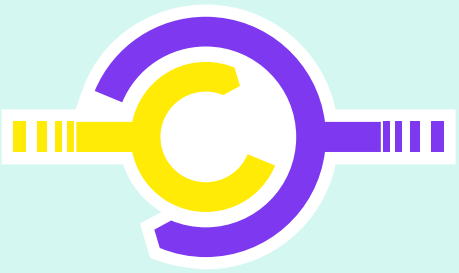
genugate Virtual

Facts & Features



High Resistance Firewall

Definition

genugate Virtual kombiniert die bewährten Sicherheitsstandards der Firewall Appliance genugate mit den Vorteilen der Virtualisierung. Sie gewährleistet eine konsistente Sicherheitsarchitektur durch ihre erweiterten Funktionen als Application Level Gateway (ALG), die eine tiefgreifende Überprüfung des Netzwerkverkehrs ermöglichen. In virtuellen Umgebungen überzeugt sie durch zuverlässige Sicherheit und hohe Verfügbarkeit.

Typische Verwendung

- Absicherung interner Netze gegen unbefugten Zugriff von außen (z. B. Internet)
- Strukturierung eines Intranets zur Einrichtung von Domänen mit unterschiedlichen Schutzmechanismen
- Schutz der Maschine-zu-Maschine-Kommunikation als Sicherheitsgateway für SOAP und Webdienste

Durchsatzmenge

Jede Instanz von genugate Virtual bietet eine Durchsatzkapazität von bis zu 5.000 Mbit/s für TCP und 7.000 Mbit/s für UDP. Diese Leistung kann durch Hinzufügen zusätzlicher Instanzen linear skaliert werden, wodurch die Gesamtdurchsatzkapazität Ihres Netzwerks effektiv erhöht wird. Diese flexible Skalierbarkeit ermöglicht es Ihnen, die Firewall-Funktionen genau auf die sich entwickelnden Anforderungen Ihrer Netzwerkinfrastruktur abzustimmen.

Gründe für genugate Virtual

- Zugelassen für den Geheimhaltungsgrad VS-NfD
- Echtes Gateway auf Anwendungsebene
- Trennung des Datenflusses und Wiederherstellung von Verbindungen (keine Verbindungstransfers)
- Proxy-Dienste für eine breite Palette von Protokollen (WWW, SMTP, SOAP, SSH, IMAP, usw.)
- Web Application Firewall (WAF)
- Schutz vor Spam und Malware
- IPv4- und IPv6-Unterstützung für die Migration und die Verwendung von zwei Protokollen
- Hohe Verfügbarkeit und erhöhte Bandbreite durch Cluster
- Protokollierung aller Netzwerkaktivitäten
- Benutzerfreundliche GUI-basierte Verwaltung
- SIEM-Integration
- Verbesserte TLS-Sicherheit für Clients und Server

Service

- Kundenservice direkt vom Hersteller
- Verwaltung des Sicherheitssystems
- Hotline Service/Update Service

SecurITy made in Germany

Die wichtigsten Vorteile der Virtualisierung

Skalierbarkeit: Skalieren Sie Ihre Sicherheit mit dem anpassungsfähigen Design von genugate Virtual, das sich problemlos an die sich entwickelnden Anforderungen Ihres Netzwerks anpassen lässt.

Schnelle Bereitstellung: Stellen Sie genugate Virtual schnell innerhalb Ihrer bestehenden Infrastruktur bereit und umgehen Sie die Komplexität physischer Setups.

Geringerer physischer Fußabdruck: Durch den Wechsel zu genugate Virtual sind Sie weniger auf physische Hardware angewiesen, sparen Platz und reduzieren Strombedarf und Kosten.

Starke Sicherheit: Bewahren Sie hohe Sicherheitsstandards mit dem leistungsstarken Application Level Gateway von genugate Virtual, das eine umfassende Kontrolle des Netzwerkverkehrs gewährleistet.

Optimierte Integration: Integrieren und verwalten Sie genugate Virtual ganz einfach in Ihre bestehende virtuelle Infrastruktur mit vertrauten Tools.

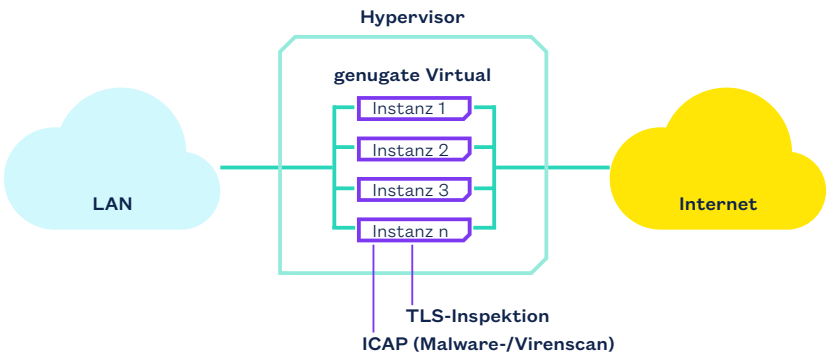
Anforderungen und Plattformunterstützung

Hardware-Anforderungen: Für eine optimale Leistung wird für genugate Virtual ein Host mit 4 CPU-Kernen und 8 GB RAM empfohlen.

Unterstützte Virtualisierungsplattformen: Durch die vollständige Kompatibilität mit den Hypervisoren ESXi und KVM eignet sich genugate Virtual für eine breite Palette von IT-Umgebungen.

Lizenzierung und Skalierbarkeit: Das flexible Lizenzmodell von genugate Virtual erlaubt die Lizenzierung kompletter Instanzen. Dies ermöglicht es, die Kapazität Stück für Stück zu erhöhen und entsprechend an die Anforderungen Ihres Netzwerks anzupassen.

Use Case



Skalierbare Netzwerksicherheit für empfindliche Infrastrukturen

Als Gateway auf Anwendungsebene bietet genugate Virtual Unternehmen konsistenten Schutz für ihre sensiblen Infrastrukturen. Als virtualisierte Lösung kann sie dynamisch skaliert werden, um steigende Leistungsanforderungen zu erfüllen.

Die TLS-Prüfung entschlüsselt und prüft den verschlüsselten Datenverkehr und gewährleistet so Datenintegrität und Vertraulichkeit. Die ICAP-Unterstützung ermöglicht eine nahtlose Integration von bevorzugten Malware-Scan-Lösungen.

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	+

Mehr Produktinfos

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 address	+	+	+	+	+	+	+	+	+	+	+
Destination address	+	+	+	+	+	+	+	+	+	+	+
Group authentication	+	+	+	+	-	-	-	-	-	-	-
Time	+	+	+	+	+	+	+	+	+	+	+

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	+

072024-04-DE

Weitere Informationen:

www.genua.de/genugate

genua GmbH
Domagkstraße 7 | 85551 Kirchheim bei München
+49 89 991950-0 | info@genua.de | www.genua.de