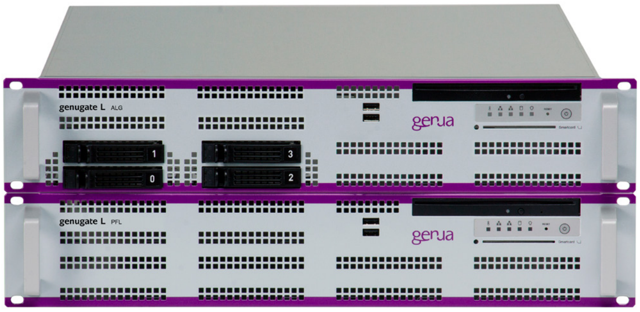
High Resistance Firewall genugate

Facts & Features



Definition:

genugate is a two-tier firewall with an application level gateway and a packet filter connected in series. The evaluation and content analysis by the application level gateway sets genugate apart from many other firewall solutions. As a comprehensive solution, genugate consists of matched hardware, operating system and firewall software. Both IPv4 and IPv6 are fully supported, thus easing the migration to IPv6, while also enabling dual-protocol use. This solution complies with the requirements of the German Federal Office for Information Security (BSI), which has certified genugate to the Common Criteria (CC) level EAL 4+ and classified it as “highly resistant”. genugate is the only firewall worldwide to have been given a highly resistant rating, which attests to the high quality of the genugate firewall.

Typical Use:

- Safeguarding internal networks against unauthorized access from outside (e.g. Internet)
- Structuring an intranet to establish domains with different protection schemes
- Protect machine to machine communication as security gateway for SOAP and web services

Throughput Volume:

- Up to 2.610 Mbit/s TCP and 4.380 Mbit/s UDP with a single genugate system, more throughput possible with clusters

Service:

- Customer service directly from the manufacturer
- Security system management
- Hotline service / update service
- Free hardware support for three years from date of purchase
- Comprehensive training courses

Reasons to Choose genugate:

- Two-tier system assures top security
- Genuine application level gateway: separation of data flow and re-establishment of connections (no connection transfers)
- Proxy services for a wide range of protocols (WWW, SMTP, SIP, SOAP, SSH, IMAP, etc.)
- Spam and virus protection
- Certification to CC EAL 4+
- Self-protection at EAL 7 level, thus the world’s only firewall with a “highly resistant” rating
- IPv4 and IPv6 support for migration and dual-protocol use
- High availability and increased bandwidth through cluster
- Logging of all network activity
- Simple integration as a complete solution
- User-friendly GUI-based administration
- SIEM integration
- Web application awareness
- Improve TLS security for clients and servers

Reasons to Choose genua:

- Leading German specialist for IT security
- Founded in 1992 – implementation of numerous major projects for industrial, government, and military organizations

SecurITy made in Germany

First Tier Firewall: Application Level Gateway (ALG)

Application Level Proxies	
WWW	Proxy for filtering / scanning web content
HTTP, HTTPS	Web server protection
SMTP, SMTPS	E-mail communication
SOAP	Web service XML validation
SSH	Secure Shell
SIP	VoIP
IMAP, IMAPS	Receive and send e-mail
FTP, FTPS	File Transfer Protocol
POP3	Receive e-mail
DNS	Domain Name Service
Telnet	Telnet services

Circuit Level Proxies	
TCP	Generic TCP connections
TCP + SSL	Encrypted TCP
UDP	Generic UDP connections
IP	Generic IP connections
UDP multicast	Generic UDP multicast
Ping	Ping (ICMP)

Stateful Filtering	
Network Address Translation (NAT)	+
Quality of Service (QoS)	+
Port forwarding	+
DDoS protection	+
Packet normalization	+
Policy filtering	+

Web Protection*	
Real time web protection	Cloud-based detection of phishing and malicious websites and botnets
Advanced web categories	Block by categories (e.g. gambling, online auctions), customizable information page

Web Filter	
Cloud Storage	+
Conferencing	+
Remote Access	+
Software Updates	+

Content Filter	WWW	FTP	SMTP	POP3
Active Content	+	–	+	+
Request method filter	+	+	–	+

Authentication	WWW	SSH	FTP	Telnet	TCP
Token card (Cryptocard)	+	–	+	+	–
LDAP / LDAP group	+	+	+	+	–
Password / local	+	+	+	+	–
Radius	+	+	+	+	–
Sidechannel (incl. time frame)	–	–	–	–	+

E-Mail	
Modes	Server/Forwarder/Proxy
Delivery Status Notification (DSN)	+
Mail aliases	+
Autocrypt e-mails	+
Maximum size	+
File extension ACL	+
MIME type ACL	+
Redirection of e-mails	+

Spam Protection	
Relay protection (sender check/blacklist)	+
Validate sender MX / IP	+
Pattern blocking	+
Sender Policy Framework (SPF)	+
Rating	+
Greylisting	+
Real-time Blackhole List (RBL)	+

Virus Scanning*	
Virus scanning	WWW, FTP, SMTP, IMAP, POP3
Real time virus protection	Protection even against unknown viruses by cloud-based detection
Scan engines	Avira AntiVir for genugate
External scan server*	+
Recursive scan	+
ICAP interface	+

WWW	
URL ACL	+
Domain ACL	+
MIME type ACL	+
Cookie	+
Websockets	+

Web Caching	
External proxy	+
ICAP interface	+

Proxy Settings	WWW	SSH	FTP	SMTP	IMAP	SOAP	POP3	Ping	Telnet	TCP	UDP	IP
Encryption (SSL, TLS, SSH)	+	+	+	+	+	+	–	–	–	+	–	–
Transparent relay	+	+	+	+	+	+	+	+	+	+	+	+

Access Control List (ACL)	WWW	SSH	FTP	SMTP	IMAP	SOAP	POP3	Ping	Telnet	TCP	UDP	IP
Source address	+	+	+	+	+	+	+	+	+	+	+	+
Destination address	+	+	+	+	+	+	+	+	+	+	+	+
Group authentication	+	+	+	+	–	–	–	–	+	+	–	–
Time	+	+	+	+	+	+	+	+	+	+	+	+

Second Tier Firewall: Packet Filter (PFL)

Stateful packet filter	+
Network Address Translation (NAT)	+
Quality of Service (QoS)	+
Queuing (traffic shaping)	+
Port forwarding	+
Filter criteria	IP address, protocol, port, operating system, flags, state
Filter action	Pass, block, log
Spoofing protection	+
DDoS protection	+
Packet normalization	+
Load balancing	+
Auto configuration	+
Configuration monitoring	+
Boot media	USB
GUI configuration	Via ALG
Logging	To the ALG
Reuse configuration objects from ALG	+

System Management

User Management	
User profiles	+
Administrator profiles	+
Supported languages	German, English
Granular administrative rights for each action	Read only, read and write
Administration	
Graphical User Interface (GUI)	+
Entire cluster management via primary system	+
Backup	
Configuration backup by	GUI, SSH, USB stick
System backup	Mirror disk*, SSH
Automated backups	+

High Availability (HA)*

Automatic configuration distribution	+
Load sharing (active-active)	+
Maximum cluster size	16
Balancing connections	+
Slow timeout of running sessions	+

Certification

genugate 9.0	CC EAL 4+ / AVA_VAN.5 (highly resistant)
genugate 8.0	CC EAL 4+ / AVA_VAN.5 (highly resistant)
genugate 7.0	CC EAL 4+ / AVA_VAN.5 (highly resistant)
genugate 6.3	CC EAL 4+ / AVA_VAN.5 (highly resistant)
genugate 6.0	CC EAL 4+ / AVA_VLA.4 (highly resistant)

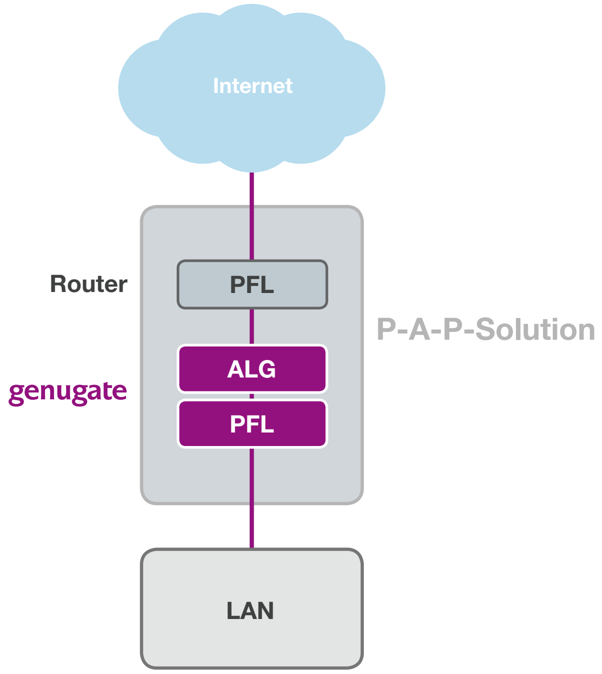
Reporting / Logging

Logfile GUI	+
Download logfiles	GUI, scp
External syslog server	+
Elastic stack integration	+
IBM QRadar integration	+
SIEM integration	+
Management summary	+
SNMP v3	+
Statistics	+
Client connection attempts	+
Server connection	+
Closing connection	+
Client request logging	+
Event notifications	E-mail, SNMP
Event reactions	Change system state, execute programs, predefined actions
Sensors	Network, e-mail, virus, hardware

* optional

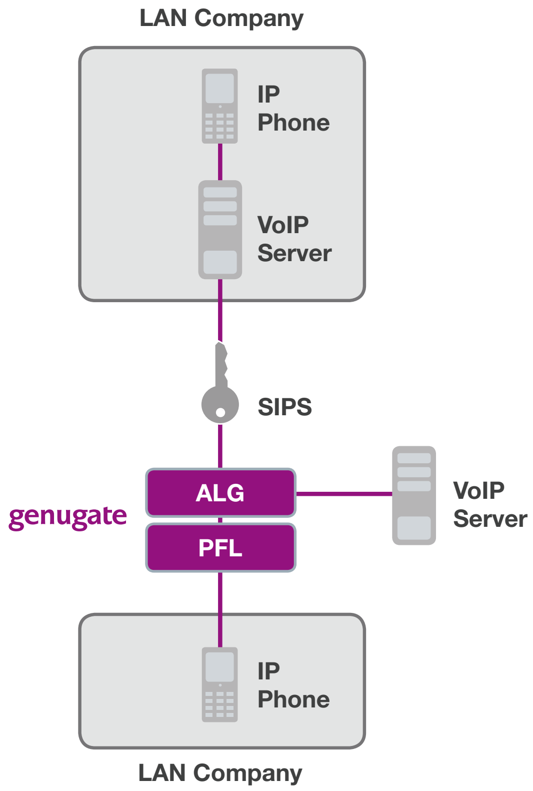
Application Examples

ALG = Application Level Gateway   PFL = Packet Filter



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: An additional Internet router configured with packet filter rules – or a genuscreen firewall & VPN appliance – can operate in conjunction with the two-tier genugate system.



Securing IP-Based Communication

The Session Initiation Protocol (SIP) plays a key role in Voice-Over-IP (VoIP) communication. With genugate secure VoIP operation can be guaranteed. The SIP protocol is analyzed in depth. Only traffic that passes the analysis and the user-configurable filters is allowed. The genugate can still inspect traffic if TLS encryption with SIP (SIPS) is employed. Session Border Controller (SBC) functions are used to prevent attacks against telephones and telephone systems, and allow the implementation of security guidelines. In addition, genugate ensures interoperability of systems that for example use different encryption standards, as well as simplifying certificate administration.

Further information:
www.genua.eu/genugate

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