



**Security Gateway for Transitions
between Red and Black Military Networks**

RSGate for Top-Secure Transitions between Networks

Having a complete picture of the current situation offers a clear advantage. For this, permanent data exchange and comprehensive networking is essential. In military information exchange strict security rules for the protection of classified information apply: That is, where networks with different security classifications are connected, it must absolutely be ensured that classified information is processed solely in trustworthy red networks and is never transferred to black networks, where unauthorized individuals would have access to it. Hence detailed surveillance of information must occur at red/black interfaces.

The Task: Content Monitoring

This requirement can only be satisfied by a security gateway that monitors the transferred data at the sensitive red/black interfaces and only transfers information of low-level classification (“Unclassified” or “For Official Use Only”) from a red network to a black network. This task cannot be performed with conventional firewall systems, since they only check the data with regard to formal and technical characteristics, such as sender, receiver and communications protocol used.

The Solution: RSGate

The security gateway RSGate allows a precise content monitoring and control of data flow. This is guaranteed by a two-stage process using a viewer and a security filter. Content monitoring can be performed automatically or manually under user control. In the automatic procedure a software parser verifies the files whose contents have a precisely defined format. Examples include: status information and position coordinates in XML documents, nautical data in NMEA 0183 or ASTERIX messages from radar devices. Files containing unformatted text or graphics must be manually displayed on the viewer and analyzed for confidentiality by an authorized user. In either case, a file is only digitally signed and released for transfer to the black network if it contains no confidential information. The security filter afterwards validates the signature and the associated user certificate.

Key Advantage over VPN Solutions

The data released by RSGate can be processed further in the target network without any safeguards. Thus RSGate transfers data from red to black. In comparison, a VPN only serves as an encrypted transfer route across a black transit network. The data must be transmitted to a red system for processing and may not be processed further in black systems.

Virus Scanning on Black-to-Red Transmission

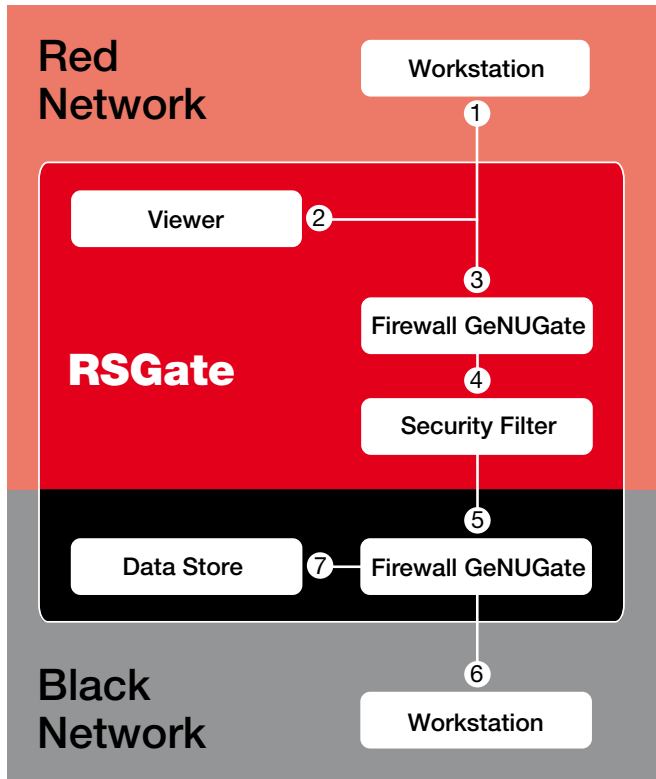
RSGate allows data transfers from black to red networks without content monitoring, but filters out viruses and other malware. Thus the sensitive red network is reliably protected against harmful code.

For Static and Mobile Use

RSGate is very versatile – it may be used in both static and mobile installations, e.g. land-based, on ships or in vehicles. Thus network interfaces in multi-dimensional operational environments and throughout all military branches can be controlled.



RSGate is flexible and versatile



Licensed for Use up to SECRET Level

Only absolutely trustworthy security systems must be used at the highly sensitive red/black interfaces. RSGate has been assessed by independent experts with the following results:

- The German Federal Office for Information Security (BSI) has granted an individual authorization for use up to SECRET level for the German Navy.
- The German Weapons Technology Agency for Information Technology and Electronics (WTD 81) has conducted a successful evaluation up to level ITSEC E3/high.

In addition, the GeNUGate firewall systems used by RSGate are certified up to CC EAL 4+ level and rated as Highly Resistant by BSI. This firewall solution cannot be overcome by attackers, even under favorable circumstances, this security feature meets Level EAL 6. GeNUGate is the only Highly Resistant Firewall worldwide. Thus RSGate meets the highest security requirements.

Data Flow from the Red to the Black Network

In the current architecture RSGate has a viewer, a security filter, two firewalls for separating the networks and a data store. The components have the following roles in the data transfer by e-mail from a red to a black network:

- 1 Red Workstation: Provides a file as an e-mail attachment to the recipient in the black network.
- 2 Viewer: Machine-verifiable files are checked automatically by a parser, others are checked manually by the user, who can authorize a release via the viewer. If a file contains no sensitive information, it is automatically or manually signed and forwarded as an e-mail to the security filter.
- 3 Security Filter: Checks the certificate. If it is correct and unchanged, the file is attached to a new e-mail and sent to the black firewall system.
- 4 Red Firewall: Accepts only e-mails and forwards these to the security filter.
- 5 Black Firewall: Scans e-mails and their attachments and deletes viruses as well as active contents. Afterwards the e-mails are forwarded to the recipients.
- 6 Black Workstation: The files are received as e-mail attachments by the recipients.
- 7 Data Store: Storage of files released via the viewer, so that they can be retrieved within the entire black network via HTTP or FTP.

Overview of functions

Base functionality

- Restriction of permitted senders and receivers by IP and/or e-mail addresses
- Protection against attacks on the red network by the integrated multi-level firewall system GeNUGate
- Virus checking of files transferred via SMTP, HTTP and FTP, filtering active contents (ActiveX, Java, Javascript)
- Logging of all communication links
- Alerting of a designated administrator in the event of security violations or breakdowns
- Functions for administrating all components
- Protection against misconfiguration

Data Transfer from Red to Black Networks

Formats supported by automatic release:

- XML documents
- NMEA 0183 messages
- milASTERIX messages
- Additional formats on request

Formats supported by manual release:

- TXT (ASCII)
- AMR (ADatP-3)
- BMP (black/white bitmaps)
- RTF (Rich Text Format), limited command set

The RSGate solution (which is certified up to the SECRET level by BSI) transfers SOA-requests in the XML format via SMTP.

Publishing of released documents on a data store for retrieval from the black network via HTTP or FTP.

Data Transfers from Black to Red Networks

- Transfer of e-mails including attachments via SMTP
- When requested by a HTTP client in the red network, transfer of files via HTTP with the following security restrictions:
 - Restriction to permitted requests by URL filters
 - Support for FTP downloads via HTTP/Proxy functionality and FTP URLs
- Transfer of SNMP traps (alarms from network components in the black network)
- Optional: Signing of attachments in e-mails that are sent from the black to the red area, so that these attachments can later leave the red network without contents checking if they are unchanged



GeNUA, Gesellschaft für Netzwerk- und Unix-Administration mbH, is a German IT security specialist. Since founding the firm in 1992 we have been involved in networks security and provide elaborate solutions in this field. Our range of competence comprises high-grade firewall solutions certified and approved for RESTRICTED data by the German Federal Office for Information Security (BSI), VPN and remote maintenance solutions, data optimization for satellite communications, mobile security, and an extensive spectrum of service and consulting offerings. Numerous large and middle-range companies and security-conscious public authorities rely on GeNUA solutions for the protection of their IT systems.

Gesellschaft für Netzwerk-
und Unix-Administration mbH
Domagkstrasse 7, 85551 Kirchheim
Germany
phone +49 (89) 991950-0
info@genua.eu
www.genua.eu



INFODAS GmbH is an independent software and consulting company with more than 30 years' experience as a competent and reliable partner in the development and integration of IT solutions. One of our focal points is best-practice IT security consulting and implementation. This core competence results in innovative solutions and development support consulting in the area of high security technology. As a result of our long experience in military and civilian telecommunications and communications flow control, we have been able to develop reliable and fast-working message parsers and viewers which form the core component of RSGate and other solutions.

Gesellschaft für Systementwicklung
und Informationsverarbeitung mbH
Rhonestrasse 2, 50765 Cologne
Germany
phone +49 (221) 70912-0
rsgate@infodas.de
www.infodas.de