



genugate

High Resistance Firewall für hochsichere Netzübergänge

Technische Informationen



Inhaltsverzeichnis

1	Warum die High Resistance Firewall genugate einsetzen?	1
1.1	Das ALG als entscheidender Sicherheitsfaktor.....	1
1.2	Zugelassenes und zertifiziertes Rundum-Hochsicherheitspaket.....	1
2	Sicherheitsmerkmale der genugate	2
2.1	Mit Netz und doppeltem Boden: Mehrstufige Firewalls.....	2
2.2	P-A-P-Struktur.....	2
2.3	Firewall-Typen.....	3
2.4	Komponenten der genugate.....	4
2.5	Weitere Sicherheitsmerkmale.....	6
2.5.1	Betriebssystem.....	6
2.5.2	Vollständige Trennung am Netzübergang.....	7
2.5.3	Vollständige Analyse und Normalisierung von Anwendungsprotokollen.....	7
2.5.4	Vollständige System- und Datentransparenz.....	7
2.5.5	Erhöhter Selbstschutz durch Intrusion Detection.....	8
2.5.6	Active-Content-Filter.....	8
2.5.7	SSL-Inspektion.....	8
2.5.8	Überwachung und Protokollierung.....	8
3	Weitere wichtige Leistungsmerkmale	9
3.1	Web-Proxy.....	9
3.2	Mail-Zentrale.....	10
3.3	DNS-Server.....	10
3.4	DMZ-Betrieb.....	10
3.5	IPv4/IPv6-Misch- und Migrationsbetrieb.....	11
3.6	Skalierbarkeit und Hochverfügbarkeit.....	12
3.6.1	genugate Hardware-Varianten.....	12
3.6.2	Cluster.....	13
4	Erweiterungsmöglichkeiten	13
4.1	genuscan.....	13
4.2	genugate ScanServer.....	14
4.3	Advanced Web Categories.....	14



5	Zertifizierung und Zulassung	15
5.1	Zertifizierung.....	15
5.2	Zulassung.....	16
6	Bedienungsfreundlichkeit	16
7	Einsatzszenarien	18
7.1	Informationsverbund Berlin-Bonn (IVBB).....	18
7.2	Klüber Lubrication SE & Co. KG.....	18
8	Support und Schulungen	19
8.1	Einführung.....	19
8.2	Schulungen.....	19
8.3	Laufender Betrieb – Software Support.....	20
8.4	Laufender Betrieb – Hardware Support.....	20
8.5	Support von genugate-Vertriebspartnern.....	20



1 Warum die High Resistance Firewall genugate einsetzen?

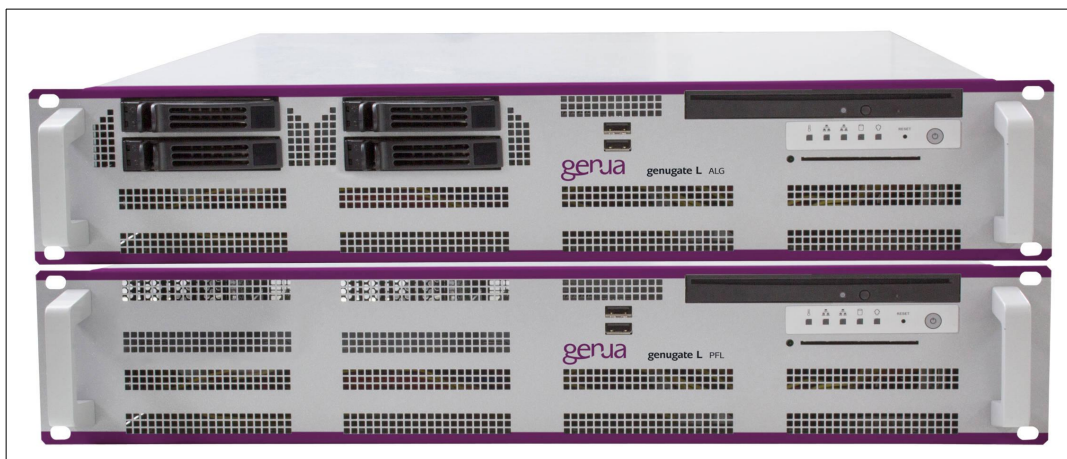
Netzwerke sind heute umfangreichen, sich verändernden Bedrohungen ausgesetzt. Paketfilter alleine reichen in der Regel nicht mehr aus, um diese Bedrohungen vollständig abzuwehren. Systembedingt sind sie nicht in der Lage, tiefer in die übertragenen Daten zu schauen, und können daher keine Malware entdecken. Eine Kombination aus Paketfilter und weiteren Sicherheitskomponenten kann den Schutz Ihrer Netzwerke deutlich erhöhen.

1.1 Das ALG als entscheidender Sicherheitsfaktor

Das Zusammenspiel von Application Level Gateway (ALG) und Paketfilter, wie bei der High Resistance Firewall genugate umgesetzt, hat sich im Vergleich zu anderen Systemen als hochwirksam erwiesen.

ALGs stellen Programme zur Verfügung, die das Protokoll der jeweiligen Applikation sprechen (z. B. HTTP, SMTP) und so die Daten auf Applikationsebene entgegennehmen, vollständig analysieren und auf Applikationsebene weiterreichen. Klassische ALGs sind z. B. Web-Proxies oder Mail-Gateways. Ein ALG kann umfangreiche Änderungen an den Daten vornehmen: So lassen sich beispielsweise aus Webseiten Plugins oder Skripte und aus Mails gefährliche Anhänge entfernen. Auch die Überprüfung verschlüsselter Verbindungen ist dabei kein Problem.

Die Weiterleitung der Daten zum eigentlichen Ziel erfolgt dann über eine neue, unabhängige Verbindung. Durch diese Trennung der Verbindungen erfolgt eine Bereinigung der Daten auf Paket- und Protokollebene, wodurch die Schutzfunktion der Firewall deutlich erhöht wird.



genugate steht für doppelte Sicherheit

1.2 Zugelassenes und zertifiziertes Rundum-Hochsicherheitspaket

Mit der genugate erhalten Sie ein vom BSI zugelassenes und nach Common Criteria in der Stufe EAL 4+ zertifiziertes Sicherheitsprodukt made in Germany.

Neben der hochwirksamen Firewall-Funktionalität können Sie mit der genugate alle wichtigen Dienste wie Mailserver, DNS-Server und Web-Proxy autonom bereitstellen. Bei der genugate handelt es sich zudem um ein robustes und hochflexibles System, das sich bei der Lösung komplexer Aufgaben im Netzwerk bewährt hat. Ein Höchstmaß an Investitionssicherheit kann genua Kunden durch umfangreichen Service, Support und konstante Produktpflege bieten.

Hochwirksames, mehrstufiges Sicherheitssystem	✓
CC EAL 4+ Zertifikat, einzige „Highly Resistant“ Firewall	✓
Inhaltliche Prüfung und Normalisierung schützt vor Malware	✓
Wichtige Webdienste unter Ihrer vollständigen Kontrolle	✓
Investitionssicherheit durch Service, Support und Produktpflege	✓
IT-Security made in Germany seit über 20 Jahren	✓

Im Folgenden erhalten Sie Informationen über die Funktionen der High Resistance Firewall genugate. Für weitere Informationen und Beratung nehmen Sie bitte zu uns Kontakt auf.

2 Sicherheitsmerkmale der genugate

2.1 Mit Netz und doppeltem Boden: Mehrstufige Firewalls

Es ist eine Binsenweisheit, die Hersteller jeglicher Software ihren Produktbeschreibungen anfügen: „Beim aktuellen Stand der Technik kann die Fehlerfreiheit der Software nicht garantiert werden.“ Wie wahr!

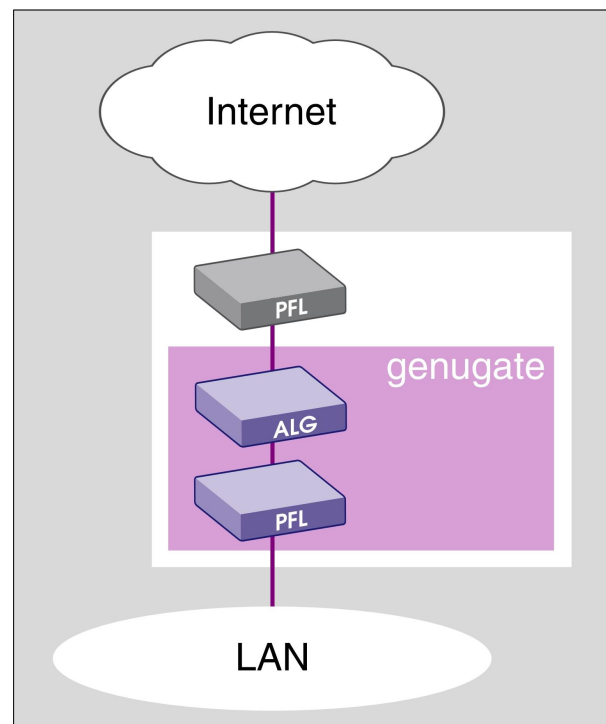
Diese Warnung gilt selbstverständlich auch für Firewalls. Nur ist in diesem Fall nicht nur ein einzelner Dienst gefährdet. Eine Schwachstelle der Firewall-Software setzt ganze Firmennetze mit vielen unterschiedlichen Diensten der Gefahr von Angriffen aus.

Die Antwort auf das Ausfallrisiko einzelner Systeme lautet Mehrfachausführung. Deshalb arbeiten z. B. in modernen Flugzeugen drei oder mehr Steuerrechner für jede Aufgabe parallel, damit der Gesamtbetrieb trotz eines einzelnen Ausfalls störungsfrei weiterläuft.

Das Gleiche gilt für Firewalls – nur mit dem Unterschied, dass die mehrfach vorhandenen Firewall-Instanzen nicht parallel arbeiten, sondern ähnlich wie die Wehranlagen einer Burg hintereinander liegen sollen. Den Weg ins Burginnere (sprich: ins interne Datennetz der Organisation) findet nur, wer alle Kontrollen besteht. Sollte eine Sperre durch einen Angriff außer Kraft gesetzt werden, so schützen die verbleibenden Verteidigungsstufen noch immer das Innere.

2.2 P-A-P-Struktur

Basierend auf den oben skizzierten Überlegungen empfiehlt das Bundesamt für Sicherheit in der Informationstechnik (BSI) den Einsatz mehrstufiger Firewalls, wenn es um die Sicherung von Datennetzen mit mittlerem oder hohem Schutzbedarf geht (www.bsi.bund.de).



Das BSI empfiehlt eine P-A-P-Firewall-Lösung

Besonders hervorgehoben wird die P-A-P-Struktur, wie sie in der Abbildung dargestellt ist. Dabei steht das Kürzel P-A-P für die Abfolge der Subsysteme Paketfilter (PFL) – Application Level Gateway (ALG) – PFL, die die Daten bei ihrem Weg durch das gesamte Firewall-System durchlaufen müssen.

Die Begriffe „Paketfilter“ und „Application Level Gateway“ wiederum bezeichnen unterschiedliche Architekturen von Firewall-Subsystemen, die weiter unten beschrieben werden.

Wichtig an dieser Stelle ist zunächst, dass unterschiedliche Firewall-Architekturen kombiniert werden. Es ist offensichtlich, dass ein Firewall-System aus mehreren gleichartigen Stufen keinen erhöhten Schutz bietet, denn bei einem erfolgreichen Angriff auf die erste, äußere Stufe ließe sich auch die zweite und jede nachgelagerte Stufe in gleicher Weise überwinden.

2.3 Firewall-Typen

Paketfilter arbeiten auf der Netzwerk- und Transportschicht-Ebene. Sie können daher Pakete aufgrund von IP-Adresse, Protokolltyp und Port-Nummer filtern. Stateful Packet Filter führen zusätzlich Informationen über den Status von Verbindungen mit und erlauben eine wesentlich intelligentere Filterung von Paketen, eine Überprüfung der Daten auf Anwendungsebene ermöglichen aber auch sie nicht.

Application Level Gateways dagegen arbeiten auf Anwendungsebene. Dedizierte Prüfprogramme – die so genannten Relays – kontrollieren und filtern die übertragenen Anwendungsdaten. Dadurch werden inhaltliche Überprüfungen z. B. auf Viren oder Active Content möglich. Darüber hinaus lassen ALGs im Gegensatz zu Paketfiltern IP-Pakete zwi-

schen den angeschlossenen Netzen niemals direkt passieren, weil dadurch weitere Angriffsformen möglich wären. Stattdessen bauen die Relays sorgfältig getrennte Verbindungen ins äußere und ins innere Netz auf.

Weitere Informationen zu Firewall-Typen bietet Ihnen eine spezielle Broschüre zu diesem Thema.

2.4 Komponenten der genugate

Die Firewall genugate wurde genau nach den Empfehlungen des BSI entwickelt. Bei ihr handelt es sich um ein zweistufiges Firewall-System: innen ein besonders stark abgesicherter Paketfilter, außen ein intelligentes ALG. Mit einem weiteren externen Paketfilter (z. B. ein Router mit entsprechenden Filterregeln) kann das System einfach zu einer dreistufigen Firewall erweitert werden. Aus der Produktpalette von genua käme als drittes Subsystem die Firewall genuscreen in Frage.

Der Paketfilter: Er steht unmittelbar vor dem internen Netz. Dieser Paketfilter lässt in der Standardkonfiguration keinerlei Verbindungsaufbauten von der Außenseite zu, sie müssen stets von innen her angestoßen werden. Bei Bedarf können gezielt Ports für den Zugriff von außen geöffnet werden. Das System ist auf die absolut notwendigen Komponenten reduziert, läuft ohne Festplatte und wird von einem USB-Stick gebootet.

Der USB-Stick kann im zertifizierten Betrieb nur auf dem ALG beschrieben werden. Anschließend muss er wieder in den PFL eingesteckt und dieser neu gestartet werden. Um die Konfiguration des PFL anzupassen, ist also ein physischer Zugriff auf die Hardware der genugate notwendig. Dies erhöht die Sicherheit des Systems wesentlich und beeinträchtigt dessen Handhabung kaum, da Änderungen am Paketfilter nach erfolgter Erstkonfiguration selten notwendig sind.

Wird auf den zertifizierten Betrieb bewusst verzichtet, können PFL-Regeländerungen auch „on the fly“ und somit ohne Reboot des PFL erfolgen. Darüber hinaus besteht die Möglichkeit, den PFL komplett ohne physischen Zugriff neu zu konfigurieren.



Das Application Level Gateway: Das ALG der genugate bietet folgende Relays und Filter:

Application Level Relays

- WWW-Relay (+SSL)
- WWW-/FTP-Caching Proxy
- FTP-Relay (+ SSL)
- SMTP-Relay (+ SSL)
- POP3-Relay
- SIP-Relay
- Telnet-Relay
- Real Audio- u. Real Video-Relay
- NNTP-Relay
- SSH-Relay
- DNS-Relay
- Web Application Firewall

Web-Filter

- Cloud Storage
- Conferencing
- Remote Access
- Software Updates

Circuit Level Relays

- TCP-Relay (+SSL)
- UDP-Relay
- IP-Relay
- Ping-Relay
- Multicast-Relay

Protokollfilter

- BGP
- DNS
- IMAP
- IPsec
- LDAP
- MSSQL
- MySQL
- PostgreSQL
- PPTP
- RDP
- SMB
- SNMPTrap
- Teamviewer
- VNC

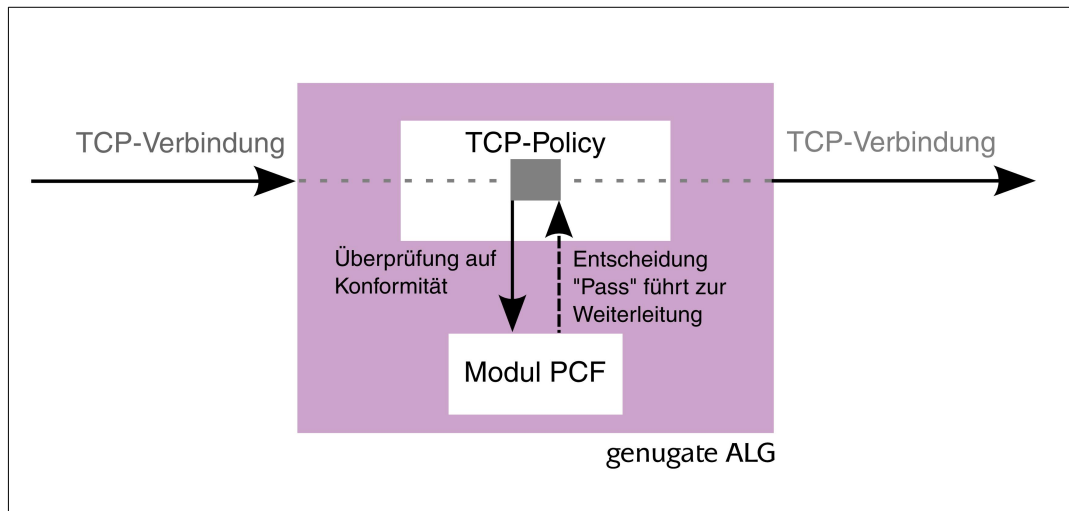
Für die tiefgreifende Analyse gängiger Anwendungsprotokolle bietet die genugate eine Reihe von **Application Level Relays**, die den Datenstrom Schritt für Schritt nachvollziehen. Eine eventuelle Verschlüsselung kann aufgebrochen, Nutzdaten können durch einen Virens Scanner überprüft werden.

Circuit Level Relays werden für unbekannte Anwendungsprotokolle verwendet. Für generische TCP- und UDP-Daten lassen sich auch individuelle Protokollkonformitätsfilter (s. u.) einrichten.

Mit **Protokollfiltern** kann ein Administrator Regeln für Anwendungen leicht konfigurieren, deren Protokolle und Ports bereits feststehen. Außerdem wird die Protokollkonformität geprüft.

Web-Filter kennen bestimmte Cloud-Anwendungen, welche über HTTP oder HTTPS laufen. Deren Verkehr wird im normalen Surf-Traffic gefunden und dann speziell behandelt. Es ist generell möglich, solche Anwendungen zu erlauben oder zu verbieten. Bei speziellen

Diensten wie etwa Cloud Storage-Anbietern (z. B. TelekomCloud, Strato HiDrive) ist es möglich, den Upload nur für zuvor verschlüsselte Dateien zuzulassen.



Ein- und ausgehende Daten durchlaufen den Prüfprozess zur Protokollkonformität

Der **Protokollkonformitätsfilter (PCF)** ermöglicht es, den Verbindungsaufbau auf Anwendungsebene innerhalb des TCP- oder UDP-Datenstroms genau zu analysieren. Damit kann zu Beginn einer entsprechenden Verbindung entschieden werden, ob diese Verbindung zulässig ist oder geblockt werden soll. Mitgeliefert werden bereits viele Definitionen von verbreiteten Standardprotokollen; eigene Erweiterungen sind über reguläre Ausdrücke möglich.

Neben den genannten Relays sind für spezielle Anforderungen weitere Optionen verfügbar. Sie können auch Port Ranges für Relays anlegen. So lassen sich über ein Relay ganze Portbereiche leiten.

2.5 Weitere Sicherheitsmerkmale

2.5.1 Betriebssystem

Minimalsystem: Beide Komponenten der genugate setzen auf das Betriebssystem OpenBSD auf, das von Anfang an mit Fokus auf Sicherheit entwickelt wird. Der Systemumfang ist auf die unbedingt notwendigen Features beschränkt. Alle potenziell gefährlichen oder für die Funktion im Firewall-Betrieb überflüssigen Bestandteile wurden entfernt, der Gesamtumfang auf das für den ALG- bzw. Paketfilterbetrieb notwendige Minimalsystem reduziert.

Kernel-Härtung: Das auf den beiden Komponenten – ALG und Paketfilter – eingesetzte Betriebssystem ist gegen Angriffe gehärtet und damit für den Einsatz auf einem Firewall-System optimiert.



Verschiedene Betriebsmodi: Neben dem normalen Betriebsmodus verfügt genugate über einen Wartungsmodus, in dem kein Netzwerk zur Verfügung steht. Nur in diesem Modus ist es möglich, neue Softwareversionen und Patches einzuspielen und damit das Betriebssystem zu verändern. Angriffe auf die Systemintegrität im laufenden Betrieb werden so ausgeschlossen.

Unveränderbare Dateien: Protokolldateien können im laufenden Betrieb nicht gelöscht und bestehende Einträge in diesen Dateien nicht geändert werden. Damit gelten sie als revisionssicher. Auch system- und sicherheitsrelevante Daten wie Gerätedateien oder Filterregeln können im laufenden Betrieb nicht geändert werden. Der Administrator benötigt für solche Änderungen physischen Zugang oder eine serielle Konsole im Wartungsmodus des Systems.

Abgeschottete Umgebungen (Cage): Für alle Relays des ALGs werden separate Umgebungen eingerichtet, in denen Netzwerkverbindungen bearbeitet werden. Die geschützten Umgebungen sind vom Rest des Systems und von anderen Umgebungen abgekapselt und schränken unerwünschte Zugriffe auf Systemressourcen oder Konfigurationsinformationen ein.

2.5.2 Vollständige Trennung am Netzübergang

Die genugate fungiert als vollwertiger Empfänger der Datenpakete, fügt diese zusammen und kann somit eine vollständige Inhaltsanalyse durchführen. Anschließend gibt sie nur die Nutzdaten an den jeweiligen Empfänger weiter. Angriffe auf Netzebene sind somit ausgeschlossen. Auch die üblichen Methoden zur Umgehung von Next Generation Firewalls und Intrusion Detection Systemen werden durch das neue Zusammensetzen des Datenstroms verhindert. Bei Einführung von IPv6 wird die Netztrennung noch wichtiger, da wieder Fehler in den IP-Stacks auftauchen. Die Migration von IPv4 auf IPv6 wird durch die Terminierung der Verbindungen auf dem ALG einfach.

2.5.3 Vollständige Analyse und Normalisierung von Anwendungsprotokollen

Wie der Name schon sagt, befindet sich das Application Level Gateway auf der richtigen Ebene, um Anwendungen zu analysieren. Die Relays der genugate können bei Mehrdeutigkeiten in die Anwendungsprotokolle eingreifen und diese normalisieren. Unerwünschte Inhalte werden sicher gestoppt. Next Generation Firewalls, die im Wesentlichen auf Paketfiltern basieren, prüfen die passierenden Datenpakete nur stichprobenweise. Diese unvollständige Prüfung können Angreifer gezielt ausnutzen.

2.5.4 Vollständige System- und Datentransparenz

genugate arbeitet nach festen und klaren Regeln. Die Umsetzung ist unabhängig geprüft und kann auf Wunsch im Quellcode nachvollzogen werden. Ein Calling-Home zum Hersteller und dynamische Updates, wie bei Intrusion-Detection-Systemen und Next-Generation-Firewalls üblich, sind nicht nötig. Der Kunde hat seine Firewall und dadurch auch sein Netzwerk stets vollständig unter eigener Kontrolle.

2.5.5 Erhöhter Selbstschutz durch Intrusion Detection

genugate bietet eine kontinuierliche System- und Prozessüberwachung, so dass außergewöhnliche Zustände erkannt werden. Versucht ein Angreifer beispielsweise, durch massives Senden von Netzwerkpaketen die Sicherheitsfunktionen der genugate außer Kraft zu setzen (Überlast), wird dies registriert und eine in der Konfiguration festgelegte Aktion eingeleitet. So genannte Port-Scans werden durch einen speziellen Monitor überwacht.

2.5.6 Active-Content-Filter

Für die Dienste E-Mail, WWW und News beinhaltet genugate einen Filter, der die folgenden aktiven Inhalte blockieren kann:

- Java
- JavaScript
- VB-Script
- Active-X

Aktive Inhalte können äußerst wirkungsvoll für Angriffe eingesetzt werden, eine Filtermöglichkeit ist deshalb unverzichtbar. Weiterhin ist eine Filterung von Cookies, MIME-Types sowie nach URLs möglich.

2.5.7 SSL-Inspektion

Mit der genugate ist es möglich, verschlüsselte SSL-Verbindungen auf dem ALG zu analysieren. Dieser Mechanismus kann in Verbindung mit SMTP-, TCP-, WWW- und FTP-Policies verwendet werden. Dabei werden die Verbindungen auf dem ALG entschlüsselt, die Verbindungen zwischen Client und ALG einerseits sowie ALG und Server andererseits bleiben weiterhin verschlüsselt. Dadurch ist es möglich, auch diese Verbindungen auf Viren und aktive Inhalte zu untersuchen.

2.5.8 Überwachung und Protokollierung

Protokollierung: Das ALG nimmt eine ausführliche Protokollierung aller erlaubten und abgewiesenen Verbindungen vor, die online ausgewertet und bewertet werden. Zur Beweissicherung können die Protokolle auch archiviert oder an einen zentralen Loghost weitergeleitet werden. Protokolliert werden u. a. Proxy-Nutzung, Aktivitäten der Systemadministratoren und Regelverletzungen.

Systemüberwachung: Alle wichtigen Systemfunktionen der genugate werden laufend überwacht und bei Fehlfunktion automatisch wiederhergestellt. Die Integrität aller statischen Dateien wird täglich überprüft.

Hardware-Monitoring: Kontinuierlich überprüfen integrierte Sensoren die Hardware der Firewall genugate. Bei Ausfall einer Komponente oder Überschreiten festgelegter Grenzwerte einzelner Parameter wird Alarm ausgelöst.

Zusammenarbeit mit SIEM-Lösungen : Logdateien auf einzelnen Komponenten auszuwerten, reicht oft nicht aus. Erst durch die Korrelation der Ereignisse auf verschiedenen



Geräten entsteht ein aussagekräftiges Lagebild. "Security Information and Event Management" (SIEM) hilft, einen Überblick über die Sicherheitslage eines Netzwerks zu gewinnen.

In diesem Zusammenhang stellt die Firewall eine wichtige Informationsquelle dar, da die gesamte externe Kommunikation über diese läuft. Die genugate bietet ihre Log-Meldungen im standardisierten Syslog-Format an, alle Log-Meldungen sind klassifiziert und dokumentiert. Die Firma IBM hat ein "Device Security Module" (DSM) für ihr SIEM-Produkt QRadar geschrieben, mit dem die Log-Meldungen automatisch erkannt werden. Andere Systeme lassen sich manuell einbinden.

Durch externes Logging bietet die genugate die Möglichkeit, die lokale Last durch Log-Aufkommen und Suchanfragen zu reduzieren. Die Auswertung wird durch spezialisierte Anbieter vorgenommen, die darüber hinaus die Daten aller Geräte analysieren und aggregieren können. Dadurch ist eine Bewertung der Sicherheit der gesamten IT-Organisation möglich.

3 Weitere wichtige Leistungsmerkmale

Sollen aus Sicherheitsgründen wichtige Dienste wie Mail oder DNS nicht ausgelagert werden, können diese mit der genugate in einer sicheren Grundausführung autonom angeboten werden.

3.1 Web-Proxy

Zur Absicherung des HTTP- und HTTPS-Protokolls kommt ein eigenes WWW-Relay zum Einsatz, in welches jahrelange Erfahrung mit nicht RFC-konformen Web-Servern und -Clients eingeflossen sind. Das World Wide Web und sein Protokoll gehören zu den dynamischsten und am schlechtesten programmierten Internetanwendungen. Als echter Web-Proxy hat das genugate die Interpretationshoheit über das Protokoll und kann in Abwägung zwischen Benutzbarkeit und Sicherheit die meisten Fehler korrigieren.

Auf Inhaltsebene lassen sich die Daten auf Viren scannen oder aktive Inhalte entfernen. Viele detaillierte Anwendungs- und Inhaltsfilter stehen zur Verfügung. Wenn gewünscht, lässt sich die SSL-Verschlüsselung des HTTPS-Protokolls aufbrechen, um auch diesen Kanal für Malware zu blockieren.

Um die Konfiguration gängiger Internetanwendungen zu vereinfachen, werden diese vom Anwendungsfiler erkannt. Dort lässt sich auf Anwendungsebene festlegen, was etwa mit Skype, Cloud-Diensten oder Teamviewer geschehen soll. Diese erweiterte Analyse ist notwendig geworden, da sich viele Anwendungsprotokolle zur Umgehung einfacher Paketfilter-Firewalls als HTTP- oder HTTPS-Verkehr tarnen.

Als Ergänzung zum WWW-Relay steht ein Squid als Web-Cache zur Verfügung. Dadurch lässt sich die Internetbandbreite reduzieren oder auch eine komplizierte Farm von Web-Servern einbinden. Die gewohnten Squid-ACLs bieten dem erfahrenen Administrator alle Möglichkeiten.

3.2 Mail-Zentrale

Das genugate kann nicht nur das SMTP-Protokoll nachvollziehen, sondern auch als vollständiger Mail-Server dienen. Beide Betriebsmodi unterstützen selbstverständlich SSL, um den Mail-Transport abzusichern. Je nach Anwendungsfall können wir flexibel auf Kundenanforderung reagieren.

Existiert bereits eine Mail-Infrastruktur, werden die SMTP-Verbindungen zum vorhandenen Mail-Server durchgeleitet. Dabei werden die Mails inhaltlich auf Viren geprüft, auf Protokollebene findet eine SPAM-Abwehr statt, nicht erlaubte Sender und Empfänger werden gefiltert.

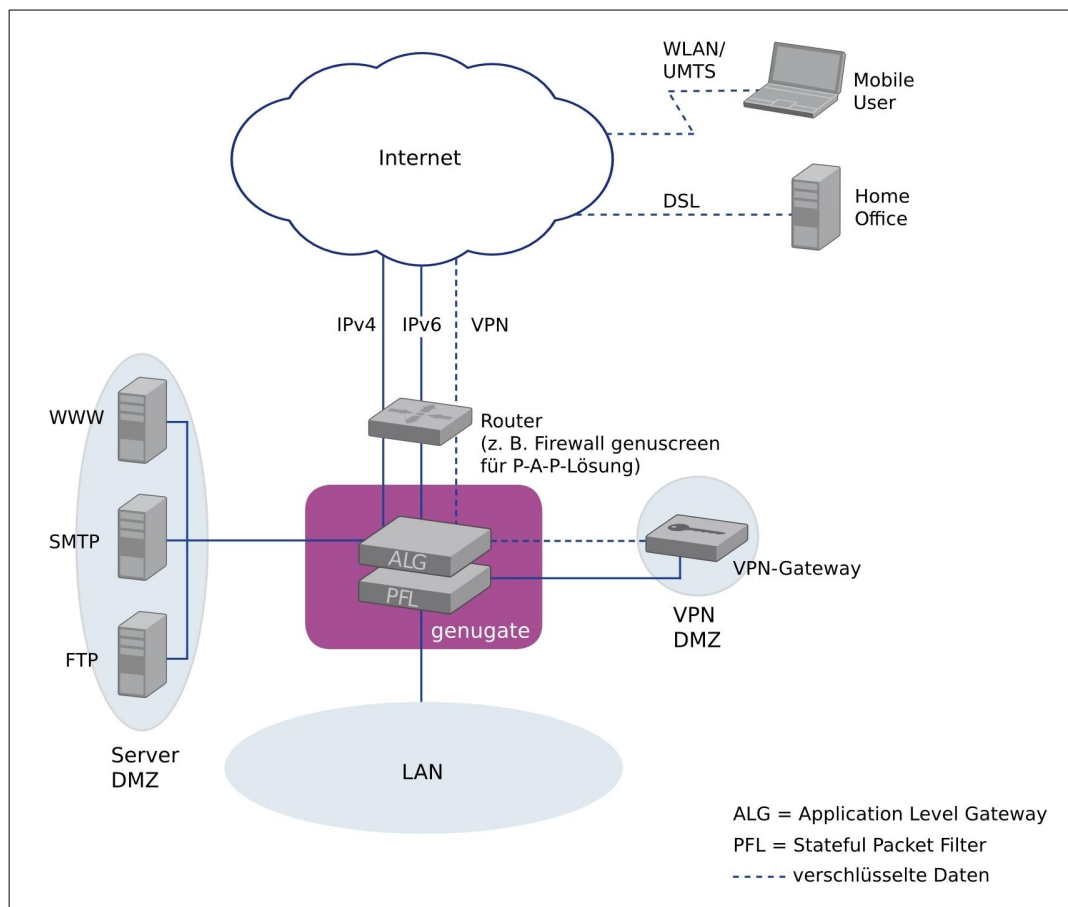
Im Betrieb als Mail-Server hingegen wird die Mail vom genugate angenommen, die Hoheit zur Weiterverteilung liegt bei der Firewall. Das erlaubt tiefgreifende Analysen, so können z. B. auch Attachments anhand unterschiedlicher Kriterien aus der Mail herausgeschnitten werden. Virenverseuchte Teile der Mail können durch individuelle Fehlernachrichten ersetzt werden. Es ist eine Authentisierung möglich, aktive Inhalte können verboten werden. Auch kann ein Mail-Routing eingerichtet werden, verdächtige Mails werden in eine Quarantäne verschoben. Die Einsatzvarianten sind nahezu unbegrenzt, das genugate kann einen komplexen Mail-Server einsparen.

3.3 DNS-Server

Neben der Möglichkeit zur reinen Prüfung und Weiterleitung der DNS-Requests, kann auch ein kompletter DNS-Server eingerichtet werden. Dieser integriert sich in den Regelsatz der Firewall. Intern kommen Name Server Daemon (NSD) und Unbound zum Einsatz, mit denen sich alle Möglichkeiten eines autoritativen und rekursiven DNS-Servers einfach einrichten lassen. Es besteht die Möglichkeit zu Zonentransfers und Domain Name System Security Extensions-Validierung (DNSSEC). Dadurch ist sichergestellt, dass nur valide Anfragen die genugate passieren. Cache und Zonenverwaltung sind bereits im Produkt enthalten und ersetzen zusätzliche Nameserver.

3.4 DMZ-Betrieb

Als zweistufiges System ermöglicht die Firewall genugate den einfachen Aufbau von demilitarisierten Zonen (DMZ), aus denen heraus Sie Dienste im Internet anbieten können, wie z. B. WWW- oder FTP-Server.



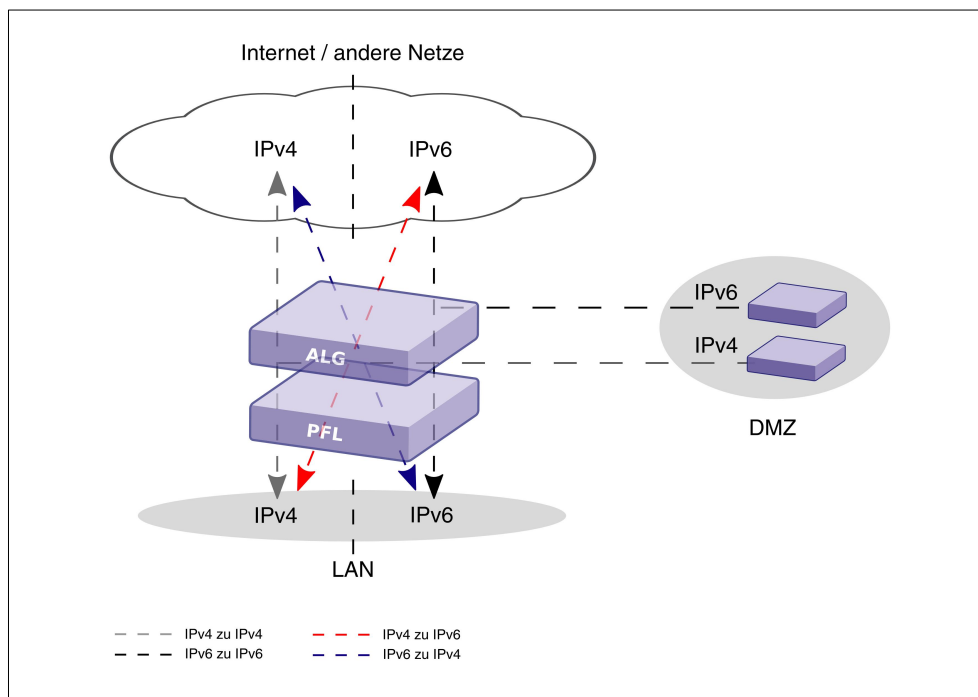
Maßgeschneiderte Sicherheitszonen für alle Anforderungen

Auch solche Server müssen so weit wie möglich vor Angriffen aus dem Internet geschützt werden, sollten aber aus Sicherheitsgründen nicht im internen Netz platziert sein. Daher ist die Einrichtung separater DMZ mit angepasster Sicherheitsrichtlinie, wie in der Abbildung dargestellt, zu empfehlen.

3.5 IPv4/IPv6-Misch- und Migrationsbetrieb

Ab Version 7.0 kann genugate sowohl mit IPv4- als auch mit IPv6-Adressen und -Netzen umgehen. Gerade im Übergangsbetrieb bei der Einführung von IPv6 ist die Unterstützung des Mischbetriebs besonders wichtig.

Damit ist auch die Umsetzung der IP-Versionen untereinander möglich. Eine flexible Mischung von IPv4 und IPv6 durch genugate gewährleistet eine einfachere Migration, auch wenn Clients und Server nur jeweils eine der beiden Versionen unterstützen. Eine mögliche Anwendung: Das interne Netz verbleibt im IPv4-Betrieb, jedoch können mit Hilfe der Protokollumsetzung über IPv6 erreichbare Dienste im Internet genutzt werden. Das ALG ermöglicht also eine IPv6-Nutzung ohne IPv6-Migration des eigenen Netzes. Eine noch flexiblere Nutzung von IPv4- und IPv6-Diensten zeigt die folgende Grafik:



Verwendung von IPv4 und IPv6 im LAN und in der DMZ

3.6 Skalierbarkeit und Hochverfügbarkeit

3.6.1 genugate Hardware-Varianten

Die genugate-Modellreihe enthält verschiedene Hardware-Varianten, unter denen Sie entsprechend der benötigten Datendurchsatzraten und der gewünschten Hardware-Redundanz auswählen können.

genugate S: Dieses System stellt ein preiswertes Einstiegsmodell für kleinere Unternehmen oder Filialen mit geringem Übertragungsvolumen dar.

genugate M: Dieses Modell ist die Lösung für mittlere Volumina.

genugate L: Dieses Modell ist die High-End-Variante der genugate-Reihe.

Alle genugate-Varianten sind durch zusätzliche Interfaces erweiterbar. Die Software der genugate ermöglicht VLAN-Trunking und Link-Aggregation auf allen Schnittstellen.

Alle Systeme werden auf Industrie-PC-Hardware in 19" Technik realisiert. Die Geräte benötigen bis zu vier Höheneinheiten. Zu beachten ist, dass der Serverschrank eine ausreichende Tiefe aufweisen sollte, um die Systeme aufzunehmen.

Da genua die Ausstattung der Hardware-Varianten (z. B. den CPU-Typ) laufend der technischen Entwicklung anpasst, unterliegen diese Daten steten Veränderungen. Die aktuelle technische Ausstattung erfahren Sie von unseren Vertriebsmitarbeitern oder über ein spezielles Hardware-Datenblatt.



3.6.2 Cluster

Für die meisten Unternehmen ist heute eine ständige Internet-Verfügbarkeit unverzichtbar. In diesen Fällen stellen Firewall Cluster die Lösung dar. Ein Cluster besteht aus mehreren genugates, die mit einer speziellen Software – dem Hochverfügbarkeitsmodul – ausgestattet sind. Für den Anwender sieht ein Cluster wie eine einzige Maschine mit mehreren Internet-Adressen aus.

Eine „Active/Active“ Cluster-Lösung zeichnet sich durch Hochverfügbarkeit und Lastverteilung aus: Die Firewalls sind gemeinsam in die laufenden Prozesse eingebunden und teilen sich die Aufgaben (Lastverteilung). Darüber hinaus überwachen sich die Systeme gegenseitig. Fällt ein System aus, übernimmt ein anderes System dessen Aufgaben automatisch (Hochverfügbarkeit).

Diese Lösung hat viele Vorteile:

- Alle für die Hochverfügbarkeit eingesetzten Systeme können im Normalfall weitere Aufgaben übernehmen.
- Ein manuelles Eingreifen beim Ausfall eines Systems ist nicht notwendig.
- Der Cluster kann nach Bedarf beliebig erweitert werden (Skalierbarkeit).

Der letztgenannte Vorteil wird immer wichtiger: Unternehmen, die das Internet intensiv nutzen, benötigen immer mehr Bandbreite. Leitungen kann man rasch zukaufen, doch die Firewalls lassen sich häufig nicht einfach an die höheren Bandbreiten anpassen. Durch parallele Anordnung mehrerer genugates in hochverfügbaren Clustern mit Load Sharing ist unsere Hardware praktisch für alle Anforderungsvolumina geeignet.

Die Cluster-Software sorgt dafür, dass alle genugate-Knoten parallel arbeiten. Sie verteilt Konfigurations- und Zustandsdaten des Clusters an alle Komponenten und hält sie dort auch aktuell. Wird ein genugate aus dem Cluster entfernt, übernehmen die anderen genugates automatisch die Aufgaben der entfernten Komponente.

Auch die Administration des Clusters erfolgt zentral auf dem Master-System übersichtlich per Web-Browser. Die Cluster-Möglichkeit muss nicht wie bei anderen Herstellern extra lizenziert werden. Die Software von genugate hat dieses Feature fest integriert. Also benötigen Sie lediglich die gewünschte Zahl weiterer genugate-Komplettssysteme.

4 Erweiterungsmöglichkeiten

In diesem Abschnitt werden Erweiterungen der Firewall-Modelle beschrieben, die zusätzlich zu dem im vorangegangenen Abschnitten beschriebenen Hochverfügbarkeits-Modul zur Verfügung stehen.

4.1 genusan

genusan ist eine fest integrierte Zusatzsoftware für die Firewall genugate, die eine Schnittstelle zu einem Virens Scanner realisiert. genusan kann die Inhalte folgender Dienste zur Überprüfung an einen Virens Scanner weiterleiten:

- SMTP
- POP3
- WWW
- FTP
- NNTP

Eintreffende Daten werden von genuscanner in einem so genannten Cage bearbeitet, einem abgeschotteten Bereich im Dateisystem der Firewall. Die Daten werden dort für den Virenschanner aufbereitet, indem sie gegebenenfalls entpackt und Archive in einzelne Dateien zerlegt werden. Diese Aufbereitung wird – sofern nötig – auch rekursiv durchgeführt.

Wenn der Scanner Viren entdeckt, werden von genuscanner entsprechende Alarmmeldungen an den Empfänger und u. U. an den Absender versendet. Die virenverseuchten Daten werden, soweit es E-Mail betrifft, von genuscanner im abgesicherten Bereich zurückgehalten. Sie können dort einer weiteren Analyse unterzogen werden. Nur Daten, in denen keine Viren gefunden wurden, leitet genuscanner an den Anwender weiter. genuscanner arbeitet mit dem Virenschanner Antivir Professional für genugate der Avira GmbH zusammen.

4.2 genugate ScanServer

Mit dem ScanServer kann das Virenschanning von der genugate auf einen externen Rechner ausgelagert werden. Dort arbeitet genuscanner wie oben beschrieben. genugate schickt die zu überprüfenden Daten an den externen ScanServer und erhält von diesem die entsprechenden Ergebnisse zurück. Dadurch wird die Firewall von den Scan-Aufgaben entlastet.

Der Produktumfang von genugate ScanServer umfasst das Betriebssystem, die Anwendungssoftware von genua inkl. genuscanner und die Lizenz. Der genugate ScanServer wird auf dem genua Application-Server L angeboten.

Alternativ zum ScanServer besteht die Möglichkeit, via ICAP-Schnittstelle Scanner-Lösungen von Drittanbietern einzubinden.

4.3 Advanced Web Categories

genugate ermöglicht die Kontrolle von WWW-Zugriffen aus den internen Netzen auf das Internet anhand eines sehr leistungsfähigen Kategorienfilters. Dieser Filter ordnet jeder aufgeführten URL charakterisierende Kategorien zu (z. B. Kriminelles, Drogen oder jugendgefährdende Seiten), die vom Administrator individuell freigegeben und gesperrt werden können. Darüber hinaus ist auch eine manuelle Freigabe oder Sperrung einzelner Webseiten möglich.

Die URL-Filterlisten von Advanced Web Categories werden mehrfach täglich mit Updates versorgt. genugate enthält standardmäßig eine Schnittstelle zur Benutzung von Advanced Web Categories.



5 Zertifizierung und Zulassung

5.1 Zertifizierung

Vertrauen ist gut, Kontrolle ist besser. Aus diesem Grund legt genua schon seit vielen Jahren auf die Produkt-Zertifizierung durch staatlich anerkannte Stellen großen Wert.

Bereits 2002 erhielt die genugate-Version 4.0 als erste Firewall überhaupt vom Bundesamt für Sicherheit in der Informationstechnik (BSI) ein ITSEC-Zertifikat der Stufe „E3 hoch“. Seitdem sind alle Hauptversionen dieses Produktes vom BSI zertifiziert worden. Seit September 2006 verfügt die genugate über ein Common Criteria-Zertifikat der Stufe EAL 4+.

Die Common Criteria – abgekürzt CC – stellen ein internationales Standardverfahren zur Evaluierung von IT-Sicherheitssystemen dar. In der Evaluationsstufe EAL 4 müssen u. a. eine detaillierte Design-Dokumentation sowie der Quellcode vorgelegt werden, so dass Hintertüren und Unsauberkeiten ausgeschlossen werden können. Die Wirksamkeit der definierten Sicherheitsfunktionen und Mechanismen ist im Detail durch automatisierte Tests nachzuweisen, und der Hersteller muss qualifizierte Prozessstandards in der Produktentwicklung und der Qualitätssicherung belegen.

So unscheinbar das Zusatzsymbol „+“ in der Zertifizierungsstufe EAL 4+ auch erscheinen mag, im Falle der genugate verbirgt sich dahinter eine entscheidende Erweiterung: Das BSI hat der genugate seit der Version 6.0 das Attribut AVA_VAN.5 zuerkannt, das die Anforderungen der Evaluationsstufe EAL7 erfüllt. Damit ist genugate die weltweit einzige Firewall, die als „highly resistant“ (widerstandsfähig gegen Angreifer mit hohem Potenzial) zertifiziert wurde.

Bei einer Zertifizierung nach CC legt der Hersteller fest, welche Sicherheitsziele und Sicherheitsfunktionen zertifiziert werden. Ohne Aussage über die zertifizierten Sicherheitsfunktionen kann daher die Qualität des Zertifikats nicht beurteilt werden.

Bei genugate wurden alle wichtigen sicherheitsrelevanten Komponenten des mehrstufigen Firewall-Systems bis hin zum Betriebssystem in die Zertifizierung einbezogen. Da es sich um ein zertifiziertes Komplettsystem handelt, hat der Kunde die Gewissheit, dass die Sicherheit des Systems nicht durch Schnittstellenprobleme, z. B. zwischen Betriebssystem und Firewall-Software, beeinträchtigt wird.

Bei der Anwendung formaler Sicherheitsverfahren oder bei Beachtung einer technischen Revision ist ein zertifiziertes System ein fast unverzichtbarer Bestandteil des Sicherheitskonzeptes.

Die Version genugate 9.0 hat das Zertifizierungsverfahren nach CC 3.1 in der Prüfstufe EAL 4+ erfolgreich durchlaufen. Die Unterstützung des IPv6-Standards ist einbezogen.

Über Details zur Zertifizierung nach CC informieren wir Sie gerne. Dazu halten wir auch eine spezielle Broschüre für Sie bereit.

5.2 Zulassung

Die High Resistance Firewall genugate erfüllt die Geheimschutzanforderungen der Verwaltungsvorschrift VSA (Verschlusssachenanweisung des Bundesministeriums des Innern) und ist zum Schutz eingestufeter Netze einsetzbar. Die Zulassung umfasst VS-NfD, RESTREINT UE/EU RESTRICTED und NATO RESTRICTED.

6 Bedienungsfreundlichkeit

Bei der Entwicklung der genugate-Modellreihe wurde großer Wert auf Bedienungsfreundlichkeit gelegt. Eine Vielzahl von Eigenschaften ermöglicht die einfache und bequeme Nutzung im Alltagseinsatz. Dabei wurde auf eine funktionale Benutzeroberfläche Wert gelegt, die dem Administrator direkten Zugriff auf wichtige Funktionen erlaubt.

Integration von Hardware, Betriebssystem und Firewall-Software: genugate ist ein vollständig integriertes Firewall-Gesamtsystem mit aufeinander abgestimmten Hardware-, Betriebssystem-, Sicherheits- und Konfigurations-Komponenten. Die allgemein verbreiteten Kompatibilitätsprobleme zwischen Komponenten verschiedener Hersteller werden in den Entwicklungslabors von genua und nicht im Produktivumfeld des Kunden gelöst. Installations- und Konfigurationszeiten verkürzen sich so erheblich.

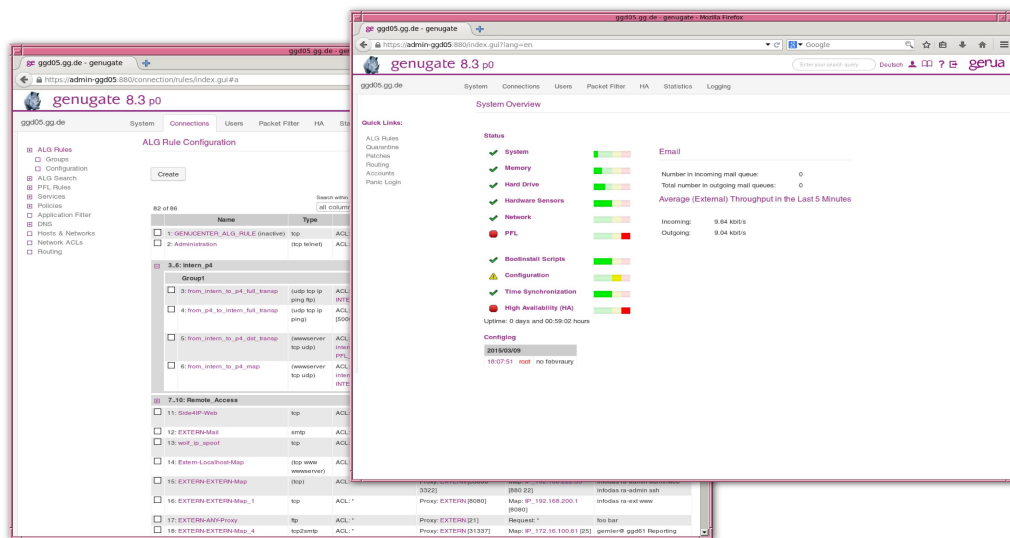
Eine Benutzeroberfläche für zwei Firewalls: Der Paketfilter und das ALG werden über ein einheitliches GUI bedient. Einmal erstellte Netzwerkobjekte und Policies können für beide Komponenten verwendet werden. Bei der Administration bemerken Sie kaum, dass Sie es mit zwei Firewall-Systemen zu tun haben.

Konfiguration und Pflege mittels Web-Browser: Sämtliche Einstellungen lassen sich mit Hilfe eines Browsers erledigen. Der Zugriff erfolgt dabei über eine verschlüsselte HTTPS-Verbindung, die zur weiteren Sicherheit auch auf eine dedizierte Netzwerkschnittstelle (das Admin-Interface) beschränkt werden kann.

Kontrolle wichtiger Web 2.0-Dienste per Mausklick: Diese Funktion ermöglicht es Administratoren, den Zugriff auf verbreitete Anwendungen wie Skype oder Cloud-Dienste schnell und einfach zu unterbinden oder an Bedingungen zu knüpfen.

Musste man bisher die Funktionsweise der jeweiligen Internet-Dienste verstehen, um die Firewall entsprechend zu konfigurieren, bringt die genugate dieses Anwendungswissen seit der Version 8.1 schon mit: Der Administrator kann einfach zentral festlegen, was er erlauben möchte und was nicht. Anwendungen wie Skype, Dropbox, Sky Drive und Team-Viewer werden bereits unterstützt, die Liste wird um weitere wichtige Dienste erweitert.

Umfangreiches Hilfesystem: Die in das GUI integrierte Online-Hilfe unterstützt Sie bei allen Aufgaben. Innerhalb der Online-Hilfe kann zusätzlich das Handbuch im PDF-Format angezeigt werden.



Grafisches User Interface (GUI)

Korreliertes Status-GUI: Auf einen Blick sehen Sie Tagesstatistiken zur Prozessorlast sowie zur Auslastung der Festplatten, des Speichers und der Hardware-Sensoren.

Konfigurationslog: Alle Änderungen an der Konfigurationsdatenbank werden protokolliert und in einem speziellen Bereich übersichtlich angezeigt. Sie erhalten sowohl eine Übersicht als auch Detail-Informationen, so dass alle genannten Aktionen vollständig nachvollziehbar sind.

Management Reports: Die Firewall erstellt Reports, bei denen Sie einstellen können, welche Informationen einfließen.

Intelligent Recovery System: Die Gesamtkonfiguration des Systems ist in einer Konfigurations-Datenbank, der so genannten Registry, gespeichert. Mit dem Intelligent Recovery System kann die Konfiguration des Systems aus dieser Registry wieder restauriert werden. Dasselbe Konzept wird für Upgrade-Prozeduren verwendet. Die Konfigurations-Datenbank kann auf einem USB-Stick gespeichert werden. Mit der Installations-CD-ROM und der gespeicherten Konfigurations-Datenbank können Sie genugate innerhalb weniger Minuten komplett neu aufsetzen.

„Set and forget“: IT-Sicherheit setzt Systemstabilität und Zuverlässigkeit voraus. Auch sollte in der IT-Abteilung kein zusätzliches Personal benötigt werden, das sich schwerpunktmäßig um die Firewall kümmern muss. Von Anwendern der High Resistance Firewall genugate erhalten wir die Rückmeldung, dass die Systeme über das übliche Einspielen von Updates und Patches hinaus ausgesprochen pflegeleicht und ressourcenschonend ihren Dienst verrichten.

7 Einsatzszenarien

7.1 Informationsverbund Berlin-Bonn (IVBB)

Als die deutsche Bundesregierung ihren Sitz nach Berlin verlegte, blieben viele Dienststellen der Ministerien in der vormaligen Hauptstadt Bonn zurück. Um den reibungslosen und schnellen Informationsaustausch zwischen beiden Standorten sicherzustellen, richtete die Bundesregierung den Informationsverbund Berlin-Bonn (IVBB) ein. An diese interne Daten-Autobahn sind alle Dienststellen der obersten Bundesbehörden angebunden – vom Präsidialamt über das Kanzleramt und alle Ministerien bis hin zum Rechnungshof.

Der IVBB ist zudem über zentrale Knotenpunkte an das Internet angeschlossen und bietet allen Behörden somit Zugang zum weltweiten Web. Für diese Übergänge vom internen Behördennetz zum öffentlichen Internet gelten hohe Sicherheits- und Leistungsanforderungen. Das zuständige Bundesamt für Sicherheit in der Informationstechnik (BSI) stellte für die dort einzusetzenden Firewalls folgenden Forderungskatalog auf:

- Hochwertige Zertifizierung der Sicherheitsleistung nach den internationalen Standards ITSEC oder Common Criteria (CC)
- Garantierte Verfügbarkeit des Systems von 99,93 Prozent
- Hoher Datendurchsatz zur schnellen Internet-Anbindung aller obersten Bundesbehörden
- Cluster-Fähigkeit zur flexiblen Anpassung an höhere Leistungsanforderungen

Diese Anforderungen erfüllt die genugate, inzwischen sind 24 Systeme beim IVBB im Einsatz. Alle Aufgaben sind auf mehrere Firewalls verteilt, die in Clustern zusammenarbeiten. Sollte ein System ausfallen, übernehmen die anderen sofort dessen Aufgaben. Die Cluster können beliebig erweitert und somit jederzeit an höhere Leistungsanforderungen angepasst werden. Das hohe Support-Level von genua sowie die Bereitschaft zur flexiblen Produkthanpassung sind sicherlich weitere Gründe, die für die genugate sprechen.

7.2 Klüber Lubrication SE & Co. KG

Mit leistungsstarken Speziialschmierstoffen und vielfältigem Service bietet Klüber Lubrication seinen Kunden aus nahezu allen Industriebereichen Lösungen, um selbst an extrem belasteten Stellen die Reibung zu minimieren. Der führende Hersteller von Speziialschmierstoffen mit rund 1.800 Mitarbeitern gehört zur Freudenberg Gruppe, Weinheim.

Aktivitäten an Standorten in über 30 Ländern und mit Geschäftspartnern in aller Welt erfordern die ständige Datenkommunikation. Diese Kommunikationswege müssen zuverlässig funktionieren und einfach zu administrieren sein.

Wichtig ist dabei die IT-Sicherheit: Die Geschäftsdaten müssen vor unbefugten Zugriffen oder Verlust unbedingt geschützt werden. Klüber Lubrication setzt hier auf zentrale Hubs, die mit High Resistance Firewalls gesicherte Internetzugänge anbieten. Hier müssen unbefugte Zugriffe, Spam, Viren und sonstiger Schadcode zuverlässig abgeblockt werden.



An dieser Stelle setzt Klüber Lubrication Firewalls des Typs genugate ein. Durch die zweistufige Konstruktion lassen sich ohne weiteres Equipment separate Sicherheitszonen bilden: Server, die Dienste im Internet anbieten wie Websites, Kundenportale oder Einwahlknoten für mobile Anwender, kommen in die so genannte demilitarisierte Zone (DMZ).

Bereits seit 1999 arbeitet Klüber Lubrication mit genua zusammen. Neben einer starken Sicherheitsleistung ist der Kundenservice direkt vom Hersteller ein wichtiges Argument, der die Administratoren der Klüber-IT bei vielen Aufgaben entlastet.

8 Support und Schulungen

8.1 Einführung

Installations- und Konfigurations-Service: genua und spezialisierte Partner unterstützen Sie auf Wunsch bei der Installation, Konfiguration und Inbetriebnahme Ihrer genugate. Dabei werden die Administratoren ausführlich in die Benutzung und Pflege eingewiesen. Falls Sie es wünschen, erstellen wir Ihnen zuvor ein Feinkonzept für Ihren sicheren Internet-Anschluss.

Anfangs-Support: Die genugate-Produktreihe ist so programmiert und dokumentiert, dass die Inbetriebnahme und der laufende Betrieb keinerlei Schwierigkeiten bereiten sollten. Wenn Sie dennoch Fragen haben oder auf Schwierigkeiten stoßen, steht Ihnen unsere Hotline kostenlos 14 Tage lang zur Verfügung.

8.2 Schulungen

genugate Administrator Training: Diese zweitägige Schulung informiert Administratoren über Aufbau und Funktionsweise der genugate sowie Konfigurationsmöglichkeiten und Überwachung des laufenden Betriebs.

genugate Specialist Training: In der zweitägigen Schulung geht es um die genugate-Optionen HA sowie die Administration komplexer Systeme. Während der Schulungen werden praktische Übungen zu komplexen Anforderungen durchgeführt und Strategien zum Troubleshooting im laufenden Betrieb vermittelt.

genugate Advanced Training: Wie die High Resistance Firewall genugate in hochkomplexen Einsatzumgebungen installiert, konfiguriert und administriert wird, zeigen wir Ihnen im zweitägigen Advanced Training. Wichtige Themen sind dabei das SSH-Relay, DNS-Konzept und SNMPv3. Um aktiv an den praktischen Übungen teilnehmen zu können, sollten Sie bereits das genugate Administrator Training absolviert haben. Die Teilnehmerzahl ist auf acht Personen begrenzt. Genauere Informationen entnehmen Sie bitte unserem Schulungskatalog.

8.3 Laufender Betrieb – Software Support

Update Service: Die genugate-Produktreihe wird ständig weiterentwickelt. Regelmäßig erscheinen neue Versionen, in denen aktuelle Entwicklungen aufgegriffen werden und der Funktionsumfang sinnvoll ergänzt wird. Je nach Bedarf erscheinen zusätzlich Zwischenversionen.

Unser Update-Service sichert Ihnen die automatische Lieferung der neuesten Versionen und Zugriff auf unsere komplette Patch-Datenbank.

Hotline: Zusätzlich zu unserem Update Service bieten wir deutsch- und englischsprachigen Support via Telefon und E-Mail. Sie können unsere Hotline für alle Fragen zu Ihrer Lösung mit der genugate nutzen. Als Option steht Ihnen der telefonische Hotline Support 24 Stunden an allen Tagen zur Verfügung.

Security System Management: Auf Wunsch übernehmen wir die komplette Administration Ihrer genugate. Sie brauchen sich dann praktisch um nichts mehr zu kümmern. Die Administration erfolgt über eine stark verschlüsselte Internet-Verbindung. Ein zusätzlicher Hotline-Support ist beim Security System Management nicht erforderlich, der Update Service dagegen muss separat bezogen werden.

8.4 Laufender Betrieb – Hardware Support

Next Business Day Austausch-Service: Bei defekter Hardware erhält der Kunde innerhalb Deutschlands am nächsten Werktag ein baugleiches Gerät im Austausch für das defekte Gerät. Leistungsumfang und Voraussetzungen entnehmen Sie bitte den Allgemeinen Vertragsbedingungen der genua GmbH.

8.5 Support von genugate-Vertriebspartnern

Support-Leistungen von Vertriebspartnern: Viele autorisierte Vertriebspartner von genua bieten zum Teil erweiterte Support-Optionen an, z. B. Vor-Ort-Austauschservice von Hardware innerhalb garantierter Maximalzeiten.

GG-WP-0620-20-D

So erreichen Sie uns:

genua GmbH, Domagkstraße 7, 85551 Kirchheim bei München
tel +49 89 991950-0, fax +49 89 991950-999, info@genua.de, www.genua.de