



GeNUGate-Datendiode

Einbahn-Datentransfer an Schwarz-Rot-Übergängen

Zuverlässige Datenübertragung erfordert Feedback

Verbindungen zwischen unterschiedlich eingestuftem Netzen – die Schwarz-Rot-Übergänge – sind heikel: An dieser Stelle muss unbedingt sichergestellt werden, dass aus dem GEHEIM eingestuftem roten Netz keine vertraulichen Informationen in das VS-NfD eingestufte schwarze Netz gelangen, da hier auch unbefugte Personen Zugriff haben. Technisch ist die Einrichtung einer strikten Einbahn-Datenverbindung von schwarz nach rot zwar problemlos möglich. Aber für häufig eingesetzte Protokolle wie SMTP für E-Mails, FTP für Dateitransfers sowie natives TCP reicht dies nicht aus. Sie benötigen in der Gegenrichtung eine Feedback-Verbindung, über die der Absender informiert wird, dass alle Datenpakete korrekt angekommen sind. Nur so können diese Protokolle eine schnelle und zuverlässige Datenübertragung garantieren. 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 Protokoll-Meldungen fließen – aber keinesfalls GEHEIM eingestufte Informationen.

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. Dass die GeNUGate-Datendiode höchste Sicherheitsanforderungen erfüllt, belegen mehrere Zulassungen vom Bundesamt für Sicherheit in der Informationstechnik (BSI).

Wichtige Anwendungen hochsicher einrichten

Mit der GeNUGate-Datendiode kann der Datentransfer von Schwarz nach Rot für betriebskritische Anwendungen komfortabel und zugleich hochsicher eingerichtet werden.

Beispiele sind

- die Spiegelung von Datenbanken (z. B. für GIS-Daten und FüInfoSys)
- der Transfer von Dateien (z. B. für TKÜ-Anwendungen)
- die Anbindung von E-Mail-Systemen

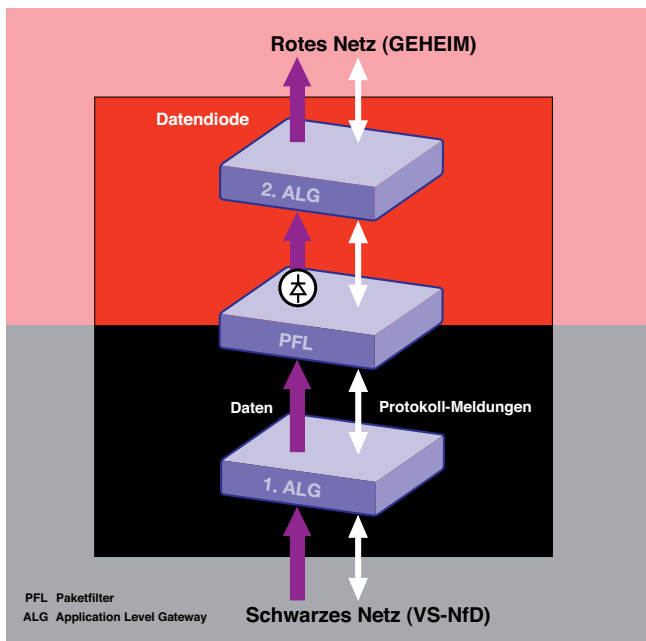




Der Ablauf des Datentransfers

Die schwarzen SMTP-, FTP- oder TCP-Daten gelangen an das erste Application Level Gateway der Diode. Hier werden sie angenommen und anschließend die Verbindung getrennt: Ein Application Level Gateway lässt keine durchgängigen TCP/IP-Verbindungen zu – es leitet lediglich die enthaltenen Daten weiter. Als weitere Sicherheitsleistung bietet diese Dioden-Komponente die Möglichkeit, die angenommenen Daten 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 im roten Netz auf und überträgt die Daten. Diese zweifache Unterbrechung des Datenstroms durch die Application Level Gateways sorgt zusammen mit der Dioden-Funktion des Paketfilters für höchste Sicherheit an Schwarz-Rot-Übergängen. Ausführliche Covert Channel-Analysen belegen das hohe Schutzniveau.

Informationsfluss bei der GeNUGate-Datendiode



Gute Basis: vom BSI zertifizierte Firewall

Die Datendiode basiert auf dem bewährten Firewall-System GeNUGate von GeNUA. Diese zweistufige Firewall mit Application Level Gateway und 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 7 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.

Umfassender Service zur GeNUGate-Datendiode

Auf Wunsch nimmt Ihnen unser Kundenservice alle Aufgaben ab: Unsere sicherheitsüberprüften Mitarbeiter installieren die GeNUGate-Datendiode und sorgen mit 24/7 Hotline Service für den reibungslosen Betrieb in Ihrem Netz. Mit regelmäßigem Update Service stellen wir zudem sicher, dass die Software stets auf dem neuesten Stand ist.

Über GeNUA

GeNUA, Gesellschaft für Netzwerk- und Unix-Administration, ist ein deutscher Spezialist für IT-Sicherheit. Seit der Unternehmensgründung 1992 beschäftigen wir uns mit der Absicherung von Netzwerken und bieten hochwertige Lösungen. Unser Leistungsspektrum umfasst Firewall-Systeme mit Zertifikat vom Bundesamt für Sicherheit in der Informationstechnik (BSI), Hochsicherheits-Gateways für Rot-Schwarz-Übergänge, intelligente VPN- und Fernwartungs-Systeme, Lösungen für Mobile Security, Datenoptimierung für Satelliten-Kommunikation sowie ein umfangreiches Dienstleistungsangebot. Viele Unternehmen und sicherheitsbewusste Behörden setzen zum Schutz ihrer IT-Systeme auf Lösungen von GeNUA.