packets according to the header data: IP address, protocol type, and port number. As a result, all data negotiates two firewall systems, with protection systems operating on different levels. The two systems effectively work as a team, each supporting the other. This two-tier system also allows the configuration of demilitarized zones (DMZ) exactly to your requirements. Additional interfaces can be used to connect servers to either the application level gateway or the packet filter. This in turn permits providing of services in the Internet that are secured by the powerful application level gateway. Alternatively, servers can be closely connected to your LAN via the packet filter.
Security vs. Performance

Two tiers, comprehensive content control, separation of all connections – the genugate high resistance firewall is a no-compromise high security design. These three features set the genugate apart from the firewall solutions of other manufacturers. They also require considerable computing capacity – an inevitable cost in terms of data throughput performance, even when the most modern hardware is used. Note this relationship between security and performance applies for all firewall systems, and means that high performance figures can only be achieved at the cost of reduced security or vice-versa – even when some manufacturers promise otherwise. You should not make compromises with the security of critical interfaces. Here, the genugate is the right solution.

genugate: the Ideal Basis for a P-A-P Solution

The German Federal Office for Information Security (BSI) recommends protecting the critical connection between the Internet and a local network with a firewall combination, consisting of two packet filters and an application level gateway, or P-A-P for short. The packet filters placed on either side of the powerful application level gateway provide optimum protection against both direct attacks and high data loads. With genugate, it becomes a simple matter to provide this high level of protection. For example, a P-A-P solution can be created with an Internet router configured with rules to act as an additional packet filter, operated in conjunction with the two-stage genugate system.

genugate: Central Security System at the LAN-Internet Interface

ALG: Application Level Gateway
PFL: Stateful Packet Filter
DMZ: Demilitarized Zone
Seal of Approval: Certified to CC EAL 4+

The genugate system has been certified at the strict EAL 4 security level by the German Federal Office for Information Security (BSI), in accordance with the international Common Criteria (CC) standard. This required the submission of detailed design documentation for all security mechanisms, including the complete source code, and involves extensive testing. This process allows independent experts to check that all security functions have been correctly implemented, down to every individual line of code. The result of this process was certification at the level EAL 4+ with the additional rating “Highly Resistant.”

Strong Self-Protection against Direct Attack

What exactly is the significance of EAL 4+ certification with the additional classification of „Highly Resistant“? EAL 4 is the first level to include a source code audit, and concurrently is the highest level that can reasonably be applied to an entire system as complex as a firewall. The addition „+“ indicates however, that level EAL 4 has been surpassed for certain criteria. genugate has achieved this in its handling of patches. However, this is a criterion other manufacturers also could fulfil in order to improve their certification level with a „+“. Far more important for your IT security is the fact that genugate meets even higher standards when it comes to self-protection: the firewall provides systematic dual protection using two different security mechanisms for all potential points of attack, such as interfaces. As a result, the system is highly resistant to direct and intelligently carried out attacks – its security capabilities correspond with the evaluation assurance level AVA_VAN.5, and comply with EAL level 7 requirements. This is a decisive point: the firewall itself has to be reliably secured against attack in order to provide the same continual degree of security to the network it protects.

Only Highly Resistant Firewall in the World

Based on this exceptional security performance, the BSI has classified genugate as “Highly Resistant” – the only firewall in the world to achieve this rating. This rating gives our customers an independent guarantee that they have purchased a high-security solution. We renew the certification of the genugate high resistance firewall by the the German Federal Office for Information Security (BSI) with every major release of the genugate to provide ongoing assurance of its high quality.

Certification

Standard: Common Criteria (CC)
Level: EAL 4
Recertification: Every major release
Special Feature: Fulfillment of level EAL 7 requirements for self-protection brings „Highly Resistant“ classification.
Hardware and Clusters to Meet all Requirements
To precisely meet a wide range of different requirements, we supply genugate in various hardware models. We can handle any bandwidth and availability requirements in excess of these capacities by using clusters: all genugate models can be bundled to clusters with any capacity requirement the customer specifies. The firewall is administrated using a consistent Web GUI. If deploying a number of genugate firewalls, you can use a management station to comfortably create and distribute configuration information such as IP addresses or server names. In addition, the genugate supplies an interface for Security Information and Event Management (SIEM) applications, such as QRadar from IBM. This assists in the integration of the firewall system log files in your central event and risk analysis.

genugate Can Do even More
A wide range of products can be added to the genugate firewall system to create a comprehensive security solution. For example, the genuscan interface package allows the integration of a virus scanner for common Internet protocols. The external genugate Scanserver can perform this role for situations with especially high performance requirements. genua also offers standby systems, URL blockers, and reverse proxies for authentication and SSL encryption.

Service Directly from the Producer
In the area of support, your wish is our command. Many customers ask us to handle the whole process of administering their firewall solution. That means they can focus on their core business, and leave their IT security in our professional hands. We also offer hotline support 24 hours a day, seven days a week, and a regular update service. When it comes to hardware support, however, there only is one choice: Every genugate comes with a Germany-wide next business day replacement service. If one of your appliances breaks down, you will receive an identical exchange unit on the next working day. This support service is provided free for the first three years after purchase of the product.
About genua

genua is a German company specializing in IT security. It has been securing networks and developing sophisticated security solutions since the company was founded in 1992. Our business activities range from securing sensitive interfaces in public authorities and industry to networking highly critical infrastructure, reliably encrypting data communication over the Internet, remote maintenance solutions and providing remote access for mobile users and home offices. Our solutions are developed and produced in Germany. Many companies and public authorities rely on solutions from genua to protect their IT.

Our Customers Include:

- Ansbach Regional Authority
- Borgers-Group
- EUROGATE
- German Federal Agency for Technical Relief (THW)
- German Federal Ministry of Labour and Social Affairs
- German Federal Public Prosecutor, Federal Supreme Court
- German Federal Statistical Office
- German Parliament Bundestag
- Homeland Security
- Information Network Berlin-Bonn (IVBB)
- KASTO Maschinenbau
- Klüber Lubrication
- MAN
- man web systems
- Mülheim an der Ruhr municipal authority
- Press and Information Office of the German Federal Government
- RTL II television channel
- Schober Information Group
- State Criminal Investigation Department of Thuringia
- Stuttgarter Lebensversicherung
- Swarco Traffic Systems
- WMF
- Würth Group

Further information:
www.genua.eu/genugate

Your Benefits from genugate:

- The two-tier system ensures top security
- Control of data content by the application level gateway
- Consequent termination and re-initialization of all connections
- Convenient migration to IPv6
- Secure cloud usage
- Convenient setup of a demilitarized zone (DMZ) on the basis of the two-tier system
- Clusters for high availability and bandwidths
- Integration in Security Information and Event Management (SIEM)
- Simple integration offered as a complete solution
- Quality guaranteed by CC certification
- The only Highly Resistant firewall in the world
- Customer service directly from the manufacturer

Further information:
www.genua.eu/genugate