# STOPA Tele-Presence-Portal
Remote maintenance via mGuard

The comprehensive teleservice and remote maintenance concept from STOPA are the solution to cost-effective automation. Security should be kept in mind when it comes to machine maintenance from any location. With the mGuard routers used by STOPA you can easily protect your parts of your STOPA system network.

Please note: different / third party VPN solutions are not supported due to compatibility and managing issues.

The clever and smart Concept
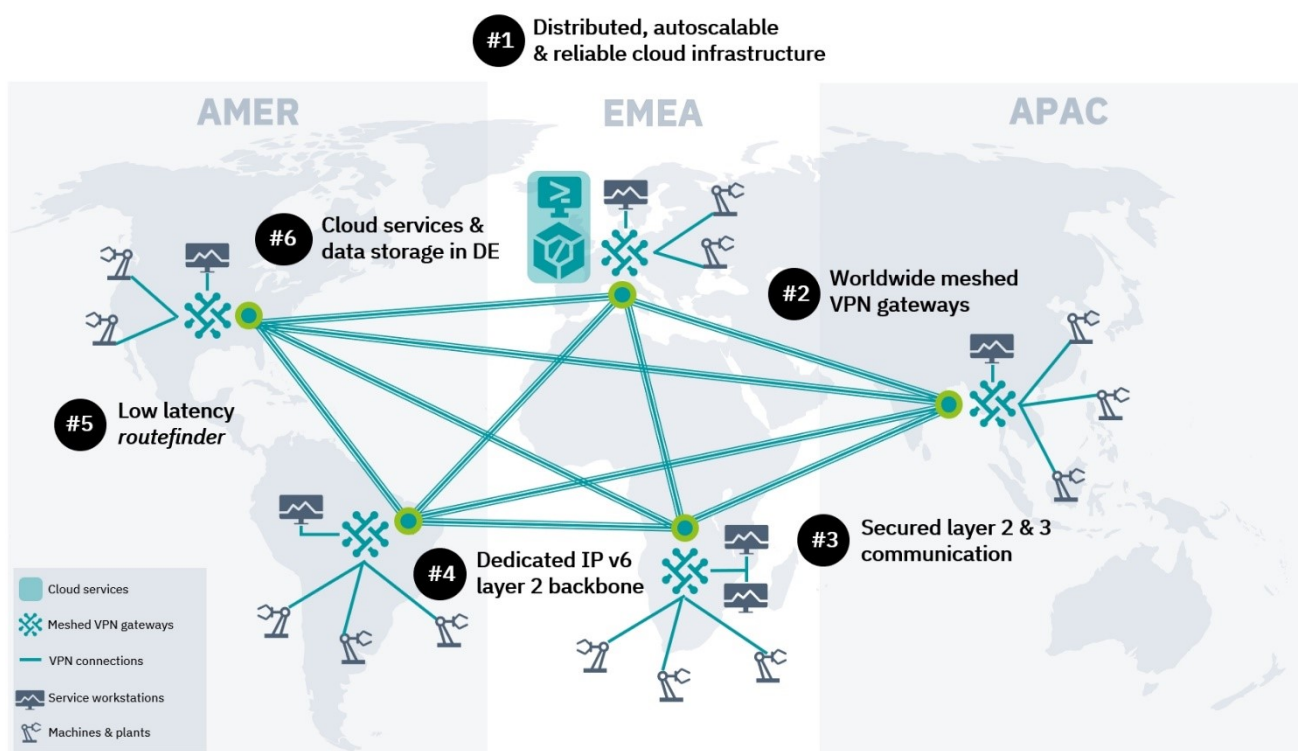
The STOPA secure remote maintenance concept from Phoenix Contact offers advantages in addition to the availability of public networks from any location:

- Reduced travel costs and downtimes
  - ➢ Remote maintenance independent of travel restrictions
- Fewer devices, as remote maintenance, routing, and firewall are combined in a single device.
- Operator network protected against unauthorized access.
- The customer alone enables remote maintenance via a Button on the STOPA machine.
- Easy machine integration in customer networks
- Machine is protected from the operator network and vice versa.
- No adaptation of machines and systems, no software required – Plug-n-Play

_____

Hardware

Phoenix mGuard modules are network components and combine the functions of a router, firewall, and VPN device. The aim: maximum security and system availability.

- Maximum level of security with Secure protocol on Layer 3 / Layer 2
- Supports current certificates such as x509.v3
- Only uses outgoing connections with standardized ports (TCP 443 / 53 or legacy ports UDP 500/4500)
- Connection for VPN exclusively available via push-button
- Integrated firewall protects the network and the system

Requirements for the STOPA Tele Presence Portal

The system (with mGuard) only needs to be able to establish a connection to the mGuard Secure Cloud Portal via the Internet (see addresses below). The mGuard remote maintenance unit is used as a router and is assigned its own IP address in the customer network. The device only and exclusively establishes a connection between the connected STOPA computer / PLC via the mGuard cloud to the STOPA customer service employee at the touch of a button. The connection is established using the following outgoing **standardized network ports**:

STOPA Tele Presence Portal mGuard Portal Version 3:
- TCP 443   (official https Port – Secure protocoll encapsulated)
  - Opened to new mGuard-Cloud address V3:
  - vpn.secure.phoenixcontact.cloud (IP: 15.197.210.88 and 3.33.199.189)
- Port 53 TCP/UDP to Internet for DNS. (standard DNS Port) or internal DNS

Legacy mGuard Version 2 :
- UDP 500   (official standard ISAKMP Port)
- UDP 4500   (official standard IPSec NAT Traversal Port)
  - Opened to mGuard-Cloud address V2:
  - machine-gw1.de.mguard.com   (IP: 18.195.180.168)

Please note: STOPA uses the internal addresses 192.168.10.X/24 for internal communication. If the same addressing is used in the company network the remote VPN connection could not work, because it could cause address-conflicts.
Please also note: Some Firewalls are configured as "Condition Firewall". These kind of firewall categorizes the content and may block the communication, regardless the ports are open.
For more and additional informationen please visit: mGuard Secure Cloud V2, Secure Cloud V3,cloud-based remote maintenance

For more information about the STOPA Tele-Presence Portal solution, please contact STOPA customer service. Here you can also receive an offer for the hardware and installation services.

STOPA Customer-Service Germany Hotline: +49-7841 704 149

E-Mail: Service@stopa.com