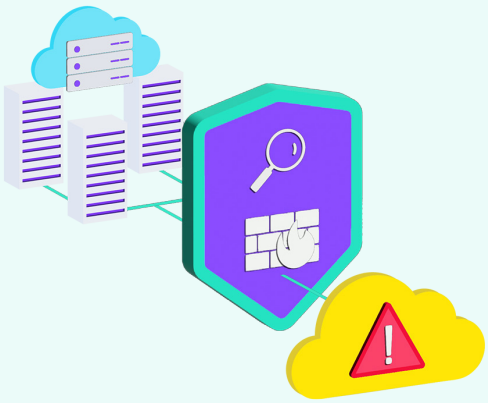
genugate Virtual

Facts & Features



High Resistance Firewall

Definition

genugate Virtual combines the rigorous security standards of genugate with the benefits of virtualization. It maintains a consistent security posture by offering advanced application-level-gateway (ALG) functionality for thorough network traffic inspection and control, distinguishing itself in virtual environments with its proven security and reliability.

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

Each instance of genugate Virtual offers a throughput capacity of up to 20 Gbit/s for TCP and 7 Gbit/s for UDP. This performance can be linearly scaled by adding additional instances, effectively increasing the total throughput capacity of your network. This flexible scalability allows you to tailor the firewall capabilities precisely to meet the evolving demands of your network infrastructure.

Reasons to Choose genugate Virtual

- Approved for the classification level German VS-NfD
- 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, SOAP, SSH, IMAP, etc.)
- Web Application Firewall (WAF)
- Geo-IP filtering for country-based network access control
- 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
- 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

SecurITy made in Germany

Excellence in Digital Security.

Key Benefits of Virtualization

Scalability: Scale your security with genugate Virtual's adaptable design, easily matching your network's evolving needs.

Rapid Deployment: Deploy genugate Virtual quickly within your existing infrastructure, bypassing the complexities of physical setups.

Reduced Physical Footprint: Switch to genugate Virtual for less reliance on physical hardware, saving space and reducing power and costs.

Strong Security: Maintain high security standards with genugate Virtual's powerful application level gateway, ensuring thorough network traffic control.

Streamlined Integration: Easily integrate and manage genugate Virtual within your existing virtual infrastructure using familiar tools.

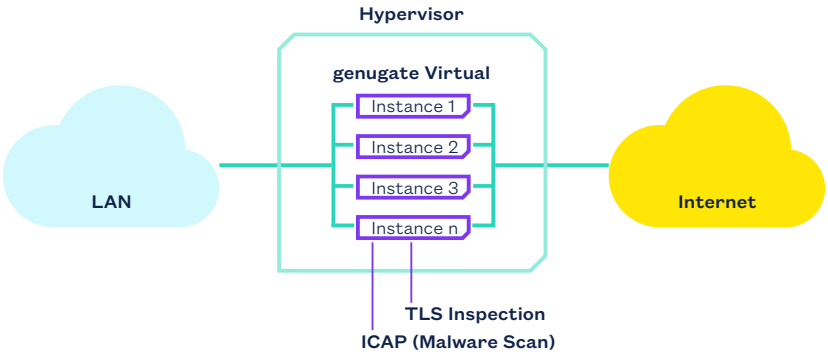
Requirements and Platform Support

Hardware Requirements: For optimal performance, a host with 4 CPU cores and 8 GB RAM is recommended for genugate Virtual.

Supported Virtualization Platforms: Fully compatible for both ESXi and KVM hypervisors, genugate Virtual fits a wide range of IT environments.

Licensing and Scalability: genugate Virtual features flexible, per-instance licensing, allowing you to scale capacity to meet your network's needs, thereby enhancing overall throughput.

Use Case



Scalable Network Security for Sensitive Infrastructures

As an application level gateway, genugate Virtual provides organizations consistent protection for their sensitive infrastructures. As a virtualized solution, it can be dynamically scaled to meet increasing performance requirements.

TLS inspection decrypts and inspects encrypted traffic, ensuring data integrity and confidentiality. ICAP support allows seemless integration with the preferred malware scanning solutions.

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 Filter			
Cloud storage	+		
Conferencing	+		
Remote access	+		
Software updates	+		
Content Filter	**WWW**	**SSH**	**FTP**
Active content	+	+	+
Request method filter	+	+	+
Malware/Virus Scanning			
ICAP interface for external malware/virus scan integration WWW, FTP, SMTP, IMAP, POP3			
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	+

High Availability (HA)

Automatic configuration distribution	+
Failover	+

More product information

Excellence in Digital Security.

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 & Destination Address (IPv4 & IPv6)	+	+	+	+	+	+	+	+	+	+	+
Group authentication	+	+	+	+	-	-	-	-	-	-	-
Time	+	+	+	+	+	+	+	+	+	+	+
Geo-IP	+	+	+	+	+	+	+	+	+	+	+
FQDN Access Control	+	+	+	+	+	+	+	+	+	+	+

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

System Management	
User Management	
User profiles	+
Administrator profiles	+
Supported languages	German, English
Administration	
Graphical User Interface (GUI)	+
Entire cluster management via primary system	+
REST-API	+
Backup	
Configuration backup	Via GUI, SSH, USB stick
System backup	SSH
Automated backups	+
Monitoring	
SNMP	+
Nagios	+

Approval by the German Federal Office for Information Security (BSI)	
German VS-NfD	+

112024-06-E

Further Information:

www.genua.eu/genugate-virtual

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