



Two-Tier Firewall GeNUGate

Facts & Features

Definition:

GeNUGate is a two-tier firewall with an application level gateway and a packet filter connected in series. The two-tier 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. This solution has also satisfied 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. This attests the high quality of the GeNUGate firewall.

Typical Use:

- Safeguarding the internal LAN against unauthorized access from outside (e.g. Internet)
- Structuring an intranet in such a way as to establish domains with different protection schemes

Throughput Volume:

- Up to 1.280 Mbit/s 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, FTP, SIP, etc.)
- Spam and virus protection
- Certification to CC EAL 4+
- Self-protection at EAL 6 level, thus the world's only firewall with a "highly resistant" rating
- IPv4 and IPv6 support
- High availability and choice of any bandwidth based on multi-clusters
- Logging of all network activities
- Simple integration as a complete solution
- User-friendly GUI-based administration
- Comfortable administration of numerous firewalls with central management station

Reasons to Choose GeNUA:

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



Application Level Gateway (ALG)

Application Level Proxies	
FTP	File Transfer Protocol
HTTP	Web services (HTTP, HTTPS)
NNTP	Network News Transfer Protocol
PING	Ping (ICMP)
POP3	Receive e-mail
SIP	VoIP
SMTP	E-mail communication
Telnet	Telnet services
WWW	Proxy for filtering / scanning web content

Circuit Level Proxies	
Generic IP	+
Generic TCP	+
Generic UDP	+

Stateful Filtering	
Network Address Translation (NAT)	+
Quality of Service (QoS)	+
Queueing (traffic shaping)	+
Port forwarding	+
DDoS protection	+
Packet normalization	+
Policy filtering	+
Load balancing	+
TCP handshake offloading	+

SMTP	
Maximum size	+
File extension ACL	+
MIME type ACL	+
WWW	
URL ACL	+
Domain ACL	+
MIME type ACL	+
Cookie	+

Authentication	FTP	TCP	Telnet	WWW
Tokencard (Cryptocard)	+	-	+	+
Kerberos	+	-	-	+
LDAP / LDAP group	+	-	+	+
Password / local	+	-	+	+
Radius	+	-	+	+
S / Key	+	-	+	-
Sidechannel (incl. time frame)	-	+	-	-
NTLM	-	-	-	+

Relay Settings	FTP	IP	NNTP	Ping	POP3	SMTP	TCP	Telnet	UDP	WWW
SSL / TLS	-	-	-	-	-	+	+	-	-	+
Transparent relay	+	+	+	+	+	-	+	+	+	+
Access Control List (ACL)	FTP	IP	NNTP	Ping	POP3	SMTP	TCP	Telnet	UDP	WWW
Source address	+	+	+	+	+	+	+	+	+	+
Destination address	+	+	+	+	+	+	+	+	+	+
Group authentication	+	+	+	+	+	+	+	+	+	+
Time	+	+	+	+	+	+	+	+	+	+

Content Filter	FTP	NNTP	POP3	SMTP	WWW
Java	-	+	+	+	+
Java Script	-	+	+	+	+
ActiveX	-	+	+	+	+
Selectable programs (e.g. Flash)	-	+	+	+	+
Request method filter	+	-	-	-	+

Virus Scanning*	
Virus scanning	FTP, NNTP, POP3, SMTP, WWW
Scan engines	Avira AntiVir for GeNUGate, Sophos Anti-Virus for GeNUGate
External scan server*	+
Supported relays	FTP, NNTP, POP3, SMTP, WWW
Recursive scan	+
ICAP interface	+

E-Mail	
Modes	Server/Forwarder
Delivery Status Notification (DSN)	+
Mail aliases	+
Autocrypt e-mails	+
Spam Protection	
Relay protection (sender check/blacklist)	+
Validate sender MX / IP	+
Pattern blocking	+
Sender Policy Framework (SPF)	+
Rating	≥ 80 predefined patterns, additional own patterns, change pattern rating
Greylisting	+
Real-time Blackhole List (RBL)	+
ICAP interface	+

Web Caching	
External proxy	+
ICAP interface	+

URL Filter – GeNUBlock*	
Redirect blocked requests	+
Block by categories (e.g. gambling, online auctions)	+
External proxy	+
ICAP interface	+

High Availability (HA)*	
Automatic configuration distribution	+
Load sharing (active-active)	+
Maximum nodes	32



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	+

Reporting / Logging

Logfile GUI	+
Download logfiles	GUI, scp
External syslog server	+
Management Summary	+
Statistic	+
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	English, German
Granular administrative rights for each action	Read only, change
Administration	
Graphical User Interface (GUI)	+
Central management station	+
Backup	
Configuration backup by	GUI, SSH, USB stick
System backup	Mirror disk*, SSH
Automated backups	+

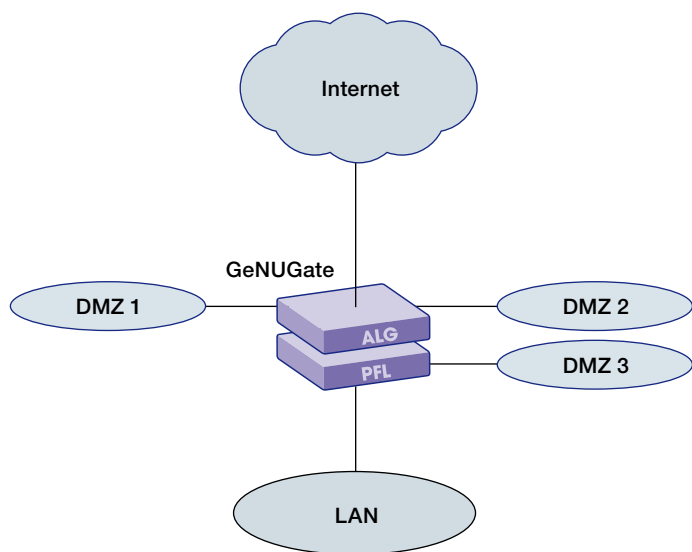
Certification

GeNUGate 6.3	CC EAL 4+
GeNUGate 6.0	CC EAL 4+
GeNUGate 5.0	ITSEC E3 high
GeNUGate 4.0	ITSEC E3 high

* optional



Application Examples

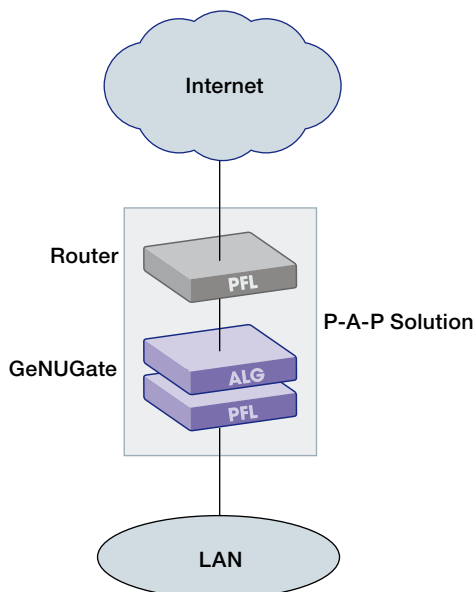


Convenient Creation of DMZs

In order to be able to offer services such as WWW, FTP, etc. on the Internet, GeNUGate, as a two-tier system, allows the convenient creation of separate demilitarized zones (DMZs). In these DMZs with individually customized security policies servers are seeded, which have to be accessed from the Internet. These servers need to be protected against attacks from the Internet, but for security reasons should not be placed in the internal network.

PFL = Packet Filter

ALG = Application Level Gateway



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 can be configured with packet filter rules and operate in conjunction with the two-stage GeNUGate system.