Remote Service Platform built by ApplicGate RSP

A new approach to secure networks…

Remote Service Platform built by ApplicGate RSP

Plant Supplier

Easy to install

Easy to operate

Fast

Cheap

Flexible

Secure

Plant

Reliable

Redundant configuration

Access from anywhere

High availability

Access controllable by plant operator

Plant Operator

Remote Service Platform by ApplicGate

reinhold.leitner@applicgate.com

Remote Service Platform - Overview

Goals

- Remote control of plants out of internal network of partners (e.g. supplier)
- Secure authentication and data transmission
- Full control by plant operator
- No additional hardware necessary

Prerequisites for remote site (plant)

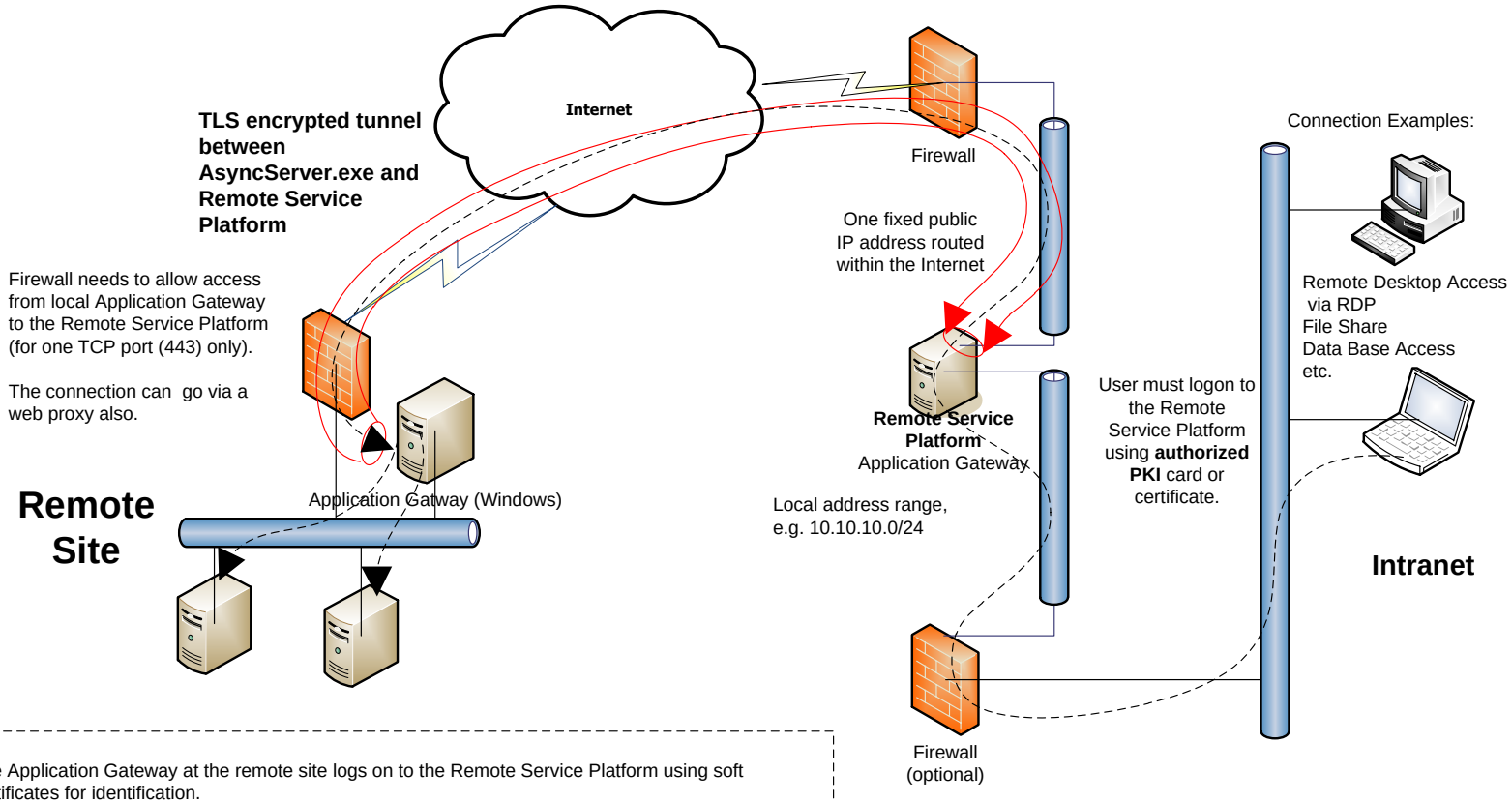
- Any Windows system (Windows 10, Windows Server) with .NET 4.8 Framework or .NET 5 or higher or any Linux system with .NET 5 or higher
- From this system outgoing sessions (TCP,TLS) to one specific public Internet address (central RSP installation) must be allowed (can be routed via web Proxy at plant)
- Works with dynamic IP addresses, no fixed IP address needed!

Functions

- Secure authentication via smartcards, soft certificates or One-Time-Password (sent via email or SMS)
- Support of various TCP protocols such as RDP, CIFS, VNC …
- Integrated logging
- Can be managed and configured by plant operator
- Optional notification by email at session setup/termination

reinhold.leitner@applicgate.com

Remote Service Platform - Access to remote Site



The Application Gateway at the remote site logs on to the Remote Service Platform using soft certificates for identification.
Logon can be activated/deactivated via a web interface at the remote site .

After successful logon, authorized users may access resources at the remote site depending on the rules defined in the Remote Service Platform and the Application Gateway at the remote site.

As an option the email notification can be configured, when a user accesses the remote site.

Various log files are provided.

Remark:

The program „Application Gateway“ is the same at the remote site and the Remote Service Platform, but with different confiuration.

reinhold.leitner@applicgate.com

Remote Service Platform versus standard VPN solution

Topics	Remote Service Platform	Standard VPN Solution
Works without client installation	yes	no
Separation of IP address ranges	yes	no
Menu of available connections (user dependent)	yes	no
Display of connection status	yes	no
Integrated shared shortcuts	yes	no
Central installation & logging	yes	no

reinhold.leitner@applicgate.com

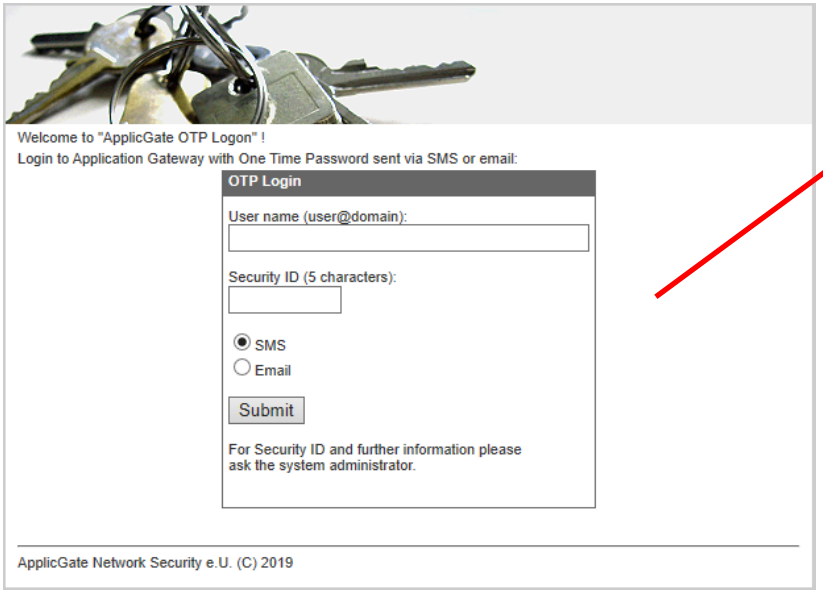
Steps to access remote sites

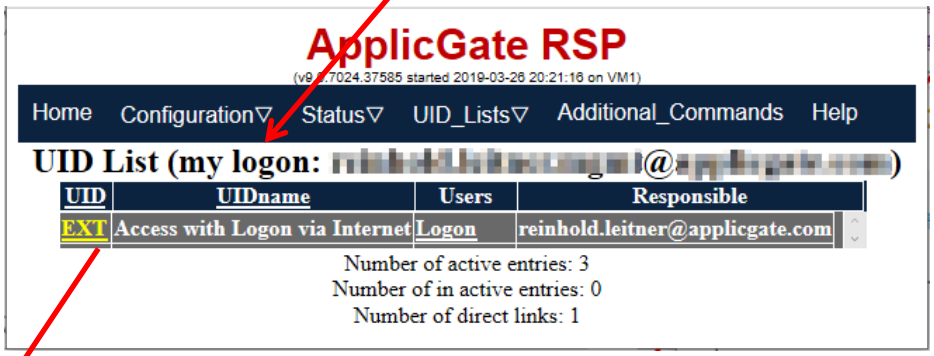
Logon to RSP	▪ Connect to central RSP by a web browser. ▪ Use soft certificate, smartcard of one-time password (OTP) for authentication.
Get a list of available installations	▪ List of available connections (dependent on user credentials) and their connection status will be shown
Select Shortcut	▪ Shortcuts can be http(s) links, files (e.g. .RDP files, .bat files to map a network share) stored on network shares or web sites.
Access remote site	▪ Click the shortcut and enter the necessary credentials to authenticate at the remote site (e.g. username/password for RDP or share mapping)

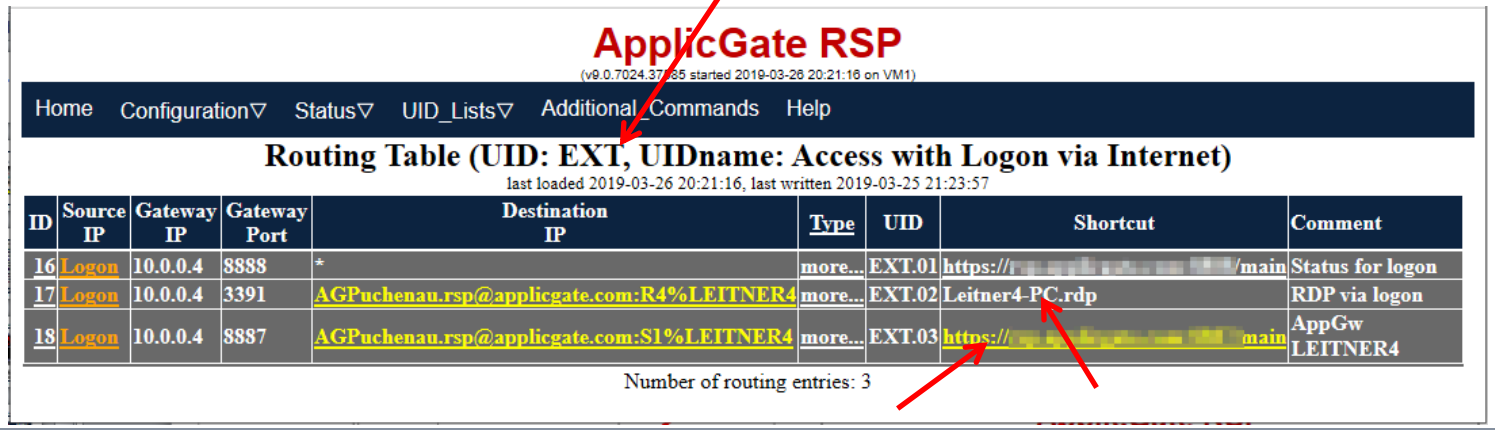
reinhold.leitner@applicgate.com

Steps to access remote sites

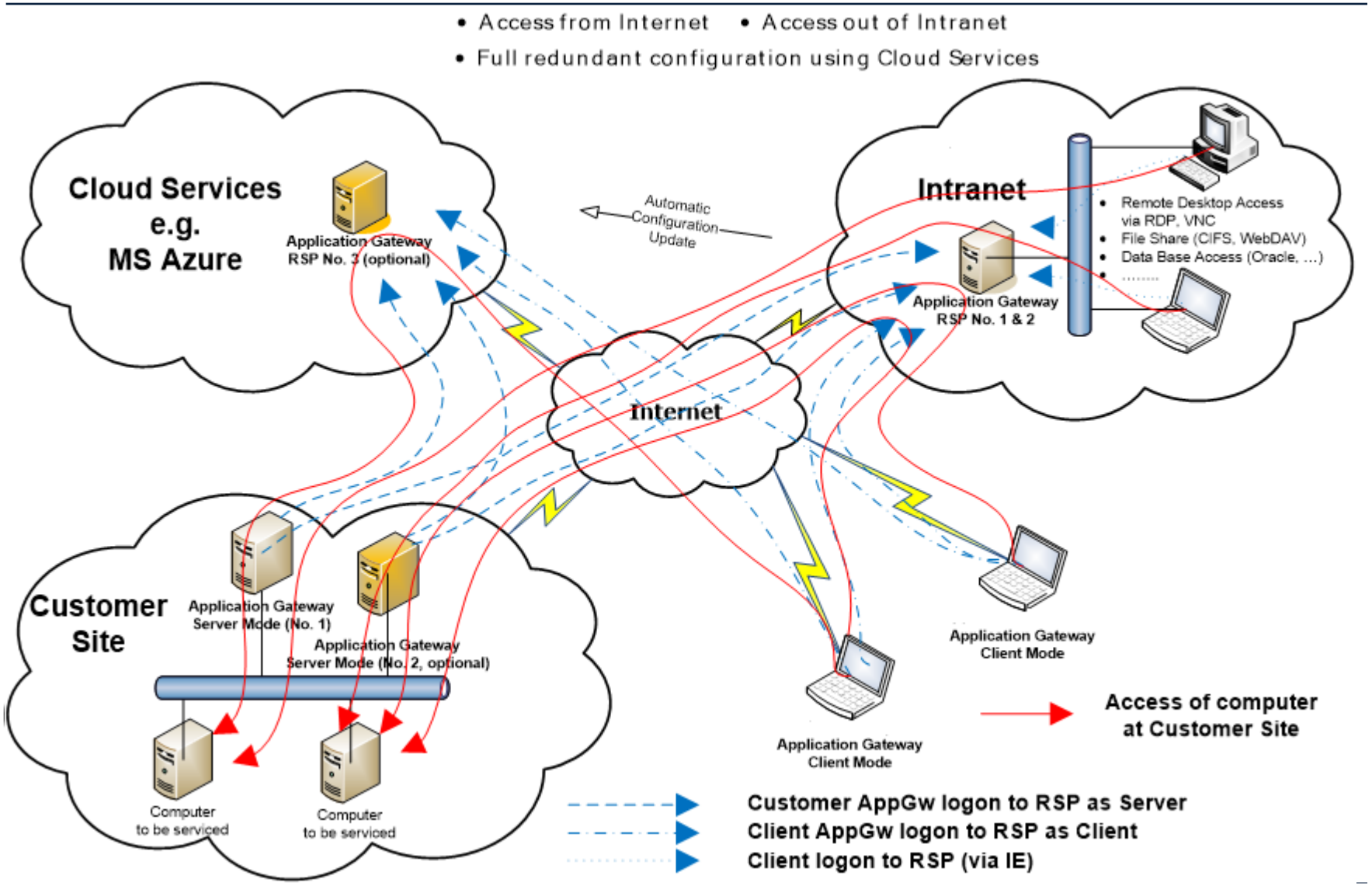
Logon with a web browser using a certificate or a One-Time-Password (see below):







Remote Access to Customer Site via RSP
RSP using Cloud Services



reinhold.leitner@applicgate.com

Remote Service Platform - FAQs (1)

- **How is the remote (customer) site connected to central RSP?**
  The Application Gateway at the remote site connects via public Internet to the official IP address of the central RSP installation, any TCP port can be used (usually port 443). Only outgoing connections (from the customers point of view)!
- **Which type of Internet access can be used at the remote site?**
  Any Internet access ((A)DSL, fiber, mobile etc.) can be used.
- **Are dynamic IP addresses for Internet access at the remote site allowed?**
  Yes, identification of the remote sites at the central Remote Service Platform depends on soft certificates and not on IP addresses of the sender.
- **Can the connections from the Application gateway be routed via web proxies at the remote site?**
  Yes, a web proxy at the remote site can be used.
- **Can I reach any computer at the remote site?**
  Depending on the restrictions of the remote site you can connect to any computer that is reachable from the Application Gateway computer at the remote site.
- **Can the customer control access to computers at the remote site?**
  Yes, the customer may enable and disable access via a web interface and all connections are logged in a log file on the customer machine at the remote site.

reinhold.leitner@applicgate.com

Remote Service Platform - FAQs (2)

- **How does the customer know when somebody connects to computers at the remote site?**
  The Remote Service Platform can send mails automatically to the customer when a connection is activated and/or when this connection is terminated. All connections are logged in a file. This log file can also be accessed via the web interface of the Application Gateway. Also the identity and e-mail address of the users are logged.
- **Does the customer have access to the configuration of the Application Gateway at the remote site?**
  Yes, all configurations can be controlled via web interface or via configuration files on the computer.
- **How are customer computers accessed by authorized users?**
  Users have to logon to the central Remote Service Platform using a certificate (soft certificate or smartcard) or One-Time-Password (transmitted via email or SMS). After successful authentication they can access the remote machines via predefined address/port combination. They will need the application credentials supplied by the customer in order to connect to a customer machine.

Remote Service Platform - FAQs (3)

- **How can the forwarding by the proxy functionality be restricted by the customer?**
  Filters with allowed addresses and ports can be configured at the customer instance.
- **Are there any passwords stored within the Remote Service Platform?**
  No, access to the Remote Service Platform is given based on certificates or One-Time-Password.
- **Where are the passwords and login information stored that are needed to logon to customer computers and applications?**
  This information is not stored in the Remote Service Platform and can be stored in any store with appropriate protection (e.g. protected network share, KeePass etc.).
- **Is the data encrypted during transmission?**
  Yes, between the central Remote Service Platform and the instance at the remote site the data is transmitted via a TLS encrypted channel.

reinhold.leitner@applicgate.com

Remote Service Platform - FAQs (4)

- **What is the required bandwidth for the Internet access at the remote site?**
  This depends on the requirements especially when uploading data.
  Please keep in mind that very often links to the Internet are asymmetric (high download bandwidth, low upload bandwidth). Very import is that the Internet connection is stable and has a low latency.
- **Is there any software installation at client machines necessary when the client is connected to the Intranet?**
  No.
- **Can a client access the remote (customer) site while not connected to the Intranet but connected to the Internet (e.g. business trip)?**
  Yes, in that case you have to run the a local installation of the Application Gateway (running in client mode) at your client.
- **Can customers access their own systems via Internet using the Remote Service Platform?**
  Yes, a local installation of the Application Gateway (running in client mode) is necessary on all clients that should be able to access the systems.
- **What about redundancy and high availability?**
  Application Gateways can be configured as hot-standby.

reinhold.leitner@applicgate.com

Contact

Reinhold Leitner

ApplicGate Network Security e.U.

Birkenweg 5

4048 Puchenau

Austria

Mobil: +43 (663) 03118601

E-mail: reinhold.leitner@applicgate.com

www.applicgate.com