

The background of the entire page is a night-time photograph of a city skyline, likely Frankfurt, with its illuminated skyscrapers and a river in the foreground. Overlaid on this image are various digital and network-themed graphics. A complex network of white lines and nodes connects different points across the cityscape. In the upper right, there is a line graph with two data series, one in red and one in blue, plotted against a grid. The graph's x-axis is labeled 'Hr' and has values from 22:40 to 23:50. The y-axis is labeled 'Power' and ranges from 16.0 to 19.5. The red line starts at approximately 17.5 and fluctuates between 16.5 and 17.5. The blue line starts at approximately 19.0 and decreases steadily to about 16.5. In the lower right, there is a teal rectangular box containing white text. At the bottom of the page, there is a white rectangular box containing a URL. The Siemens logo and tagline are in the top left corner.

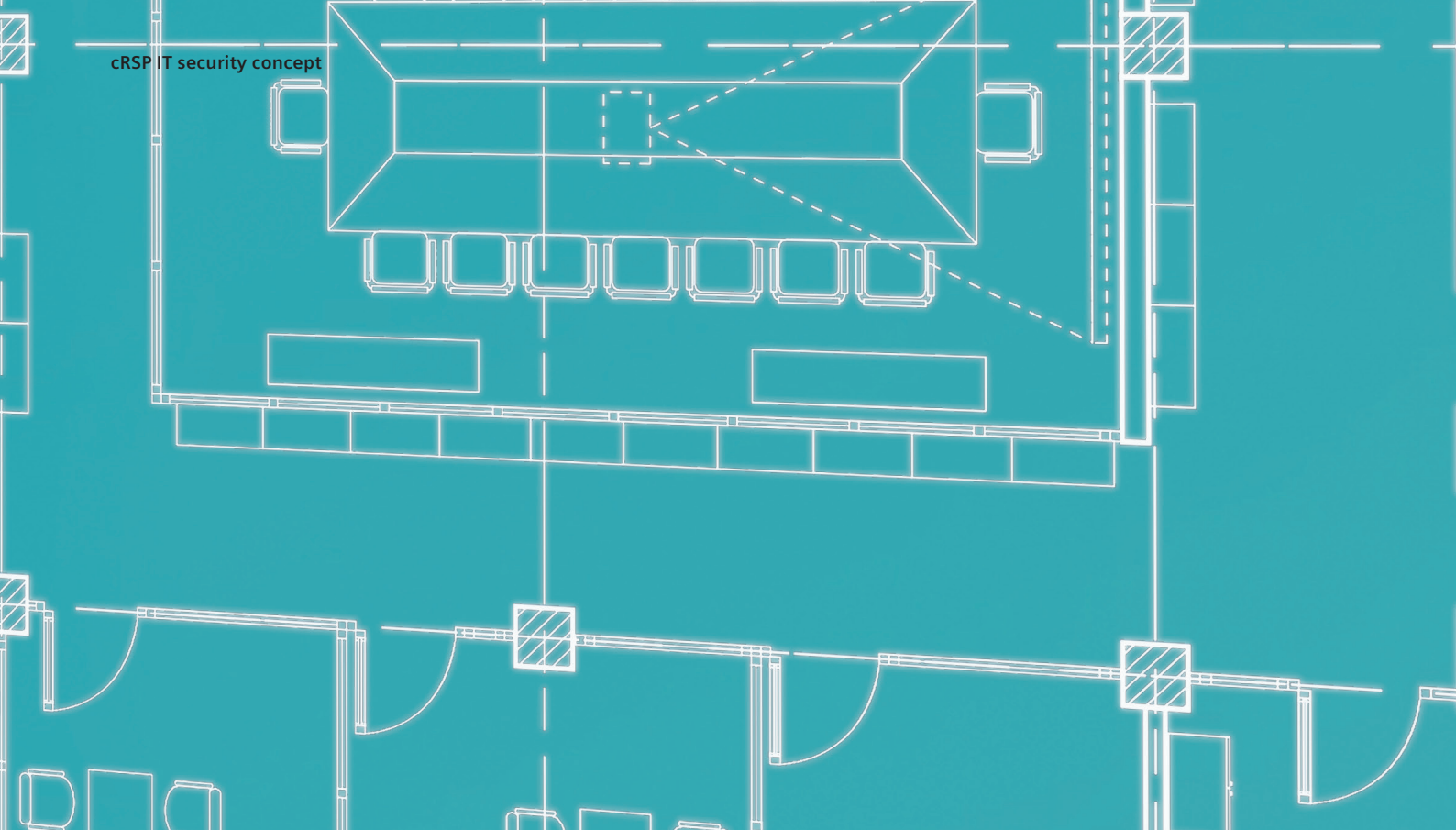
**SIEMENS**

*Ingenuity for life*

# cRSP IT security concept

[siemens.com/smart-infrastructure](https://www.siemens.com/smart-infrastructure)





#### Document objective

The Siemens common Remote Service Platform (cRSP) is the IT platform used throughout the group for implementing remote access to IP-based equipment. This security concept describes the measures that we at Siemens Smart Infrastructure take to protect customer data and IT systems when using our remote services. In its current version, this concept is applied to all our security, fire safety and building automation systems for which remote services are available over the entire life cycle.

#### Document layout

This document is divided into two main sections: general operating concept and technical security concept.


The first section, the general operating concept for remote services, discusses the fundamental aspects of information security within our company. The topic of remote services for building technology is introduced next, along with a look at the application-specific use cases for remote connections. This part also deals with the strategic security measures in the areas of data management and personnel selection, which are organizationally implemented for remote services.

It gives customers a general understanding of data security in remote connections.

The second section, the technical security concept, provides technical measures and advice on remote access, including access types and logging, secure IT infrastructure, protecting data transmissions and protecting against attacks.

The technical components, processes and procedures, such as authentication and authorization, are described in detail here. This part is therefore especially helpful for IT specialists who are interested in the type of connection or encryption methods.

Finally, you will find an overview of the various connectivity options in the appendix.



Data and information on building infrastructure must be available reliably, quickly, globally and securely.

Siemens common Remote Services meet all these requirements to the greatest extent.

## Contents

<b>Introduction</b>	02
<b>General operating concept</b>	04 – 07
<ul style="list-style-type: none"><li>• Data security</li><li>• Remote services</li><li>• Data management</li><li>• Personnel selection</li><li>• Platform availability</li></ul>	
<b>Certified technical security concept</b>	08 – 11
<ul style="list-style-type: none"><li>• Customer-controlled access</li><li>• Access scenario</li><li>• Authentication and authorization</li><li>• Network structure</li><li>• Virtual private network (VPN)</li><li>• Security measures on the Internet/customer network</li></ul>	
<b>Appendix</b>	12 – 13
<ul style="list-style-type: none"><li>• Connectivity options</li></ul>	

# General operating concept

## Data security as a basic requirement

Confidentiality and long-term partnerships are highly valued at Siemens. That is why we give the security of your data the highest priority. Before Siemens implements and enhanced service package with remote support, an in-depth analysis of the situation will be conducted, taking into account national and international regulations, technical infrastructures and industry specifics.

Our emergency call and service centers are available to you 24/7.

Trained specialists are also standing by to provide you with remote assistance.



## Remote services for building technology

As modern systems and solutions become more and more interconnected, we at Siemens take on the resulting challenge: we offer an extra service portfolio in addition to our existing on-site system service. It is based on remote support, thus providing an even higher level of flexibility and system availability.

The remote connection does not only make it possible to determine the causes of system issues faster and more efficiently, but also enables these issues to be solved quickly and intelligently from a remote location. Even in cases where remote repairs cannot be carried out, the information obtained in advance through remote diagnosis will help the service technician to provide our customers the best possible and highly efficient support on site. This means that our technician exactly knows what is to be expected on site and will have appropriate equipment at hand.

But that is not all. With our proactive services, provided according to the specific use case, Siemens takes preventive action to avoid errors instead of responding only after they have occurred, thus minimizing your system down times.

In addition to this, critical data (e. g. login data) will not be stored in the cRSP.

Within the scope of our proactive services data will be sent on a regular basis via the existing secured connection from the systems to Siemens. This connection will be established after a successful authorization (see "Authentication and authorization" below).

## Use cases for remote services

Below is a list of use cases, which may vary according to access type and duration.

Remote commissioning: support for commissioning systems, customizing the configuration/supply

- Operational assistance: Customer support in operating the system
- Remote diagnosis: Advance diagnosis of faults from a remote location, collection of diagnostic information for technician deployment
- Remote repair: Restoring operation, clearing faults, customizing the configuration/supply
- Maintenance support: Preparation and support for maintenance and repairs, downloading updates and patches
- Performance monitoring: Electronic monitoring of the system for faults, threshold values and states

## The remote advantage

Remote service provides additional support to optimally service your fire safety, security and building automation systems in the face of growing complexity.

The advantages of cRSP include

- Remote monitoring to proactively detect and correct interruptions in order to minimize system downtimes
- Faster and more efficient determination of the causes of system problems
- Fast, intelligent correction of problems through remote intervention
- Service engineers arrive on site already well informed and optimally equipped
- Fast user support for application issues
- Ability to escalate support





### Data management

Siemens treats your data as confidential and grants access only on a need-to-know basis. The implementation of this principle is supported by rule-based access mechanisms, which are mapped within an infrastructure and tool landscape designed specifically for this purpose. The data management measures implemented depend on your data protection requirements, the type of data and the provisions of applicable regulations.

### Personnel selection

Our service technicians and experts are aware of the need for confidentiality in handling your data and know the serious consequences of failure to comply with the relevant regulations. As a result, only employees who have been trained in data protection and IT security are allowed to work in our Remote Service Center. Siemens has strict selection criteria, and our service technicians must participate in ongoing training and processes. Your data is thus always in safe hands

### Platform availability

The availability of our remote services is secured by three data centers in Germany, Singapore and the United States. The capacity of each center was designed so that the cRSP platform remains unaffected in the event of a malfunction. The integration of additional plans for disaster recovery (DR)

and business continuity management (BCM) ensures the highest possible availability of our remote services.

### Siemens CERT auditing

The Siemens Computer Emergency Response Team (CERT) is an internal, independent and trustworthy partner which develops preventive security measures and assesses the information security of the IT infrastructure.

### Certification

Siemens was one of the world's first organizations to implement an internationally valid information security management system (ISMS) according to ISO/IEC 27001 for remote services. Our cRSP platform is audited regularly for effective protection and continuous improvements.



### You determine how access takes place

As a basic requirement, you must contractually authorize every service activity. Access is designed to only be granted for the contractually agreed use cases.

To enable access to your systems from outside the Siemens network, the Customer Web Portal (CWP) with enhanced security requirements (2 factors authentication) has been established. In addition to just setting up a connection, you also have the option of explicitly barring access to individual destinations and enabling them again only when needed. Combined with the retrieval of log files on successful access attempts, this gives you always control over remote access to your system.

### Access scenario example

- The customer has the possibility to lock all connections or just specific systems. The service technician requiring access to a locked system needs to contact the customer. The customer can then log in to CWP and unlock the required connection. After that, the technician can connect and implement the necessary service tasks remotely. When the service is finished, the customer can lock the connection again.
- Full access: an expressly authorized service engineer has the customer's permission to connect to the system at any time. Each system access is automatically logged for customer review. Customers commonly choose to grant full access when proactive preventive maintenance and highest possible system availability are their key considerations.
- In real time or at agreed intervals. This makes it possible to collect statistical data for system optimization, proactive fault management and services. Siemens works closely together with the customer to ensure that only the agreed type of data is transmitted.





### Authentication and authorization of Siemens service personnel

The central backend of the cRSP platform is in a separate segment within the Siemens intranet.

Siemens therefore issues PKI certificates for employees. Every time a service technician logs into the cRSP portal, her / his access rights are verified based on PKI, a strong authentication method using a smart card. The access models you define are then mirrored within our cRSP platform and converted to authorized IT system access levels. These access levels are then matched to the service technicians verified identity.

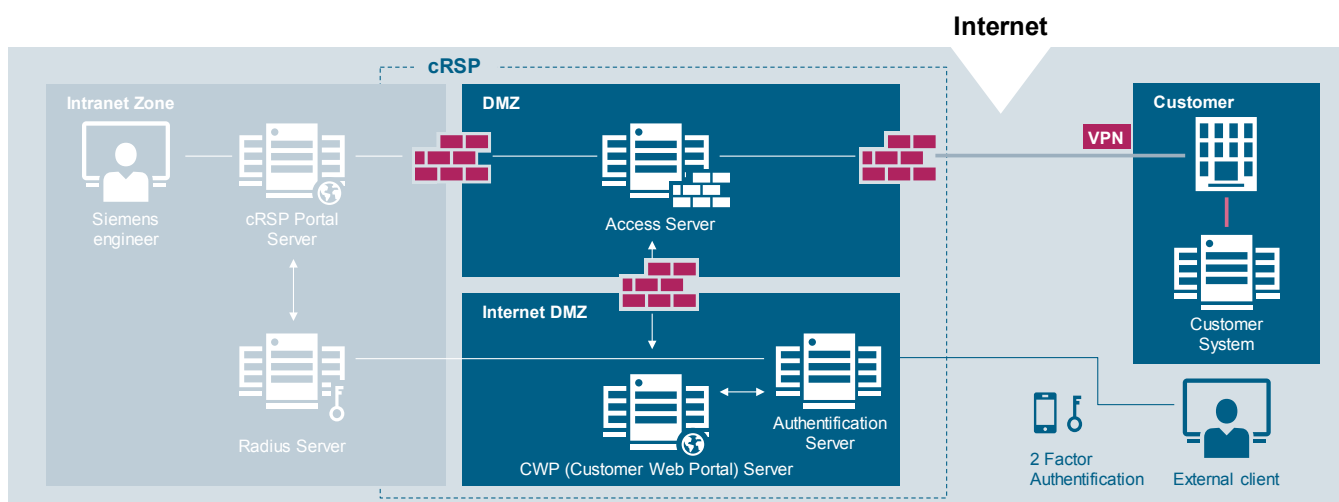
Using this procedure means that service technicians can access only those areas of your system for which they have been expressly authorized ahead of time.

### Authenticating and authorizing your personnel

To enable you to access your systems outside the Siemens network, the Customer Web Portal (CWP) with enhanced security requirements (two factors authentication) has been established.

The CWP itself is within the Siemens DMZ (Demilitarized Zone; see Network structure for more information). Established users and their authorizations, like Siemens intranet users, are stored on a server in another network segment. Authentication takes place in the CWP with the user ID, a password and a mobile PIN. If you need to access the web portal, enter your user name and password as well as your mobile PIN or email.

If you have any questions or need assistance, please contact your usual local country organization.



# Technical security concept

## Network structure

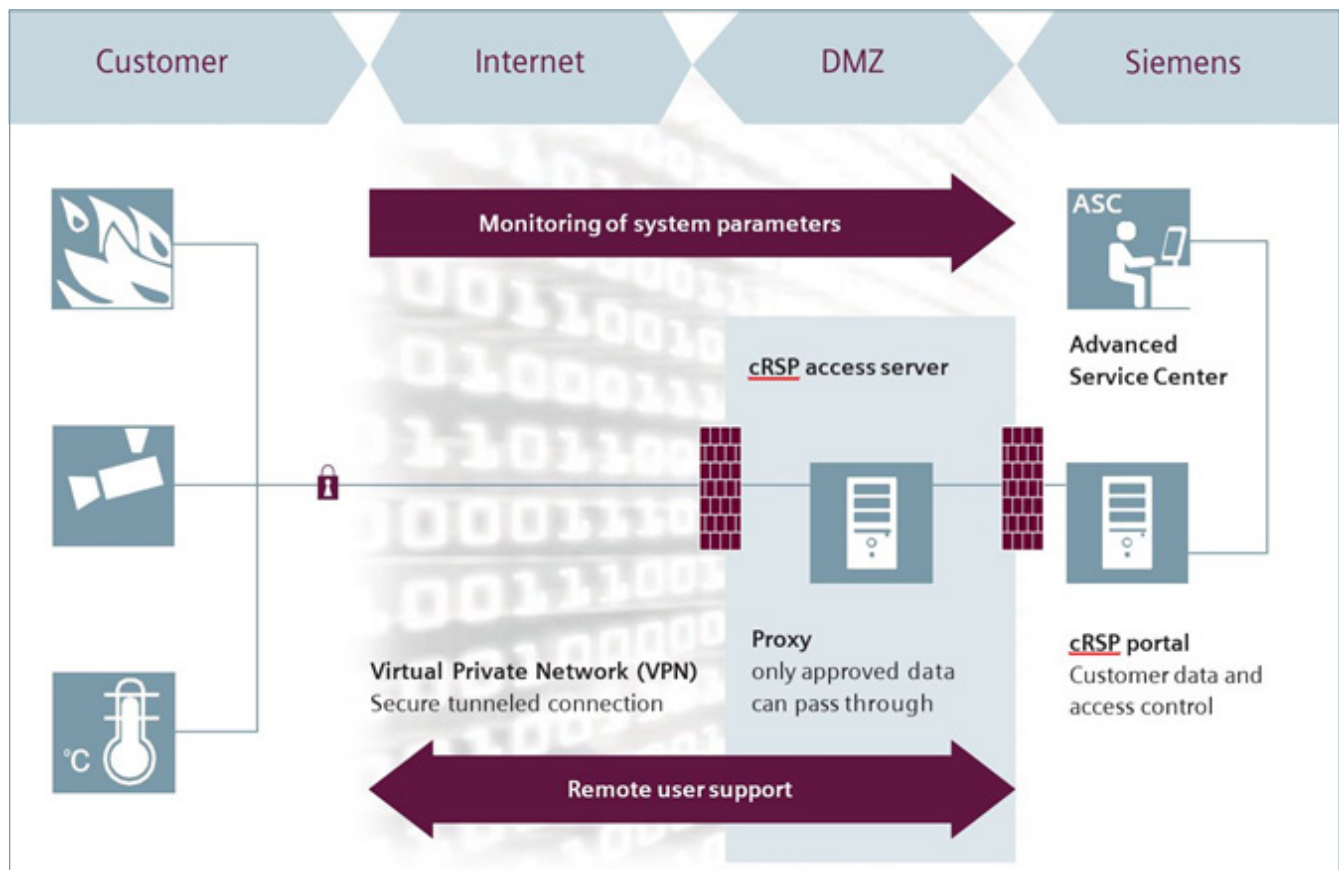
To protect your network as well as the Siemens intranet against threats, Siemens has secured the cRSP infrastructure in a DMZ. Service technicians do not set up end-to-end connections to your systems or vice versa. Instead, the connections end in the DMZ, which is secured on both sides by firewalls. The reverse proxy server establishes the connection to your system and mirrors the incoming communication to the Siemens intranet. This prevents a connection from being set up between the Siemens intranet and your network using unauthorized protocols, since the mirroring (procedure) only works with predefined protocols.

This architecture prevents, for example:

- Unauthorized access from one network to the other
- Access from a third network (by unauthorized systems and users)
- Fraudulent use of secret passwords, access data, etc.
- The transmission of viruses or other harmful programs from one network to the other

## Virtual private network via a broadband connection

**cRSP always uses** a secure VPN tunnel over a broadband internet connection. This offers the following advantages: a maximum level of security, high data transfer rates, high availability.

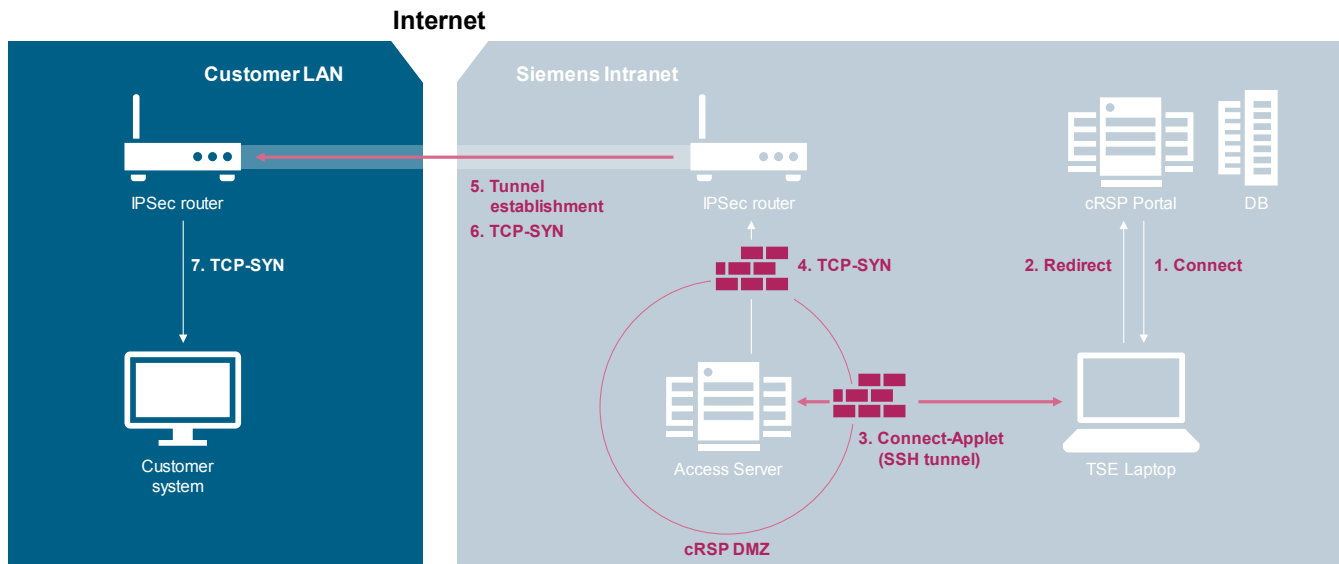




### Security measures for IPsec

Siemens uses the established standard IP Security (IPSec) with preshared secrets for encrypted and authenticated data transmission. A minimum recommended configuration is: Preshared secrets consist of an arbitrary string of minimum 12 random characters. The Internet Security Association and Key Management Protocol (ISAKMP) is used to exchange securely encryption key

information. Encrypted secure payload (ESP) ensures data confidentiality through an AES-256 encryption while the SHA2 hash method offers integrity and authenticity of your data. Diffie Hellman key exchange with a key size of 2048 bit (group 14) is used for key exchange security and Perfect Forward Secrecy (PFS).

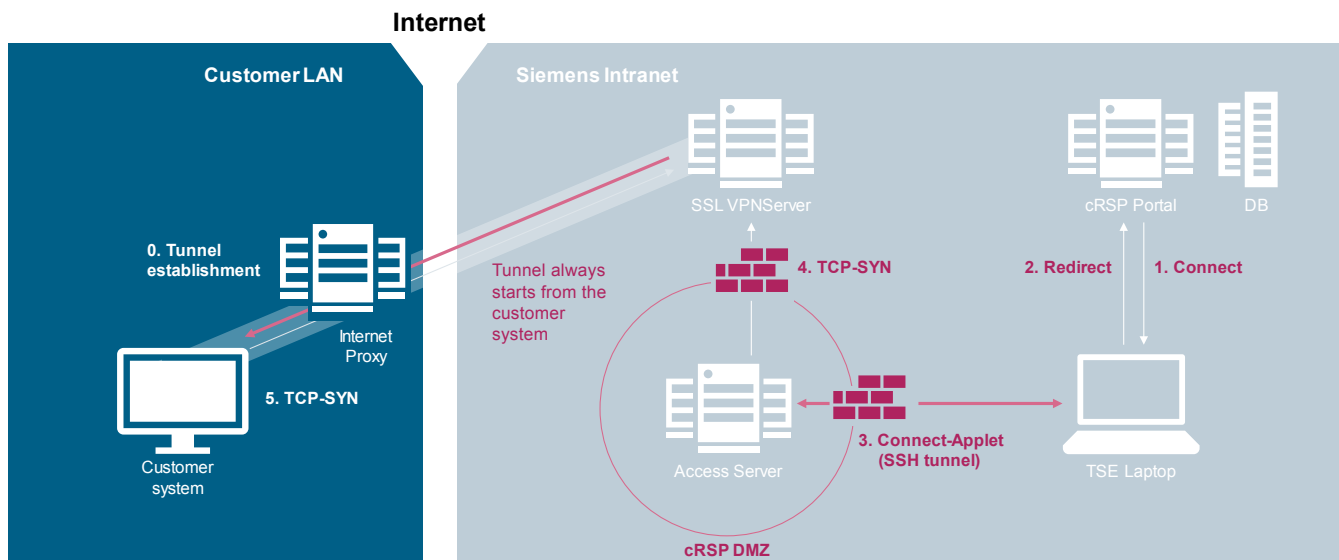


### Security measures for SSL-VPN

As an alternative to IPsec VPN Siemens also provides a solution based on SSL VPN (using state-of-the-art TLS 1.3). This solution can be installed on windows or linux (only specific distributions are supported). It is also installed on the DigitalizationBox and on the Remote Solution Gateway.

Before a connection is set up, the device must be registered with a one-time pass-

word (OTP). This OTP is generated using the system's unique data and is valid only for its registration process. The SSL connection to the VPN server can be established only if the server certificate was signed by an internal Siemens Certification Authority (CA). This ensures that only this specific device is able to communicate with the cRSP servers. An additional hardware-based hash ensures that no unauthorized device can set up a connection to the cRSP (system cloning)



### Security measures in the customer network

The following section provides a list of the protocols and services used. Should you need any other specific security measures or customized firewall functions for special applications, network segments, etc., they are available depending on your choice of connectivity options.

#### Protocols

Depending on the product type to be serviced, various protocols are supported by the cRSP secured connection to the customer system

- The HTTP protocol (preferably HTTPS)
- Microsoft Remote Desktop, Telnet, PuTTY, NetOp, WinVNC; Anydesk
- BACnet
- A large range of UDP based connectivity products (e.g. FS20 fire systems)
- Other protocols, if needed
- Ftp/sftp (file transfer protocol, secure file transfer protocol)

### Secured cRSP server

Our backend exclusively consists of hardened systems which are designed for stability. Moreover, frequent updates make sure that actively developed distributions remain secure. According to the current state of the art, infections by worms, viruses, Trojan horses and other attacks therefore remain highly unlikely. In addition, our secured cRSP servers as well as the encrypted databases on these servers are in accordance with the most recent security guidelines. The effectiveness of these protection measures is audited (ISO/IEC 27001:2013) on a regular basis ensuring that the cRSP servers are operated with state-of-the-art technology.



*“The risks are manageable  
if the industry relies on a  
universal security concept.”*

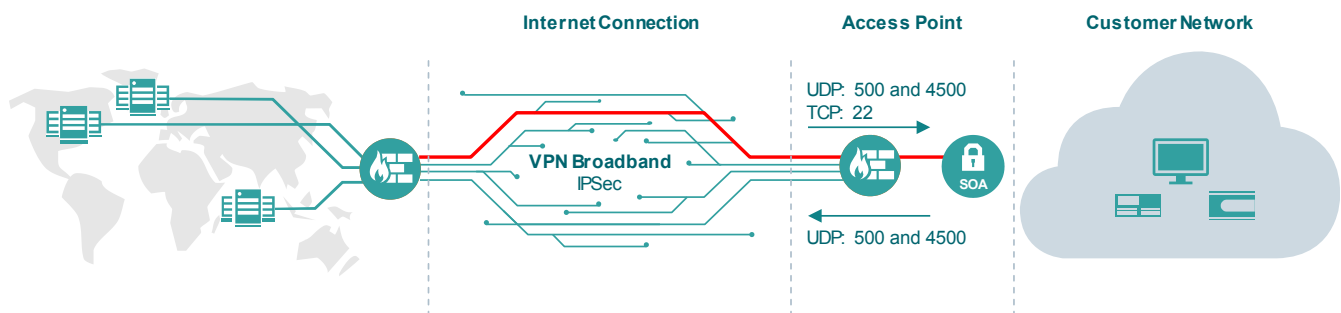
Dr. Rolf Reinema,  
Head of the IT Security Technology Field  
within the Research and Development Department  
of Siemens, Corporate Technology (CT)

# Appendix

## IPsec

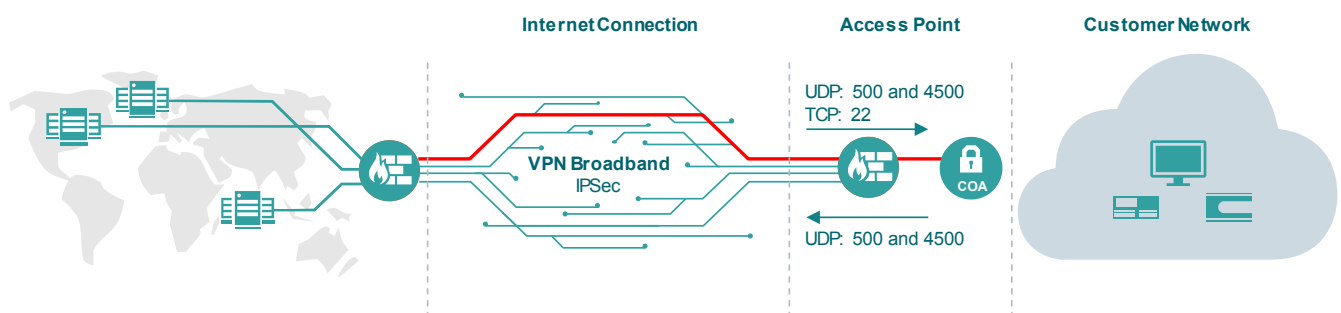
### Siemens Owned Access

Connection between cRSP infrastructure and customer network is performed through a router provided by Siemens.



### Customer Owned Access

Connection between cRSP infrastructure and customer network is performed through a customer router or it ends at the customer's firewall.

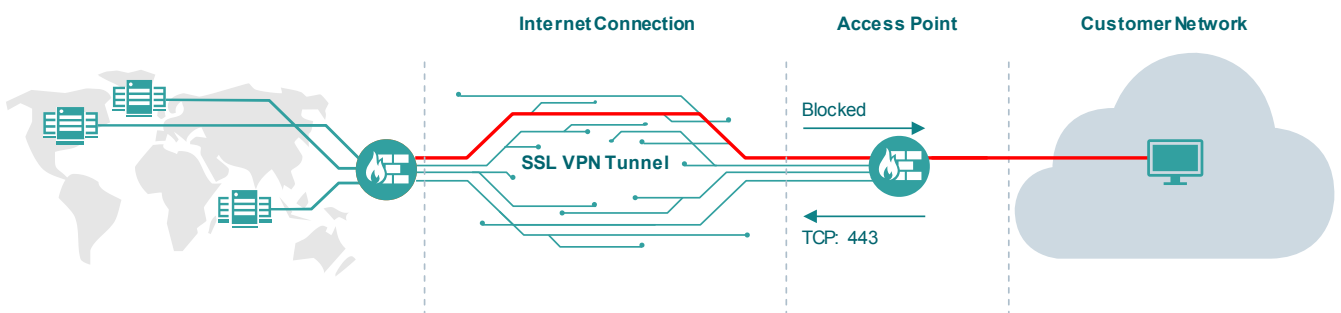




# SSL VPN

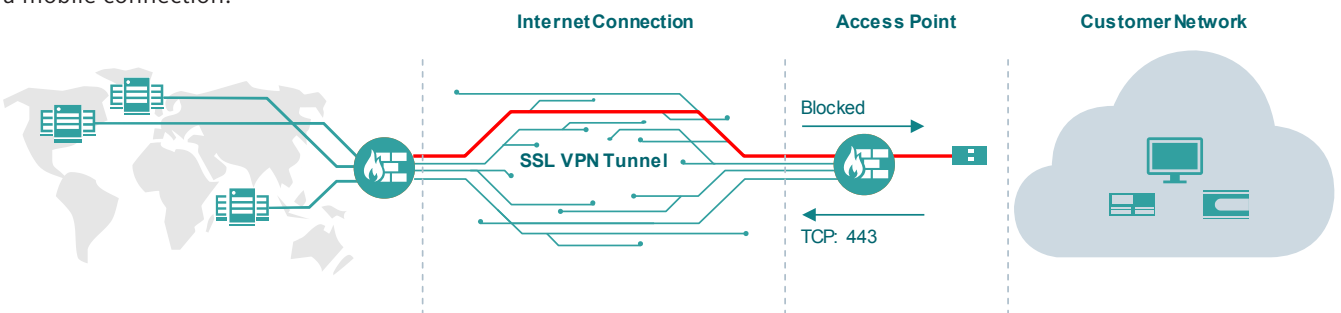
## Internet Based Connection

Each equipment is connected to cRSP through internet and utilizes a secure SSL VPN tunnel. Access to internet is provided by the customer.



## DigitalizationBox/Remote Solution Gateway

Connection between cRSP infrastructure and customer network is performed through a router provided by Siemens. Access to internet is provided by the customer or over a mobile connection.



People spend about 90 percent of their time indoors.

Improve the places where they spend their lives  
and you improve their lives.

With our people and technology, our products  
and services, our aim is to create perfect places.

For every stage of life.

When building technology creates  
perfect places – that's Ingenuity for life.

Creating environments that care  
[siemens.com/smart-infrastructure](https://www.siemens.com/smart-infrastructure)

Article no. BT\_0123\_EN (Status 07/2019)

Subject to changes and errors. The information  
given in this document only contains general  
descriptions and/or performance features which  
may not always specifically reflect those described,  
or which may undergo modification in the course  
of further development of the products.

The requested performance features are binding  
only when they are expressly agreed upon in the  
concluded contract.

