



# SIEMENS

*Ingenuity for life*

## cRSP IT security concept

[siemens.com/bt/services](https://www.siemens.com/bt/services)

#### Document objective


The Siemens Remote Service (SRS) platform 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 Building Technologies take to protect customer data, applications 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 parts: General operating concept and Technical security concept. The first main part, the General operating concept for remote services, discusses fundamental aspects of data protection and 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 in our certified information security management system (ISMS).

It gives employees and customers a general understanding of data security in remote connections. The second main part, 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, such as Siemens Owned Access (SOA), Customer Owned Access (COA), among other things.





Data and information on building infrastructure must be available reliably, quickly, globally, securely and in protected form. Siemens Remote Services meet all these requirements to the greatest extent possible.

## Contents

<b>Introduction</b>	02
<b>General operating concept</b>	04 – 05
• Data security	
• Remote services	
• Data management	
• Personnel selection	
• Platform availability	
<b>Certified technical security concept</b>	06 – 09
• Customer-controlled access	
• Access models and logging	
• Authentication and authorization	
• Network structure	
• Virtual private network (VPN)	
• Security measures on the Internet/customer network	
<b>Appendix</b>	11 – 15
• Connectivity options	

# General operating concept

## Data security as a basic requirement

We value confidentiality and long-term partnerships. That is why we give the security of your data the highest priority. Before we implement an enhanced service package with remote support, we conduct an in-depth analysis of the situation, taking into account national and international regulations, technical infrastructures and industry specifics. Our service employees carefully evaluate your needs on an individual basis with a view toward information security and data protection.



## 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 and thus provides an even higher level of flexibility and system availability. The remote connection not only makes it possible to determine the causes of system problems faster and more efficiently, but also enables these issues to be corrected quickly and intelligently from a remote location. Even in cases where remote repairs cannot be carried out, the information obtained through diagnosis can provide the service technician with the best possible support on site. The technician thus knows exactly what to expect when arriving on site and has the appropriate equipment at hand. But that's not all. With our proactive services, provided according to the specific use case, we take preventive action to avoid faults instead of responding only after they have occurred, thus minimizing your system down times.

## Use cases for remote services

Remote connections offer specific use cases for systems in all disciplines, which can extend over the entire life cycle, depending on availability. 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 SRS 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 SRS 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

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

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



### Data management

We treat your data as highly confidential and grant 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. We can provide comprehensive consulting on data storage, backup, ownership rights and data destruction for individual solutions.

### 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 conditions. As a result, only employees who have been trained in data protection and IT security are allowed to work in our Remote Service Center. We have strict selection criteria, and our service technicians must participate in ongoing training and validation processes. Your data is thus always in safe hands.

### Platform availability

The availability of our remote services is secured by three fully redundant data centers in Germany, Singapore and the United States. The capacity of each center was designed so that the SRS platform

remains unaffected in the event of a malfunction, provided that two of the data centers do not completely shut down unexpectedly. 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 Cyber Emergency Readiness Team (CERT) is an internal, independent and trustworthy partner which develops preventive security measures and assesses the information security of the IT infrastructure. Our SRS platform is audited on a regular basis to ensure valid protection and continuous improvement.

### 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. The Siemens Cyber Emergency Response Team (CERT) is an internal, independent and trusted partner which develops preventive security measures and evaluates the information security of the IT infrastructure. Our SRS platform is audited regularly to ensure effective protection and continuous improvements.



# Technical security concept

You maintain control over the remote access to your systems at all times.

## You determine how access takes place

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

To enable you to access your systems from outside the Siemens network as well, we have established the Customer Web Portal (CWP) with enhanced security requirements. 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 control over remote access to your system at all times.

## Access models

Some of the access models that our customers prefer for remote services are:

- **Connection on request:** A customer system can be accessed only upon individual request. For example, a service technician can request access for a limited period of time in order to clear a specific fault. This access is not continuous. The type of access can be contractually agreed and also defined in the customer's firewall settings.
- **Supervised access:** The customer can follow the service technician's work on the system in real time by remote desktop sharing. The range of services for this option and the technical resources for limiting the access to this level are mutually agreed upon.
- **Outbound communication:** The customer's system sends information to the Siemens Service Center via the SRS platform – 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.
- **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.



### Access logging

Each direct access to your system is recorded in the SRS platform and provided with a time stamp. The log also records the unique user ID of the particular service technician. We can thus let you know within an appropriate length of time which of our service technicians accessed your data and when this took place. We save these access logs for a period of at least one year.

### Authentication and authorization of Siemens service personnel

The central user interface of the SRS platform is in a separate segment on the Siemens intranet.

Siemens therefore issues digital certificates (so-called digital IDs) for employees and business partners according to the provisions of the Public Key Infrastructure Disclosure Statement (PKI). Every time a service technician logs into the SRS portal, his access rights are verified on the basis of PKI, a strong authentication method using a smart card. The access models you define are then mirrored within our SRS platform and converted to authorized IT system access levels. These access levels are then matched to the service technician's 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. Therefore, they cannot access other areas within the customer network that are not maintained by Siemens.

### Authenticating and authorizing your personnel

To enable you to access your systems from outside the Siemens network as well, we have established the Customer Web Portal (CWP) with enhanced security requirements.

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. The PIN number will be sent to your mobile phone number stored in your user account and must be entered within a period of three minutes. Otherwise, you must restart the authentication process. If you have any questions or need assistance, please contact your usual local country organization.

### Traceable audit trail

Siemens is always able to inform customers which service engineer had access to which data, and when and what communication activities were performed on each system. This audit trail is enabled by the following measures:

- Every single access to a customer system is recorded. Entry and exit time stamps as well as the engineer's identity are applied.
- Report logs are kept on file for at least twelve months, and retention may be extended at the customer's request. Customer requests to include supplementary information in the audit trail can be taken into account as far as they are technically possible.

### Verified partner access only

Some services might need the involvement of external service and engineering partners. To ensure the same reliable level of security is maintained in such cases, our SRS platform features a partner access mechanism.

Following successful completion of a very thorough and strictly enforced authentication process, verified business partners are granted access to a specifically-defined area of a customer system via the SRS platform.

Siemens issues digital certificates (so-called digital IDs) for employees and business partners according to the provisions of the Siemens Public Key Infrastructure (PKI).

### Network structure

To protect your network as well as the Siemens intranet against reciprocal problems and attacks, we have secured the SRS server in a so-called 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 via unauthorized protocols, since the mirroring takes place only for predefined protocols. This architecture prevents, for example:

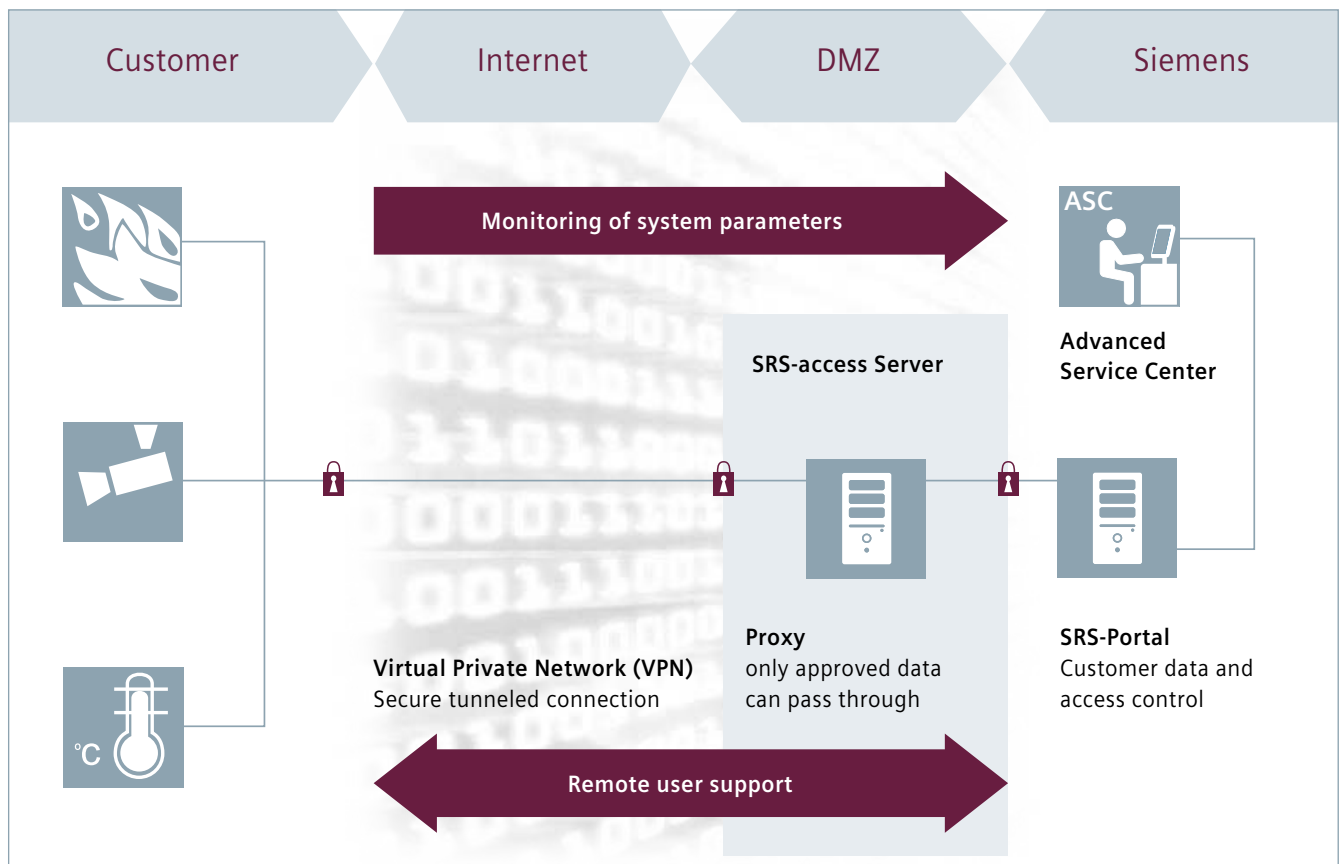
- unauthorized access from one network to the other
- access from a third network (by hackers, for example)
- fraudulent use of secret passwords, access data, etc.
- the transmission of viruses or other harmful programs from one network to the other

### Virtual private network via a broadband connection

We generally recommend using a secure broadband connection over the Internet. This offers the following advantages: a maximum level of security, high data transfer rates, high availability and access to all Siemens Remote Services.

An IPsec-secured VPN connection between the Siemens DMZ and your network access is a very secure technical solution. For mobile systems, we also offer an SSL-based VPN connection between the system and the DMZ. If a suitable infrastructure is already in place, our technicians will be happy to coordinate the parameters needed for a connection with you, which must then be secured against unauthorized changes. If you do not have a VPN end point for a connection, Siemens will provide you with a Cisco router. The VPN end point at our end (in the DMZ) is also a Cisco router.

Also keep in mind that, in rare instances, you will not be able to set up an operational connection with routers from other manufacturers, due to compatibility problems. If this is the case, do not hesitate to contact our regional consultants for advice.





### Security measures for IPsec

Siemens uses the established standard IP Security (IPsec) with preshared secrets for encrypted and authenticated data transmission. 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) provides data confidentiality through encryption with algorithms AES or AES-GCM (AES-128, AES-192, AES-256, AES-GCM 128, AES-GCM 192, AES-GCM 256) and ensures the integrity and authenticity of your data using the Hash method SHA-256, SHA-384, or SHA-512. Various Diffie Hellman Groups (5-1536 bit, 14-2048 bit, 15-3072 bit, 16-4096 bit, 19-256 bit ec, 20-384 bit ec, 21-521 bit ec, 24-2048/256 bit) is used for key-exchange security and Perfect Forward Secrecy (PFS).

### Security measures for SSL-VPN

The Secure Socket Layer (SSL) protocol can be used as an alternative for hardware based VPN endpoints (IPsec). Before a connection is set up, the device must be registered with a one-time password (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 SRS servers. An additional hardware-based hash ensures that no unauthorized copy software can set up a connection to the SRS server.

### Security measures in the customer network

In light of the security aspects that need to be considered, specific measures must be taken to access your network from the outside. The main security features depend on the selection and configuration of the chosen SRS access router at the customer's end. In principle, a distinction is made between Customer Owned Access (COA) and Siemens Owned Access (SOA). In addition, two more options are available for fixed and mobile connections. These connectivity options, including the ports to be opened in the firewall for an operational remote connection, are illustrated and explained in detail in the appendix. 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

The following protocols can be used for remote access, depending on the system:

- the HTTP protocol (preferably HTTPS)
- RPD, Telnet, PuTTY, NetOp, WinVNC; Citrix/MS-Terminal Server; X.11 service tools/protocols
- BACnet
- A large range of UDP based connectivity products
- other protocols, if needed

When transmitting data during diagnosis, only the technical data needed is sent automatically from the system to the SRS platform. The following services are used, depending on the system:

- ftp/sftp (file transfer protocol, secure file transfer protocol)
- or, as an option, other services of other system management services.\*
- Transparent proxy:
- The cRSP transparent proxy can be used with most cRSP applications with the option parameter "useTransparent-Proxy". It is specifically created for connections that use applications that do not support proxy connections. The solution maps the remote system's actual IP address (configured in the real host IP address) to a local network address. Note that the first time the transparent proxy is used, a \*.msi installer is installed on the client (administrator rights required).

### Client site requirements

- Current Java version
- Web browser
- Supported operating systems and web browsers. See CWP login page for details.

### Secured SRS server

We use Linux servers exclusively for our SRS access servers. Linux is the top choice for a server operating system since, as a Unix system, not only is it designed for stability, but also 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 SRS servers as well as the encrypted databases on these servers are always state of the art.

Public IP addresses of the productive cRSP DMZ:

- DMZ Fuerth (Germany): 194.138.37.194
- DMZ Malvern (USA): 12.46.135.194
- DMZ Singapore: 194.138.240.119

\* Please contact your regional consultant for more information.

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

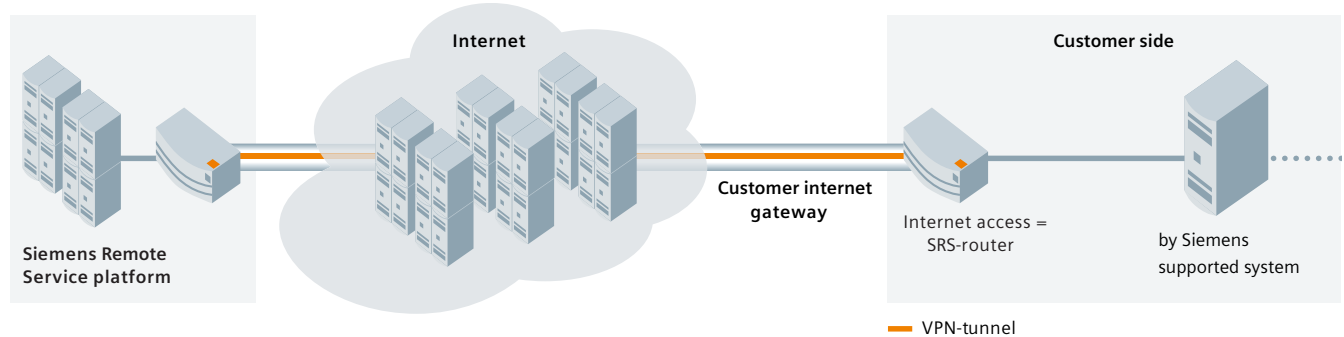
**Dr. Rolf Reinema, head of the IT Security Technology Field  
within the Research and Development Department of  
Siemens, Corporate Technology (CT)**

# Appendix

Information on how to implement a connection to your systems with the Siemens Remote Service platform is provided below.

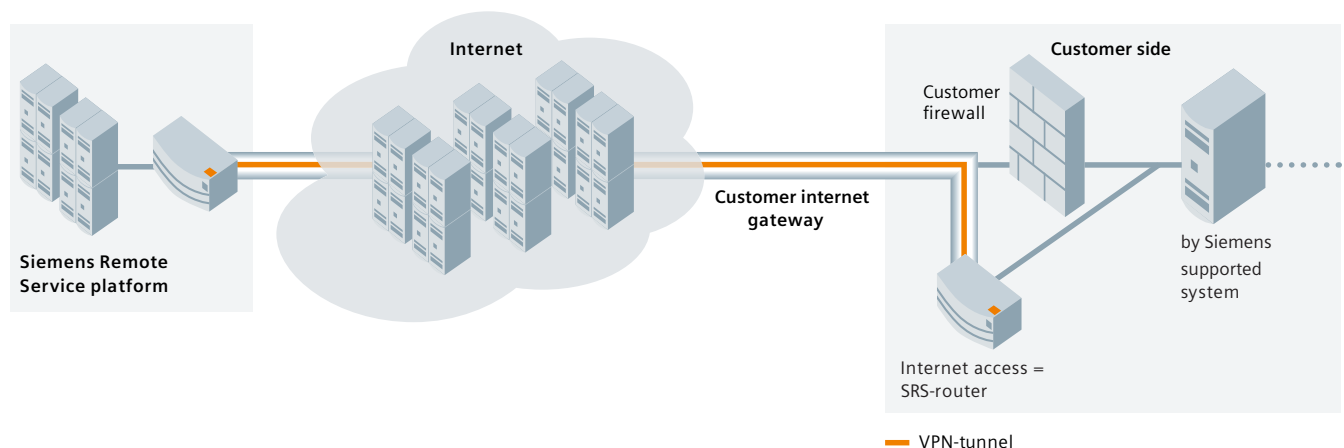
## Siemens Owned Access (SOA) directly

In this case, the Internet connection ends directly at the SRS access router. No additional gateway is needed.



## Siemens Owned Access (SOA) bypasses the customer's entire firewall

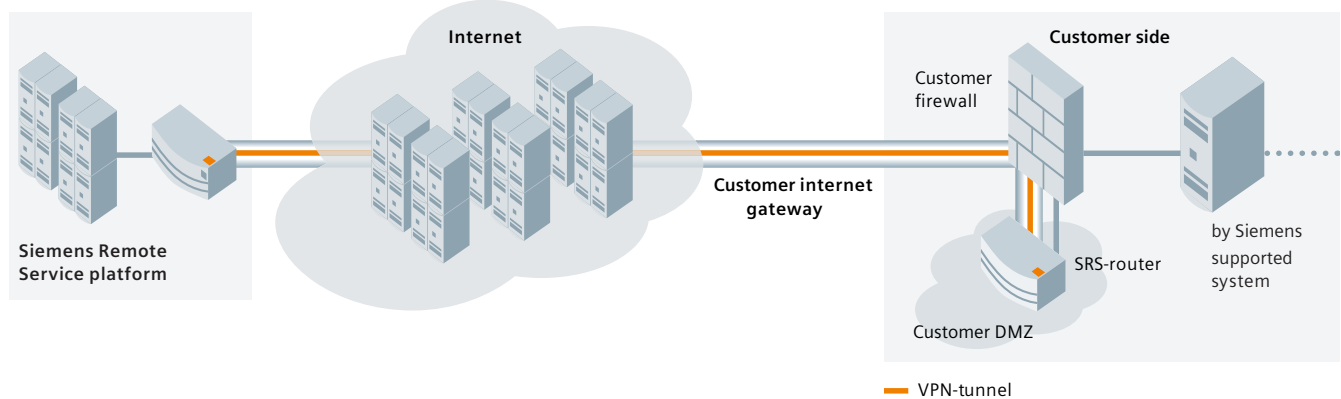
In this case, the SRS access router bypasses the customer's entire firewall. This solution should be selected only if the customer's firewall is not capable of forwarding the VPN traffic to a device in the customer network and also does not have a DMZ.





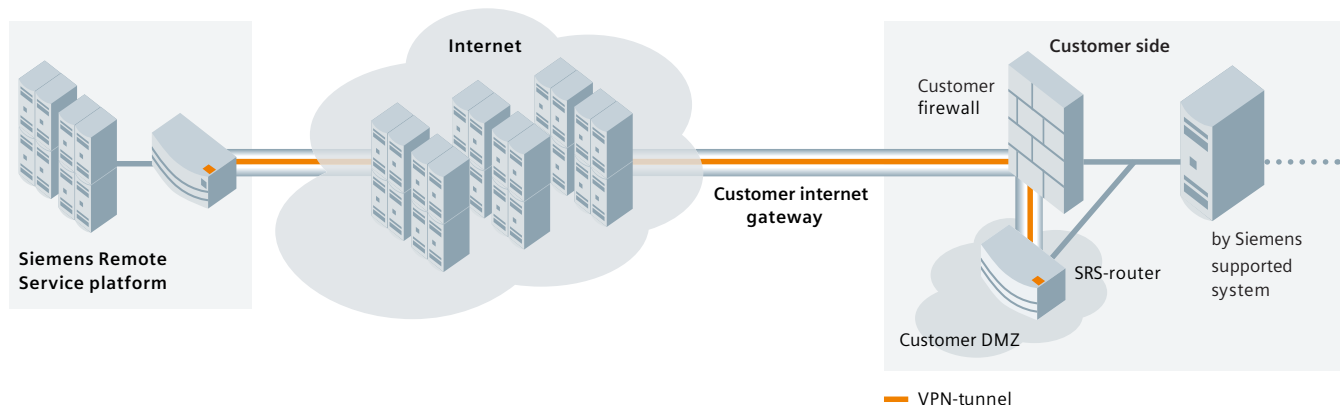
### Siemens Owned Access (SOA) router is located in the customer's

In this case, the Internet connection ends at the customer's system, but the VPN tunnel continues to end at the Siemens router. The Siemens router is located in the customer's DMZ, behind the firewall. SSH (TCP port 22), ISKMP (UDP port 500/4500), ESP (IP protocol number 50) and AH (IP protocol number 51) are needed for forwarding to the SRS access router (WAN address).



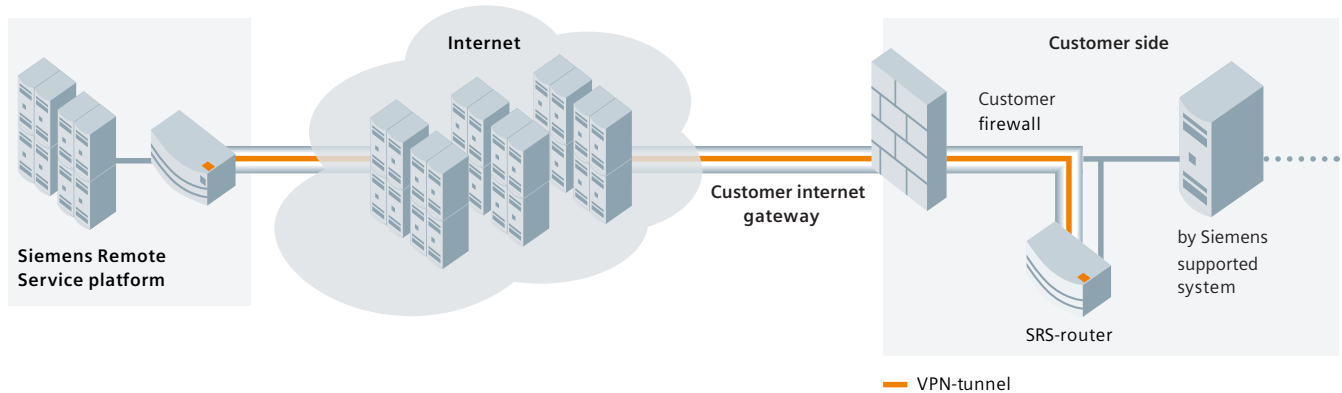
### Siemens Owned Access (SOA) router is in the DMZ of the customer's firewall, but the LAN interface is connected directly

In this case, the Internet connection is set up from the customer's system, but the VPN tunnel ends at the Siemens router. The router is in the DMZ of the customer's firewall, but the LAN interface is connected directly to the customer's network. SSH (TCP port 22), ISKMP (UDP port 500/4500), ESP (IP protocol number 50) and AH (IP protocol number 51) are needed for forwarding to the SRS access router (WAN address).



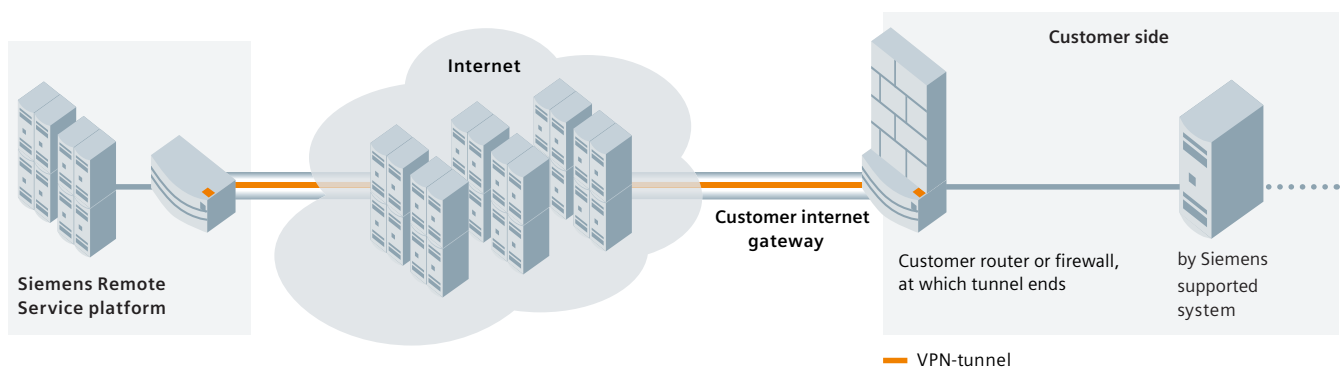
### Siemens Owned Access (SOA) router is placed within the customer network

In this case, the Internet connection ends at the customer's system, which, however, is not capable of terminating the VPN tunnel. In addition, the system does not have a DMZ in which the router can be placed. The Siemens router is placed within the customer network. SSH (TCP port 22), ISKMP (UDP port 500/4500), ESP (IP protocol number 50) and AH (IP protocol number 51) are needed for forwarding to the SRS access router (WAN address).



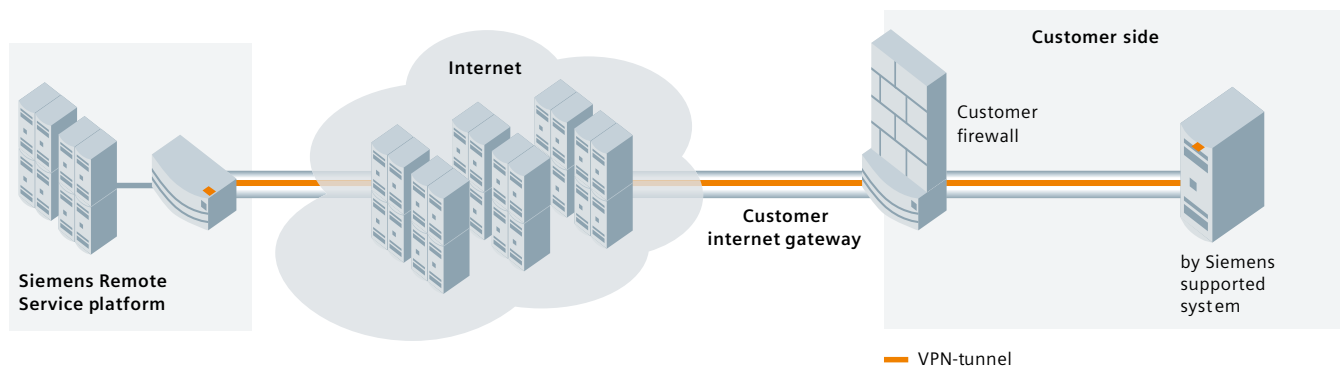
### Customer Owned Access (COA)

In this case, the Internet connection and the VPN tunnel end at the customer's firewall. All necessary parameters are verified between the contact people.



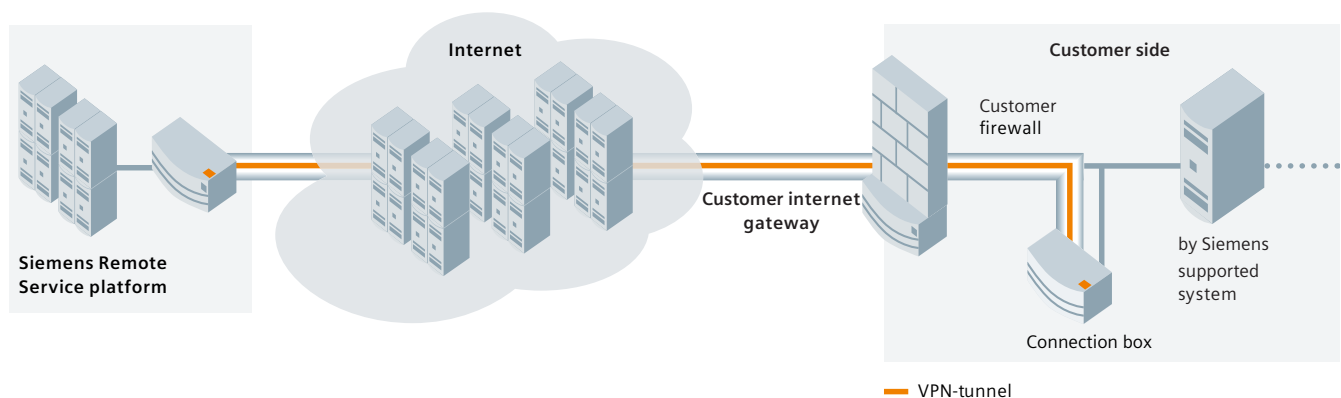
### SSL VPN client

In this case, the Internet connection ends at the customer system, but the VPN tunnel ends with an SRS SSL client directly at the supported system. TCP port 443 from the inside to the outside must be opened in the customer's firewall.



### Connection box via COA

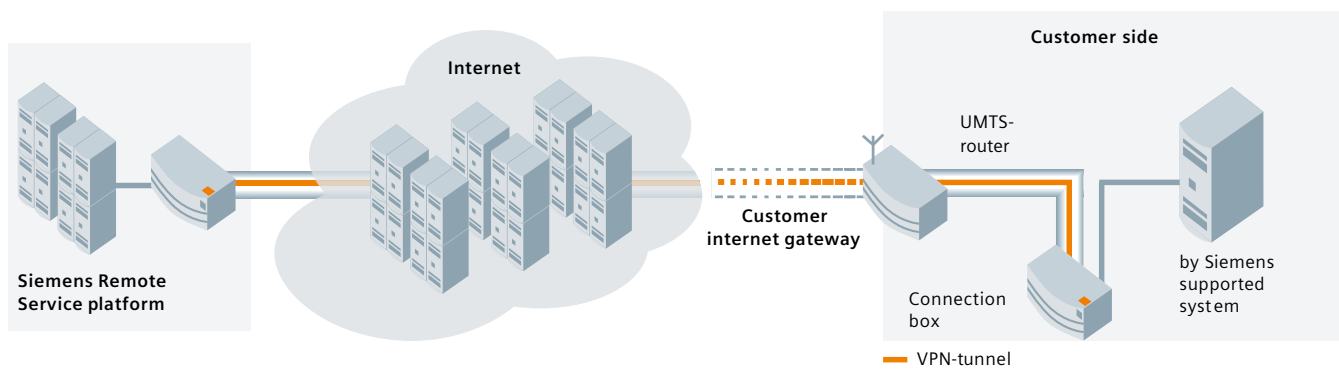
In this case, the Internet connection ends at the customer system. The VPN tunnel ends at the 2E connection box, which is placed in the customer network. The connection box is based on hardware that contains the two SW functions: the BT BACnet stack and SSL VPN. It is configured via a web interface. The 2E connection box is equipped with two network ports. It can therefore be used as a router between the VPN connection and the separate network. To be able to set up a connection to the SRS platform, the communication must be opened from the inside to the outside in the customer's firewall via TCP port 443.





### Connection box via mobile network

In this case, the customer does not have an Internet connection. The MRC box, a portable variant of the connection box, establishes the connection via a UMTS(3G) router. After initial startup, it can be easily adapted to the changing project circumstances. The settings needed to do this can be parameterized either at the device or from a remote location. The workflow for integration into the SRS platform is similar to the one for the SSL VPN connection.



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

Never too cold. Never too warm.  
Always safe. Always secure.

With our knowledge and technology,  
our products, our solutions and our services,  
we turn places into perfect places.

We create perfect places for their users'  
needs – for every stage of life.

#CreatingPerfectPlaces  
[siemens.com/perfect-places](https://www.siemens.com/perfect-places)

Article no. BT\_0122\_EN (Status 06/2017)

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.

