



# GeNUGate-Datendiode

## Zuverlässiger Einbahn-Datentransfer an Rot-Schwarz-Übergängen

Verbindungen zwischen unterschiedlich eingestuftem Netzen – die Rot-Schwarz-Übergänge – sind heikel: An dieser Stelle muss unbedingt sichergestellt werden, dass aus dem höher eingestuftem roten Netz keine vertraulichen Informationen in den schwarzen Bereich gelangen, da hier auch unbefugte Personen Zugriff haben. Dies gilt sogar, wenn ausschließlich der Einbahn-Datentransfer vom schwarzen ins rote Netz eingerichtet wird. Denn für die schnelle und zuverlässige Übertragung in Richtung rotes Netz wird in der Gegen-

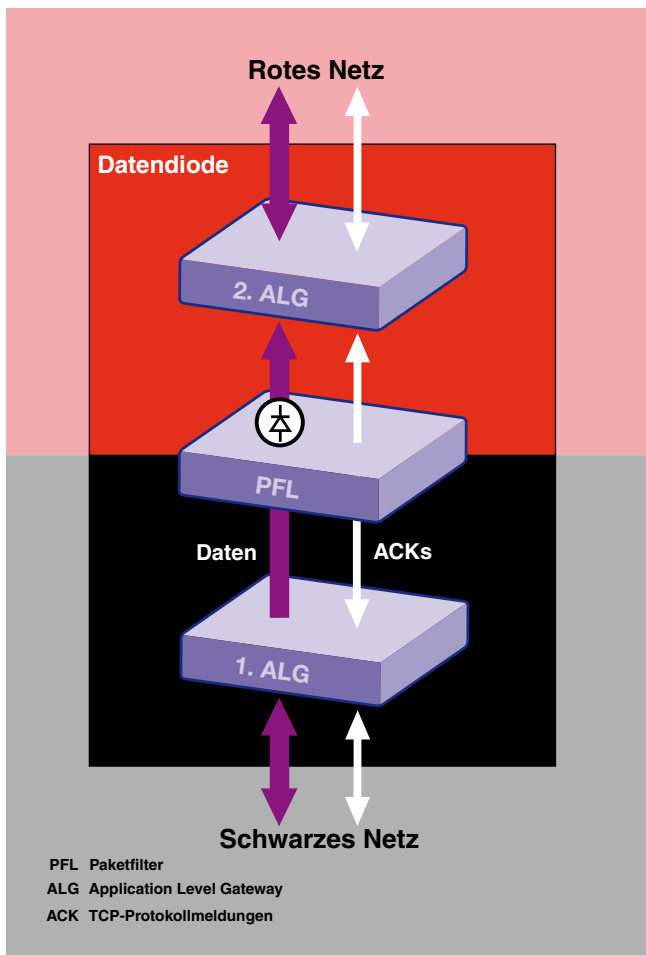
richtung eine Feedback-Verbindung benötigt, über die der schwarze Absender informiert wird, dass alle Datenpakete korrekt angekommen sind. Die häufig eingesetzten Protokolle TCP für Daten sowie SMTP für E-Mails funktionieren so. Verfahren ohne Rückkanal sind dagegen deutlich langsamer und verlieren immer wieder Pakete, so dass die übertragenen Dateien unbrauchbar sind.

### Rückkanal muss abgesichert werden

Wichtige Anwendungen und die Übertragung größerer Datenmengen erfordern somit Protokolle mit Rückkanal. Die technische Herausforderung dabei: Über den Weg von Rot nach Schwarz dürfen ausschließlich die für den Datenaustausch erforderlichen Protokollmeldungen (ACKs) fließen – aber keinesfalls vertrauliche Informationen.

### GeNUGate-Datendiode als Sicherheitsschleuse

Für diese Aufgabe haben wir die GeNUGate-Datendiode entwickelt. Die Lösung setzt sich aus drei in Reihe geschalteten Sicherheitssystemen zusammen – einem Application Level Gateway, einem Paketfilter und einem zweiten Application Level Gateway (A-P-A-Aufbau). Diese drei Komponenten funktionieren zusammen wie eine Schleuse mit einem breiten und einem verengten Kanal: Daten aus dem schwarzen Netz werden angenommen und über eine neue Verbindung zum roten Bereich transferiert, in umgekehrter Richtung dürfen dagegen lediglich auf das unbedingt Notwendige reduzierte Protokoll-Informationen passieren.



## Der Ablauf des Transfers

Die schwarzen TCP- oder SMTP-Daten gelangen an das erste Application Level Gateway der Diode. Hier werden sie angenommen und anschließend die Verbindung getrennt – ein Application Level Gateway lässt keinen durchgängigen Datenstrom zu. Als weitere Sicherheitsleistung bietet diese Dioden-Komponente die Möglichkeit, die angenommenen E-Mails auf Viren und Malware zu filtern, um das rote Netz zu schützen. Jetzt wird die neue Verbindung zum zweiten Application Level Gateway geöffnet. Der zwischengeschaltete Paketfilter lässt diese Daten passieren, kontrolliert jedoch sehr sorgfältig den Verkehr in Gegenrichtung: Lediglich Protokoll-Meldungen, die vom zweiten Application Level Gateway für den Datentransfer an das erste zurückgesendet werden und auf die unbedingt erforderlichen Informationen reduziert sind, werden durchgelassen. Alle anderen Inhalte werden entfernt, Pakete von anderen Absendern konsequent geblockt. Schließlich baut das zweite Application Level Gateway wieder eine neue Verbindung zum Empfänger auf und überträgt die Daten ins rote Netz. Diese zweifache Unterbrechung des Datenstroms durch die Application Level Gateways sorgt zusammen mit der Dioden-Funktion des Paketfilters für höchste Sicherheit an Rot-Schwarz-Übergängen. Ausführliche Covert Channel Analysis belegen das hohe Schutzniveau.

## Wichtige Anwendungen hochsicher einrichten

Mit der GeNUGate-Datendiode kann der Datentransfer von Schwarz nach Rot für wichtige Anwendungen komfortabel und hochsicher eingerichtet werden. Beispiele sind:

- die Spiegelung von Datenbanken für Geo-Informationen-Systeme (GIS)
- der Transfer von Dateien
- die Anbindung von E-Mail-Systemen

## Gute Basis: Vom BSI zertifizierte Firewall

Die Datendiode basiert auf dem bewährten Firewall-System GeNUGate von GeNUA. Diese zweistufige Firewall aus einem Application Level Gateway und einem Paketfilter ist vom Bundesamt für Sicherheit in der Informationstechnik (BSI) nach CC EAL 4+ zertifiziert und zusätzlich als Highly Resistant eingestuft, da beim wichtigen Sicherheitsmerkmal Selbstschutz der Level EAL 6 erfüllt wird. Die GeNUGate ist die einzige Highly Resistant Firewall der Welt. Für die dreistufige Datendiode wurde dieser hochwirksamen Sicherheitslösung ein weiteres Application Level Gateway hinzugefügt. Je nach Leistungsanforderung bieten wir die GeNUGate-Datendiode auf unterschiedlichen Hardware-Systemen an, bei denen alle wichtigen Komponenten redundant angelegt sind. Das stärkste Einzelsystem erreicht einen Datendurchsatz von 600 Mbit/s, darüber hinausgehende Anforderungen lösen wir mit hochverfügbaren Clustern.

## Service für jeden Kundenwunsch

Sie bekommen von uns genau den Service, den Sie benötigen. Auf Wunsch übernimmt unser System Management über stark verschlüsselte Internet-Verbindungen die fortlaufende Überwachung und komplette Administration der Sicherheitssysteme. Wir bieten aber auch Hotline Service via Telefon und E-Mail 24 Stunden an allen Tagen sowie regelmäßigen Update Service, damit Ihre Lösung stets auf dem neuesten Stand ist.

## Über GeNUA

GeNUA, Gesellschaft für Netzwerk- und Unix-Administration, ist ein deutscher Spezialist für IT-Sicherheit. Seit der Firmengründung 1992 beschäftigen wir uns mit der Absicherung von Netzwerken – und bieten ausgefeilte Lösungen. Unser Leistungsspektrum umfasst Firewall-Systeme mit BSI-Zertifikat, Hochsicherheits-Gateways für Rot-Schwarz-Übergänge, VPN- und Fernwartungs-Lösungen, Datenoptimierung für Satellitenkommunikation sowie ein umfangreiches Serviceangebot. Viele Unternehmen und sicherheitsbewusste Behörden setzen zum Schutz ihrer IT auf Lösungen von GeNUA.

