genugate

Facts & Features

High Resistance Firewall

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 systems.

genugate complies with the requirements of the German Federal Office for Information Security (BSI), which has certified the firewall to the Common Criteria (CC) level EAL 4+ and classified it as "highly resistant". In addition, genugate is approved for classification levels German VS-NfD, NATO RESTRICTED, and RESTREINT UE/EU RESTRICTED.

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 5,475 Mbit/s TCP and 6,820 Mbit/s UDP with a single genugate system, expandable with clusters

Reasons to Choose genugate

- Certified according to CC EAL 4+, AVA_VAN.5, ALC_PAM.1
- Approved for classification levels German VS-NfD, NATO RESTRICTED, RESTEINT UE/ EU RESTRICTED
- 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.)
- Web Application Firewall
- Spam and malware protection
- 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
- Improved TLS security for clients and servers

Service

- Customer service directly from the manufacturer
- Security system management
- Hotline service/update service
- Comprehensive training courses

SecurITy made in Germany

Excellence in Digital Security.

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
DNS	Domain Name Service

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	+
DoS protection	+
Packet normalization	+
Policy filtering	+

E-Mail

Modes	Server/Forwarder/Proxy
Delivery Status Notification (DSN) +	+
Mail aliases	+
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)	+

Web Protection*

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	SSH	FTP
Active content	+	-	+
Request method filter	+	+	-

Virus Scanning*

Virus scanning	WWW, FTP, SMTP, IMAP, POP3
Scan engine	Avira AntiVir for genugate
Recursive scan	+
ICAP interface	+

WWW

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

Authentication	WWW	SSH	FTP
LDAP/LDAP group	+	+	+
Password/local	+	+	+
Radius	+	+	+

Web Application Firewall

Protection Against Critical Security Risks

Command injection	Injection flaws such as SQL, NoSQL, OS, and LDAP injection etc.
Sensitive data exposure	+
XML external entities (XXE)	+
Broken access control	+
Security misconfiguration	+
Cross-site scripting XSS	+
Insecure deserialization	+
Using components with known vulnerabilities	+

* Available as option

More product information

First Tier Firewall: Application Level Gateway (ALG)

Proxy Settings	WWW	SSH	FTP	SMTP	IMAP	SOAP	POP3	Ping	TCP	UDP	IP
Encryption	+	+	+	+	+	+	+	+	+	-	-
Transparent relay	+	+	+	+	+	+	+	+	+	+	+
Access Control List (ACL)	**WWW**	**SSH**	**FTP**	**SMTP**	**IMAP**	**SOAP**	**POP3**	**Ping**	**TCP**	**UDP**	**IP**
Source address	+	+	+	+	+	+	+	+	+	+	+
Destination address	+	+	+	+	+	+	+	+	+	+	+
Group authentication	+	+	+	+	-	-	-	-	-	-	-
Time	+	+	+	+	+	+	+	+	+	+	+

Second Tier Firewall: Packet Filter (PFL)

Packet Filter (PFL)	
Stateful packet filter	+
Network Address Translation (NAT)	+
Quality of Service (QoS)	+
Queuing (traffic shaping)	+
Filter criteria	+
Filter action	Pass, block, log
Spoofing protection	+
DoS protection	+
Packet normalization	+
Auto configuration	+
Configuration monitoring	+
Boot media	+
GUI configuration	+
Logging	+
Reuse configuration objects from ALG	+

Reporting/Logging

Logfile GUI	+
Download logfiles	GUI, scp
External syslog server	+
Elastic stack integration	+
Logstash 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

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	+
REST-API	+
Backup	
Configuration backup	Via GUI, SSH, USB stick
System backup	Mirror disk*, SSH
Automated backups	+
Monitoring	
SNMP	+
Nagios	+

Certification by the German Federal Office for Information Security (BSI)

CC EAL4+	+
AVA_VAN.5	+
ALC_PAM.	+

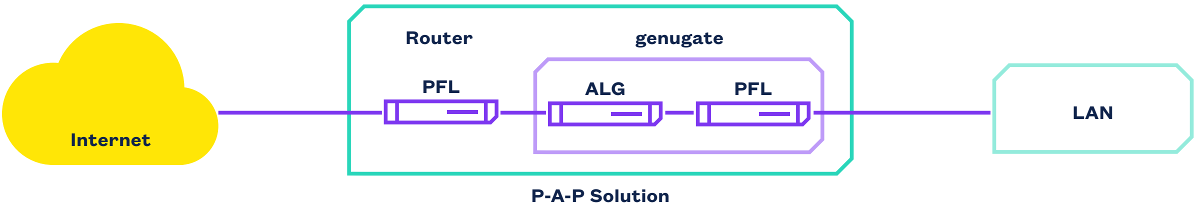
Approval by the German Federal Office for Information Security (BSI)

German VS-NfD	+
NATO RESTRICTED	+
RESTREINT UE/ EU RESTRICTED	+

High Availability (HA)*

Automatic configuration distribution	+
Load sharing (active-active)	+
Maximum cluster size	16

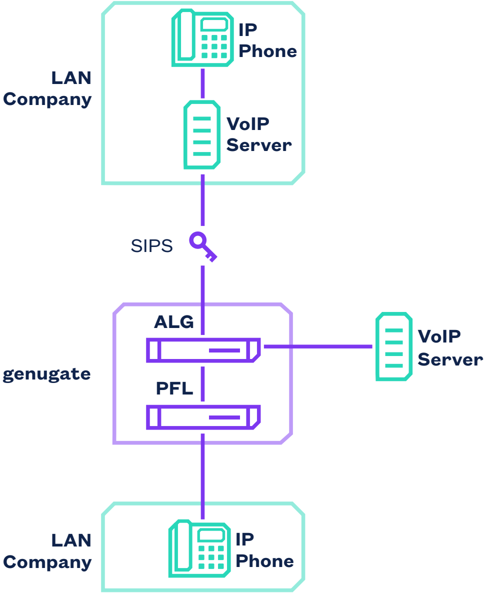
Use Cases



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.

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 Firewall & VPN Appliance genuscreen – 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. 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
+49 89 991950-0 | info@genua.eu | www.genua.eu