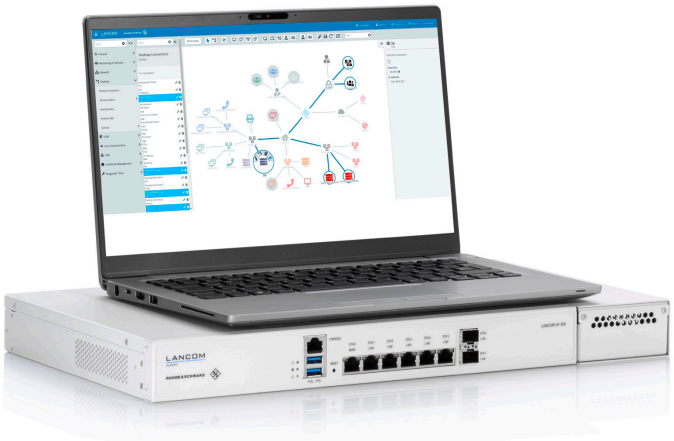
# REDUCING COMPLEXITY FOR SECURE ACCESS TO T&M DEVICES AND APPS

With IT and OT environments converging, security concerns relating to devices and applications deployed in networked test labs, especially in T&M environments, are growing. The demands on IT security here are manifold and include, for example, remote access to in-house infrastructures, equipment rented from external providers, and the continuous deployment of devices across different time zones.



T&M equipment must be externally accessible without sensitive devices being affected, measurement results being falsified or compromised or, in the worst case, elaborate and cost-intensive equipment being damaged. Protecting external access to vulnerable T&M equipment and applications involves complex processes whose validity and functional reliability must be ensured at all times in order to prevent hostile access with the aim of industrial espionage. The answer is a unified approach using a firewall and user interface designed to prevent security gaps due to misconfiguration.

## Your task

Where IT and OT technologies come together, having reservations about the unfamiliar technology on the other side is a natural reaction. In the past, either IT experts had to learn how to deal with new machines and applications, or test engineers had to get acquainted with unfamiliar network architectures and IT security concepts. OT equipment generally did not incorporate dedicated security features, so IT security had to be subsequently implemented using external resources, including firewalls that were outdated and/or difficult to configure and manage.

Administration of these legacy firewalls with their complicated, tabular sets of rules was another drawback, as this was time-consuming, error-prone and required expert knowledge. Providing IT security in general was a complex task and called for in-depth networking knowledge. Not to be ignored were the considerable work and expense involved since users had to make error-prone text entries instead of working with a straightforward user interface visualizing the network and rule sets in graphical form. As a result, working without dedicated IT security experts was difficult.

## Rohde&Schwarz solution

The Secure Application Gateway platform from Rohde&Schwarz now allows cybersecurity standards to be configured and implemented in T&M environments while significantly reducing complexity. A graphical user interface enables the configuration of rule tables, role dependent assignment of access rights, and network segmentation without dedicated IT security expertise.

The LANCOM R&S®Unified Firewall as the central component of the Secure Application Gateway is set up via an advanced web interface in a current web browser. The elements for configuring the firewall, such as network components, sets of rules and user authentication, are graphically represented on a dashboard, making configuration quick and easy. Rule sets are used to precisely specify, among other things, which data may be transferred from the laboratory to the outside world. This intuitive approach,



ROHDE&SCHWARZ
Make ideas real

visualizing all the elements and steps necessary for firewall configuration, does away with error-prone text entries and enables even lab engineers not familiar with IT technology to configure a firewall to be “watertight”.

An automatic rule hierarchy ensures that rules are processed in the correct order. Rules are automatically sorted based on their specificity, and handling them is intuitive even for newcomers to cybersecurity.

The intuitive dashboard shows very well the degree of abstraction achieved in the solution. The network architecture with the applied security concepts and the T&M devices are organized and displayed in a way that anyone can deal with. With firewall configuration performed at the application level, no detailed knowledge of the various network protocols and ports is required. Applications and their associated data streams are assessed and routed on depending on their business criticality.

## Application

The user-friendly web interface of the LANCOM R&S®Unified Firewall is the control center of the Secure Application Gateway solution and helps users configure and implement state-of-the-art firewalls satisfying the highest standards of cybersecurity. Human errors when configuring a firewall are significantly reduced, as all of the network firewall rules are clearly and concisely visualized by graphics on a dashboard. This browser based central management console helps fine tune a configuration while providing a comprehensive overview of secured devices and connections in the network. This not only facilitates the implementation of security requirements, but also saves time as it makes it easy to merge IT and OT rules. Audit and compliance reports further contribute to maximum transparency.

The Rohde&Schwarz solution reduces OPEX in the long term. The resources consumed by an IT security environment are strongly related to the consequences of incorrect configurations. By visualizing complex functions, rules and steps on a graphical user interface and by easy-to-use security concepts, the amount of work and any misconfigurations can be significantly reduced. Furthermore, easy-to-understand monitoring and logging functions enable direct, fast and agile response to any incidents.


Network security by design:
web UI based, made in Germany.

**Rohde&Schwarz GmbH&Co. KG**
www.rohde-schwarz.com

**Rohde&Schwarz training**
www.training.rohde-schwarz.com
**Rohde&Schwarz customer support**
www.rohde-schwarz.com/support

R&S® is a registered trademark of Rohde&Schwarz GmbH&Co. KG
Trade names are trademarks of the owners
PD 3609.9328.92 | Version 01.00 | October 2022 (ja)
Reducing Complexity for Secure Access to T&M Devices and Apps
Data without tolerance limits is not binding | Subject to change
© 2022 Rohde&Schwarz GmbH&Co. KG | 81671 Munich, Germany

3609932892
3609.9328.92 01.00 PDP/PDW 1 en