RSGate: IT Security Gateway for Monitored Information Transfer at Red/Black Interfaces

Successful Pilot Project on F124 Frigate – High-Security Gateway Designed by GeNUA and INFODAS is Granted ITSEC E3/High Certification

When working with classified information using information technology, it is vital to ensure that all confidentiality provisions are complied with, in particular those relating to protection against unmonitored transfer and transmission to a system with a lower level of security.

The acid test: the RSGate worked flawlessly on the F124

In the German armed forces, such information is typically processed in the weapons deployment, management information, and message transmission systems.

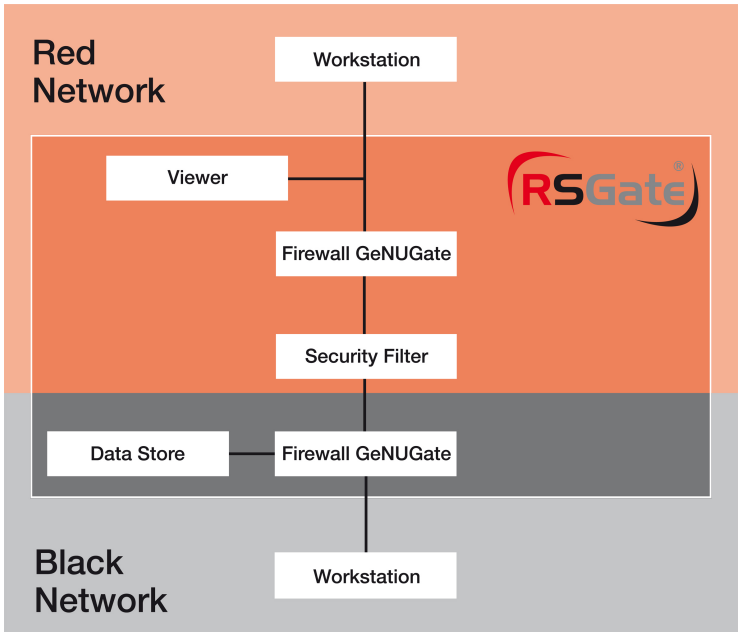
Because in the past these systems were often based on proprietary communications methods, linking to external systems was not possible. Now, however, thanks to the synergies resulting from linking the systems, the German armed forces – and also the most important allied forces – are migrating all information systems to IP-based communication.

Examples of such networking include the following:

- On new ships such as the K130 corvette and F125 frigate, the German Navy has designed integrated onboard networks to which all weapons and information systems are connected.
- In the case of information relating to highly complex modern weapons systems, such as the Eurofighter 2000, this must always be correctly divided into operational and tactical information, since the data obtained during the flight is to be forwarded to different mission and support systems.
- Similar challenges are faced in the case of the new generations of helicopters.

Finally, even connection to global public networks such as the Internet is a completely realistic option for a warship. Here, NATO stipulates a rigid red-black procedure: wiring, components, devices, systems, networks, etc. that process or transmit the classified information in plain text – red – must be separated from corresponding hardware items that process or transmit information that is encrypted or categorized as unclassified information – black.

The question therefore arises how to connect a red network to a black network, and permit monitored and secure communication between systems in both networks. Unmonitored data transmissions from a red network to a black network must be prevented at all times. Generally, linking of red and black networks is permitted only when it is ensured that the black network receives from the red network only information that the black network is entitled to process by virtue of its classification.



Secure interface: RSGate between the red and black networks

While the transmission of red data via black networks by means of tunneling or encryption of this data presents no problems, there is increasingly a need to transfer data not only via a black network, but also from a red network into a black one.

In this process, the data must be monitored in terms of content, and the authorizations for the transfer must be carefully checked in a verifiable manner. Conventional firewall systems filter data only in terms of their protocol characteristics such as sender, recipient, and communications protocol used. Examination of the content of the transmitted data is not undertaken, however.

For this function, the monitoring of data flow in accordance with the regulations, the German companies GeNUA and INFODAS have developed a reliable IT security gateway, the RSGate (for “Rot-Schwarz-Gateway” or red-black gateway), which is to be used at the interface between the red and black networks. The GeNUGates with CC EAL 4+ certification take over the network protection and protocol checking functions. Thanks to the solution developed by INFODAS, RSGate is able to monitor the content of the transmitted data: before information is sent from the red network to the black network, the user or a check routine defined by the user must ensure that it is information of a low classification level only (security classification “unclassified” or “restricted information – for official use only”).

Compact RSGate: all components in one rack

RSGate was used in an army trial on board an F124 frigate “Hessen” in order to control and monitor the data flow in a reliable, effective and user-friendly manner even in live, pressured situations. The features of the modular RSGate installed on the frigate, which has received a successful evaluation up to level ITSEC E3/high from the Testing Center for IT Security in the German armed forces (PZITSichhBw) of the German Military Technology Agency for Information Technology and Electronics (WTD 81), include:

- Automatic checking of status messages and sensor data exchanged between the CDS operational software (red Combat Direction System) and the IMCS automation system (black Integrated Monitoring and Control System)
- Careful checking by the security filter (“to the exact byte”) of the data to be transmitted against a configurable set of rules, and thus the monitored transfer of the data
- The manual approval of e-mails from a user in the red network to a recipient in the black network by means of:
- A reliable representation (“What you see is what you sign” principle)

- Supported file formats in the transfer from red to black: TXT, AdatP-3, BMP, and RTF
- Verification of the signatures provided by means of the central security filter
- Protection against attacks from the black network by means of an integrated firewall function
- Integrated functions for secure administration of the components.

The result of the military trial: the management system officer of the F124 frigate “Hessen” confirmed that the RSGate that had been used “worked flawlessly.”

Contact details:

GeNUA mbH • Domagkstrasse 7 • 85551 Kirchheim • Germany

tel +49 (89) 99 19 50 0 • fax +49 (89) 99 19 50 999 • info@genua.eu • www.genua.eu