



Sicherheits-Gateway  
für Rot-Schwarz-Übergänge

# RSGate für hochsichere Rot-Schwarz-Übergänge

Wer stets ein aktuelles Bild der Lage hat, ist klar im Vorteil. Dafür sind ständiger Datenaustausch und eine umfassende Vernetzung erforderlich. Im militärischen Bereich gelten hier die strikten Vorgaben des Geheimschutzes: Werden unterschiedlich eingestufte Netze gekoppelt, ist unbedingt sicherzustellen, dass Verschlusssachen ausschließlich in den vertrauenswürdigen roten Netzen bearbeitet werden und nicht in schwarze Netze gelangen. Denn hier haben auch nicht ermächtigte Personen Zugriff. An den Netzwerk-Übergängen – den Rot-Schwarz-Schnittstellen – muss also eine exakte Kontrolle stattfinden.

## Die Aufgabe: Kontrolle des Inhalts

Diese Anforderung kann nur mit einem Sicherheits-Gateway erfüllt werden, das an der hochsensiblen Schnittstelle den Inhalt der übertragenen Daten kontrolliert: Es darf Informationen von Rot zu Schwarz nur dann weiterleiten, wenn sie lediglich als „offen“ oder „VS-NfD“ eingestuft sind. Mit herkömmlichen Firewalls ist diese Aufgabe nicht zu lösen, da hier die Daten lediglich anhand formaler und technischer Eigenschaften wie Absender, Empfänger und Protokolltyp geprüft werden.

## Die Lösung: RSGate

Das Sicherheits-Gateway RSGate ermöglicht die exakte inhaltliche Kontrolle und Steuerung des Datenflusses. Dies wird durch ein zweistufiges Verfahren mittels Prüfserver

und Sicherheitsfilter garantiert. Die Inhaltskontrolle kann dabei sowohl automatisiert als auch manuell erfolgen. Bei maschinellen Verfahren prüft ein Parser die Dateien, deren Inhalt in ein genau definiertes Format eingebettet ist. Beispiele sind Statusinformationen und Standort-Koordinaten in XML-Dokumenten, nautische Daten im Format NMEA 0183 oder ASTERIX-Meldungen von Radargeräten. Dateien mit beliebigen Texten oder Grafiken sind vom Anwender manuell mit einem Viewer zu prüfen. Wenn keine vertraulichen Informationen enthalten sind, werden die Daten digital signiert und somit zur Übertragung in das schwarze Netz freigegeben. Der Sicherheitsfilter verifiziert anschließend die Gültigkeit von Signatur und zugehörigem Benutzer-Zertifikat.

## Entscheidender Vorteil gegenüber VPN-Lösungen

Die vom RSGate freigegebenen Daten können im schwarzen Netz ohne weitere Schutzmaßnahmen verarbeitet werden. Somit transferiert ein RSGate tatsächlich Daten von Rot nach Schwarz. Ein VPN dient dagegen nur als verschlüsselte Übertragungsstrecke über ein schwarzes Transitnetz. Am Ziel müssen die übertragenen Daten unbedingt wieder einen roten Bereich erreichen, wo sie verarbeitet werden dürfen. Es findet keine Übertragung in schwarze Systeme statt.

## Virenschanning von Schwarz nach Rot

Vom schwarzen in Richtung rotes Netz lässt das RSGate Daten ohne Inhaltskontrolle passieren, filtert jedoch nach Viren und Schad-Software. Durch dieses Virenschanning auf der schwarzen Firewall wird das sensible rote Netz zuverlässig vor schädlichem Code geschützt.

## Stationär und mobil einsetzbar

Das RSGate ist vielseitig einsetzbar – sowohl stationär an Land als auch an Bord von Schiffen und Fahrzeugen. Somit können Netzwerk-Übergänge in vielfältigen Einsatzumgebungen und allen Teilstreitkräften mit dieser Sicherheitslösung kontrolliert werden.



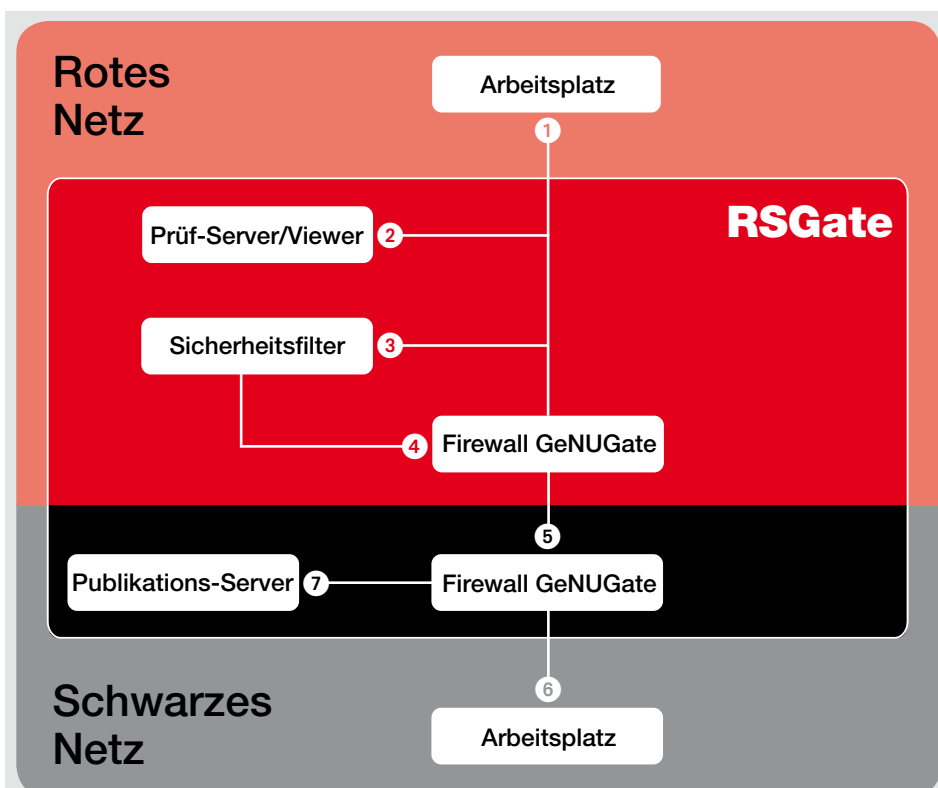
RSGate ist flexibel einsetzbar

## Zulassung für Einsatz bis GEHEIM

An den hochsensiblen Rot-Schwarz-Übergängen dürfen nur absolut zuverlässige Sicherheitssysteme eingesetzt werden. Deshalb haben wir das RSGate von unabhängigen Experten prüfen lassen, mit diesen Ergebnissen:

- Bundesamt für Sicherheit in der Informationstechnik (BSI) hat die Zulassung für den Einsatz bis GEHEIM bei der Bundesmarine erteilt.
- WTD 81 hat eine Evaluierung nach ITSEC E3/hoch erfolgreich durchgeführt.

Darüber hinaus sind die beim RSGate verwendeten Firewall-Systeme des Typs GeNUGate vom BSI nach CC EAL 4+ zertifiziert und zusätzlich als Highly Resistant eingestuft. Denn die Firewall ist auch unter günstigen Bedingungen selbst von geschickten Angreifern nicht zu überwinden – die Leistung bei diesem Sicherheitsmerkmal entspricht dem Level EAL 6. Die GeNUGate ist die einzige Highly Resistant Firewall der Welt. Somit haben Sie die Gewähr, dass das RSGate die hohen Sicherheitsanforderungen erfüllt.



## Der Weg von Rot nach Schwarz

Das RSGate besteht aus Prüf-Server, Sicherheitsfilter, zwei Firewalls zur Trennung der Netze und einem Publikations-Server. Hier das Zusammenspiel der Komponenten beim Datentransfer vom roten zum schwarzen Netz:

- ➊ Roter Arbeitsplatz: Eine Datei für einen Empfänger im schwarzen Netz wird als E-Mail-Anhang gesendet.
- ➋ Prüf-Server: Maschinell prüfbare Dateien werden voll automatisiert vom Parser kontrolliert, andere Formate manuell vom Anwender, der über den Viewer eine Freigabe erteilen kann. Falls keine vertraulichen Informationen enthalten sind, wird die Datei maschinell bzw. manuell digital signiert und als E-Mail an den Sicherheitsfilter weitergeleitet.
- ➌ Sicherheitsfilter: Prüft die Signatur. Falls diese korrekt und unverändert ist, wird die Datei an eine neue E-Mail angehängt und an die rote Firewall weitergeleitet.
- ➍ Rote Firewall: Nimmt ausschließlich vom Sicherheitsfilter kommende E-Mails entgegen und leitet diese weiter an die schwarze Firewall.
- ➎ Schwarze Firewall: Scant E-Mail und Anhang und entfernt Viren sowie aktive Inhalte. Anschließend wird die E-Mail an den Empfänger weitergeleitet.
- ➏ Schwarzer Arbeitsplatz: Die Datei trifft als E-Mail-Anhang beim Empfänger ein.
- ➐ Publikations-Server: Hier können mittels Prüf-Server freigegebene Dateien abgelegt werden, um sie im gesamten schwarzen Netz zum Abruf per HTTP oder FTP bereitzustellen.

# Übersicht der Funktionen

## Basis-Funktionalitäten

- Beschränkung auf zulässige Absender und Empfänger nach IP-Adressen und/oder E-Mail-Adressen
- Schutz des roten Netzes vor Angriffen durch mehrstufiges Firewall-System GeNUGate
- Virenprüfung der per SMTP, HTTP und FTP übertragenen Daten, Filterung aktiver Inhalte wie Java, Javascript, ActiveX
- Protokollierung aller Kommunikationsverbindungen
- Alarmierung eines festzulegenden Administrators bei Sicherheitsverstößen und Störungen
- Funktionen zur Administration aller Komponenten
- Schutz vor Fehlkonfiguration

## Datentransfer von Rot zu Schwarz

### Unterstützte Formate bei maschineller Freigabe:

- XML-Dokumente
- NMEA 0183-Meldungen
- milASTERIX-Meldungen
- weitere Formate auf Anfrage

### Unterstützte Formate bei manueller Freigabe:

- TXT (ASCII)
- AMR (ADatP-3)
- BMP (schwarz-weiß Bitmaps)
- RTF (Rich Text Format) mit eingeschränktem Befehlssatz

Die RSGate-Lösung mit BSI-Zulassung bis GEHEIM transferiert SOA-Anfragen im XML-Format via SMTP.

Veröffentlichung freigegebener Dokumente auf einem Publikations-Server zum Abruf per HTTP oder FTP aus dem schwarzen Netz

## Datentransfer von Schwarz zu Rot

- Übertragung von E-Mails inklusive beliebiger Anhänge per SMTP
- Auf Anfrage eines Clients im roten Netz Datenübertragung per HTTP mit diesen Sicherheitsbeschränkungen:
  - HTTP-Header sind auf GET und HEAD beschränkt
  - URL-Filter schränken zulässige Anfragen ein
  - FTP-Downloads werden über HTTP/Proxy-Funktionalität und FTP-URLs unterstützt
- Übertragung von SNMP-Traps (Alarmer von Netzkomponenten im schwarzen Netz)
- Optional: Signierung von Anhängen in E-Mails, die vom schwarzen in den roten Bereich gesendet werden, damit diese Anhänge den roten Bereich ohne Inhaltsprüfung wieder verlassen können, sofern sie unverändert sind.



GeNUA, Gesellschaft für Netzwerk- und Unix-Administration mbH, ist ein Spezialist für IT-Sicherheit. Seit der Unternehmensgründung 1992 beschäftigen wir uns mit der Absicherung von Netzwerken – und bieten ausgefeilte Lösungen. Dazu gehören hochwertige Firewall-Systeme mit Zertifikat vom Bundesamt für Sicherheit in der Informationstechnik (BSI), VPN- und Fernwartungslösungen, Datenoptimierung für Satellitenkommunikation sowie ein umfangreiches Dienstleistungsangebot. Zahlreiche große und mittelständische Unternehmen sowie sicherheitsbewusste Behörden und Organisationen setzen zum Schutz ihrer IT auf Lösungen von GeNUA.

Gesellschaft für Netzwerk- und Unix-Administration mbH  
Domagkstraße 7, 85551 Kirchheim  
tel +49 (89) 99 1950-0  
info@genua.de, www.genua.de



INFODAS GmbH ist als unabhängiges Software- und Beratungsunternehmen seit mehr als 30 Jahren ein kompetenter und verlässlicher Partner in der Entwicklung und Integration von IT-Lösungen. Einer unserer Leistungsschwerpunkte ist die best practice IT-Sicherheitsberatung und -umsetzung. Diese Kernkompetenz führt im Hochsicherheitsbereich zu innovativen Lösungen und entwicklungsbegleitenden Beratungsleistungen. Aufgrund zusätzlicher, langjähriger Projekterfahrung im Meldewesen und der Kommunikationsflusssteuerung ist es uns gelungen, zuverlässige und schnelle Meldungsparser und Viewer, die u.a. Kernbestandteil der RSGate-Lösung sind, zu entwickeln.

Gesellschaft für Systementwicklung und Informationsverarbeitung mbH  
Rhonstr. 2, 50765 Köln  
tel +49 (221) 70912-0  
rsgate@infodas.de, www.infodas.de