SIEMENS

Ingenuity for life

cRSP classic
IT Operational Security Practices

common Remote Service Platform classic

http://www.mindsphere.io

Siemens may adapt this Security White paper from time to time without further notice or consent.

Document objective

The Siemens' common Remote Service Platform classic (cRSP classic) is an IT platform that is used throughout the whole Siemens Group for implementing remote access to IP-based equipment.
The purpose of this IT Operational Security Practices paper is to describe the measures that Siemens Digital Industries Software takes to protect customer data, applications and IT systems when using remote services. In its current version, it is applied to all Siemens' industrial automation systems, solutions and services for which remote services are available over the entire life cycle.

Document abstract

This document is divided into two main parts:
General operating practices and technical security practices.

The first part, the general operating practices for remote services, encompasses fundamental aspects of data protection and information security within Siemens.

The topic of remote services for Industry Solutions is then introduced, along with a look at the application-specific use cases for remote connections. This part also includes strategic security measures in the areas of data management and personnel selection, which are organizationally implemented for remote services in Siemens' certified information security management system (ISMS). It provides employees and customers a general understanding of data security in remote connections.

The technical security practices describe technical measures and advice on remote access, including access types and logging, secure IT infrastructure, protecting data transmissions and protecting against attacks.
This includes technical components, processes and procedures, such as authentication and authorization. This information is especially important for IT specialists who are interested in the type of connection or encryption methods.

Finally, an overview of the various connectivity options, such as Siemens Offered Access (SOA) and Customer Offered Access (COA), is given in the appendix.

Contents

02 **Introduction**

05–06 **General operating practices**
Data security
Remote services
Data management
Personnel selection
Platform availability

07–11 **Certified technical security practices**
Customer-controlled access
Access models and logging
Authentication and authorization
Network structure
Virtual private network (VPN)
Security measures on the Internet/customer network

12–15 **Appendix**
Connectivity options

Abbreviations

AH	Authentication Header
BCM	Business Continuity Management
CA	Certification Authority
CERT	Cyber Emergency Readiness Team
COA	Customer Offered Access
cRSP	Common Remote Service Platform
CWP	Customer Web Portal
DMZ	Demilitarized Zone
DR	Disaster Recovery
ESP	Encrypted Secure Payload
IP	Internet Protocol
IPsec	Internet Protocol Security
ISAKMP	Internet Security Association and Key Management Protocol
ISMS	Information Security Management System
LAN	Local Area Network
LTE	Long Term Evolution
OTP	One-time Password
PFS	Perfect Forward Secrecy
PKI	Public Key Infrastructure
SOA	Siemens Offered Access
SSH	Secure Shell
SSL	Secure Socket Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunication System
VPN	Virtual Private Network
WAN	Wide Area Network

General operating practices

Data security as a basic requirement

Siemens values confidentiality and long-term partnerships, which is why data security is given the highest priority. Before implementing an enhanced service package with remote support, an in-depth analysis of the situation is conducted, considering national and international regulations and certifications, as well as technical infrastructures.

Service employees carefully evaluate customer needs on an individual basis with a focus on information security and data protection.

Emergency call and service centers are available 24/7. Trained specialists are always standing by to provide remote assistance

Remote Services for Digital Industries

Remote support for industrial products and services provide a high 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 proactive services, Siemens is able to take preventive action to avoid faults, instead of responding only after they have occurred. As a result the customer’s system down time is reduced.

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
- **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 cRSP advantage

Remote service provides additional support to optimally service industrial 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

All data is treated as highly confidential and access is granted 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, which are implemented, depend on customer data protection requirements, the type of data and the provisions of applicable regulations. Siemens can provide comprehensive consulting on data storage, backup, ownership rights and data destruction for individual solutions.

Personnel selection

Service technicians and experts are bound by the need for confidentiality in handling customer data and are trained to understand the serious consequences of failure to comply with the relevant conditions. Only employees who have been trained in data protection and IT security, and pass strict selection criteria, are allowed to work in Remote Service Centers. Furthermore, service technicians must participate in ongoing training and validation processes.

Platform availability

The availability of Siemens’ 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 cRSP platform remains unaffected in the event of a malfunction at a data center. The integration of additional plans for disaster recovery (DR) and business continuity management (BCM) ensures the highest possible availability of remote services.

Siemens CERT auditing / Certification

Siemens was one of the world’s first organizations to implement an internationally valid information security management system (ISMS) that is operated according to ISO/IEC 27001 for remote services.

The Siemens Cyber Emergency Readiness Team (CERT), an internal, independent and trustworthy partner, develops preventive security measures and assesses the information security of the IT infrastructure. The Siemens’ cRSP platform is audited on a regular basis to ensure valid protection and continuous improvement.

Technical security practices

Maintain constant control over the remote access to systems.

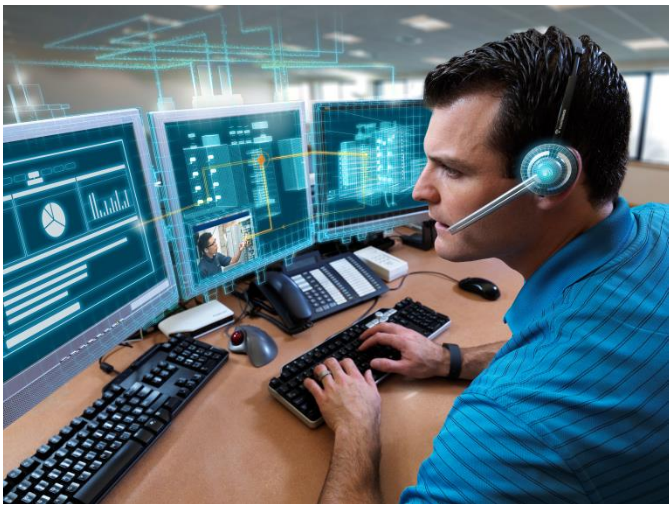
The customer determines how access takes place

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

Access models

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

- **Connection on request:**
  A customer's system can be accessed only upon individual request. For example, a service technician may request access for a limited period of time in order to clear a specific fault. This access is not continuous. This type of access is contractually agreed upon and is also defined in the customer's firewall settings.
- **Supervised access:**
  The customer follows the service technician's work on the system in real time using 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 using the cRSP 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.
- **Third party access:**
  The Customer Web Portal (CWP), with enhanced security requirements, enables customers and their business partners to access their systems outside of the Siemens network. In addition to just setting up a connection, customers also have the option of explicitly barring access to individual destinations and enabling them only when needed. Combined with the retrieval of log files on successful access attempts, this provides control over remote access to the system at all times.



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

Access logging

Each direct access to a system is recorded in the cRSP platform and provided with a time stamp and unique user ID of the service technician – for entry and exit. This information allows quick identification of the service technician who accessed data and when this took place.

Authentication and authorization of Siemens service personnel

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

Siemens therefore issues digital certificates (so-called digital IDs) for employees according to the provisions of the Public Key Infrastructure Disclosure Statement (PKI). Every time a Siemens service technician logs into the cRSP portal, his access rights are verified on the basis of PKI, a strong authentication method using a smart card. The defined customer access are then mirrored within the cRSP platform and converted to authorized IT system access levels.

These access levels are then matched to the Siemens service technician's verified identity.

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

Authentication and authorization customer personnel

To enable customers and their business partners to access systems from outside the Siemens network, the Customer Web Portal (CWP) is located 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.

When accessing the web portal, the user must enter their user name and password as well as their mobile PIN. The PIN number will be sent to the mobile phone number stored in the user account and must be entered within a period of two minutes. Otherwise, the authentication process starts over.

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 and retention may be extended on customer's request. Customer requests to include supplementary information in the audit trail can be adressed if 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, the cRSP 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's system via the cRSP platform.

Network structure

To protect a customer network as well as the Siemens intranet against reciprocal problems and attacks, the cRSP server is secured in a DMZ. Service technicians do not set up end-to-end connections to customer's 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 a customer's system and mirrors the incoming communication to the Siemens intranet.

This prevents a connection from being set up between the Siemens intranet and a customer 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

It is generally recommended to use a secure broadband connection over the Internet.

This offers the following advantages:

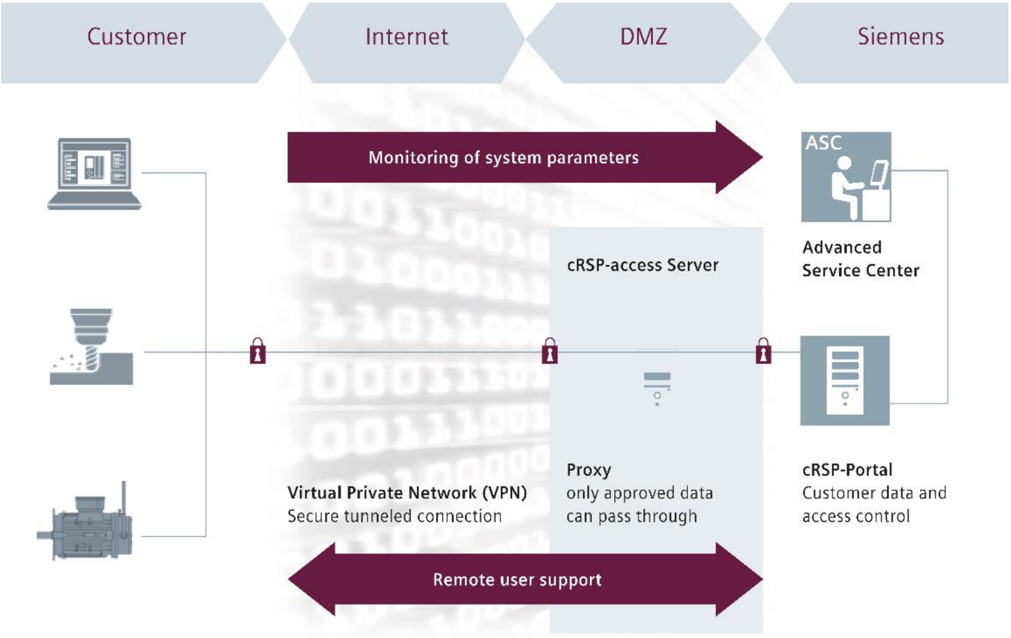
- A maximum level of security
- High data transfer rates
- High availability
- Access to all available remote services

An IPsec-secured VPN connection between the Siemens DMZ and the customer's network access is a highly secure technical solution (site-to-site VPN).

An SSL-based VPN connection between the system and the DMZ is also available.

If a suitable infrastructure is already in place, Siemens' technicians will be happy to coordinate the parameters needed for a connection with the customer, which must then be secured against unauthorized changes. If there is no VPN endpoint for a connection, Siemens will provide one with a prequalified router. The VPN endpoint at Siemens' end (in the DMZ) are Cisco routers.

In rare instances, the customer will not be able to set up an operational connection with routers from other manufacturers, due to compatibility problems.


Customer
Internet
DMZ
Siemens
Monitoring of system parameters
ASC
Advanced Service Center
cRSP-access Server
Proxy
only approved data can pass through
Virtual Private Network (VPN)
Secure tunneled connection
cRSP-Portal
Customer data and access control
Remote user support

Security measures for IPsec

Siemens uses the established standard Internet Protocol 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 securely exchange 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 the customer's 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) are used for key-exchange security and Perfect Forward Secrecy (PFS).

Security measures for SSL-VPN client

The SSL VPN client (using TLS-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 TLS-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 software copies can establish a connection to the cRSP 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 the customer network from the outside. The main security features depend on the selection and configuration of the chosen cRSP access router at the customer's site. In principle, a distinction is made between Customer Offered Access (COA) and Siemens Offered Access (SOA).

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.

Protocols

This section provides a list of the protocols and services used. If any other specific security measures or customized firewall functions are needed for special applications, network segments, etc., they are available depending on the choice of connectivity options.

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

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

When transmitting data during diagnosis, only the required technical data is sent automatically from the system to the cRSP 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.[1]
- Transparent proxy:
  The cRSP transparent proxy can be used with most cRSP applications with the option parameter "useTransparentProxy". 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

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

[1] Please contact remoteaccessservices.industry@siemens.com for more information.

Secured cRSP server

Siemens uses Linux servers exclusively for cRSP access servers. Linux is the top choice for a server operating system, as it is not only designed for stability, but also frequent updates make sure that the system remains secure.

According to the current state of the art, infections by worms, viruses, Trojan horses and other attacks therefore remain highly unlikely. In addition, the secured cRSP servers, as well as the encrypted databases on these servers, are always state of the art.

Public IP addresses of the productive cRSP DMZ:

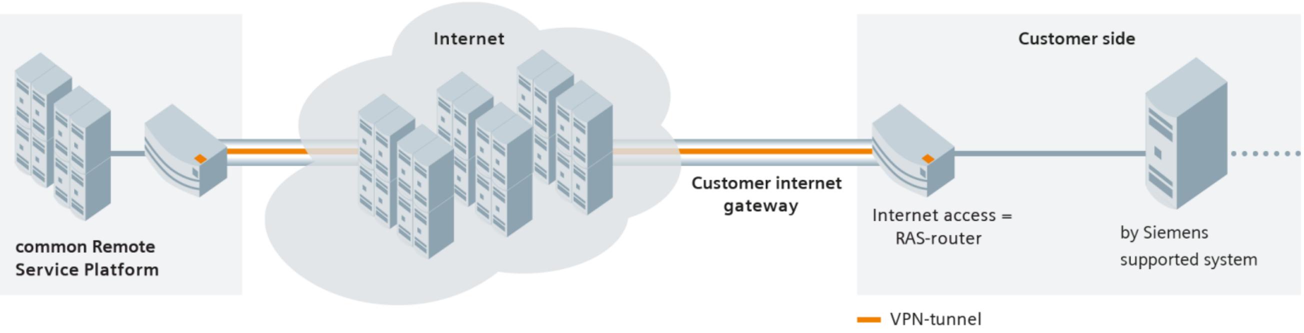
- DMZ Fuerth (Germany): 194.138.37.194
- DMZ Malvern (USA): 12.46.135.194
- DMZ Singapore: 194.138.240.119

Connectivity options

In the following an overview on how to implement a connection to customer's systems with the cRSP is given.

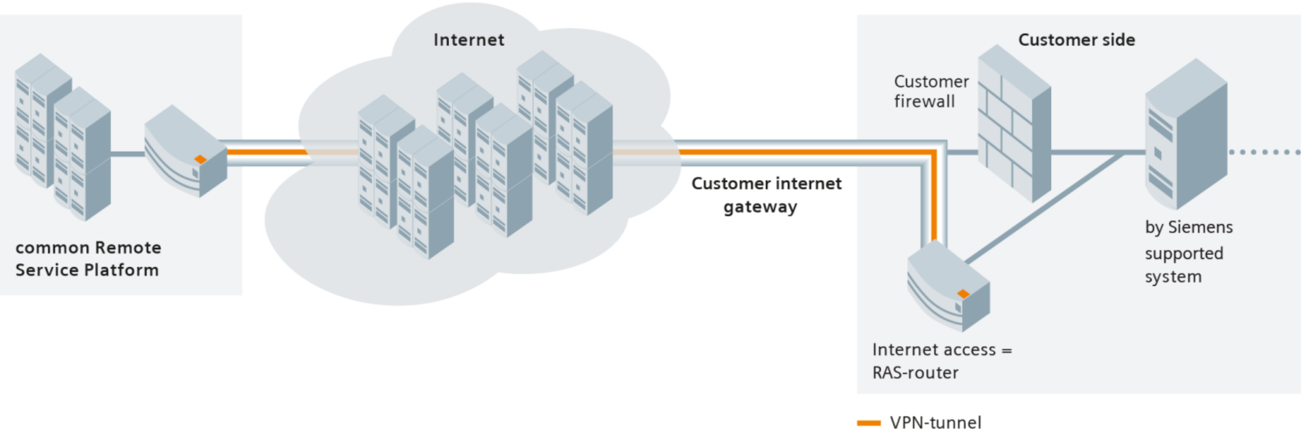
Siemens Offered Access (SOA) is directly connected

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


Internet
Customer side
Customer internet gateway
Internet access = RAS-router
by Siemens supported system
common Remote Service Platform
VPN-tunnel

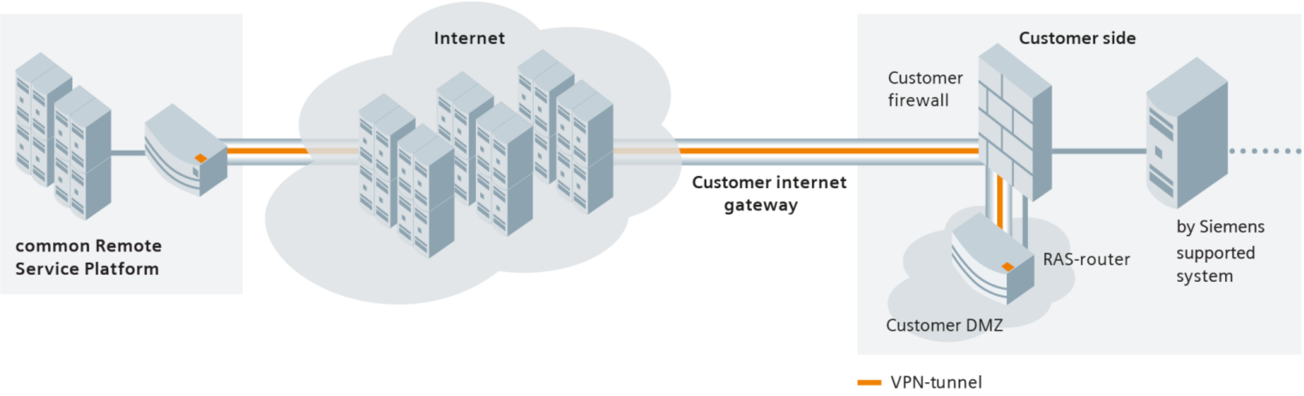
Siemens Offered Access (SOA) bypasses the customer's entire firewall

In this case, the RAS 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's network and also does not have a DMZ.


Internet
Customer side
Customer firewall
Customer internet gateway
by Siemens supported system
common Remote Service Platform
Internet access = RAS-router
VPN-tunnel

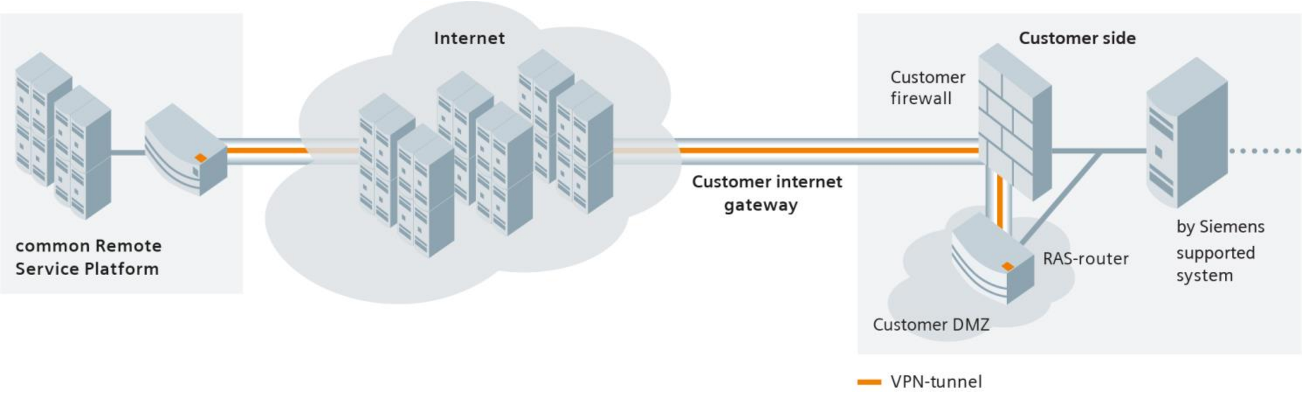
Siemens Offered Access (SOA) router is located in the customer's DMZ

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


Internet
Customer side
Customer firewall
common Remote Service Platform
Customer internet gateway
RAS-router
by Siemens supported system
Customer DMZ
VPN-tunnel

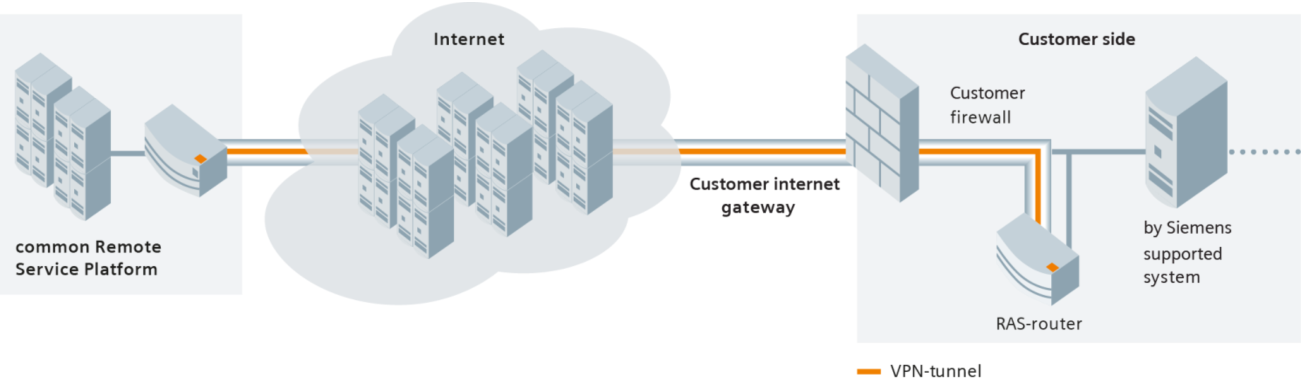
Siemens Offered Access (SOA) router is in the DMZ of the customer's firewall, but the LAN interface is directly connected

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), ISAKMP (UDP port 500/4500), ESP (IP protocol number 50) and AH (IP protocol number 51) are needed for forwarding to the RAS access router (WAN address).


Internet
Customer side
Customer firewall
common Remote Service Platform
Customer internet gateway
RAS-router
by Siemens supported system
Customer DMZ
VPN-tunnel

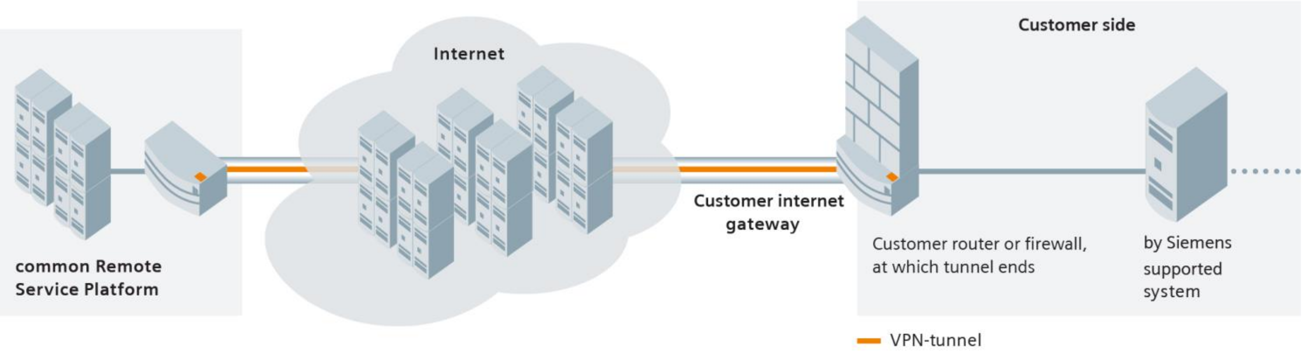
Siemens Offered Access (SOA) router is placed within the customer's network

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's network. SSH (TCP port 22), ISAKMP (UDP port 500/4500), ESP (IP protocol number 50) and AH (IP protocol number 51) are needed for forwarding to the RAS access router (WAN address).


Internet
Customer side
Customer firewall
Customer internet gateway
by Siemens supported system
common Remote Service Platform
RAS-router
VPN-tunnel

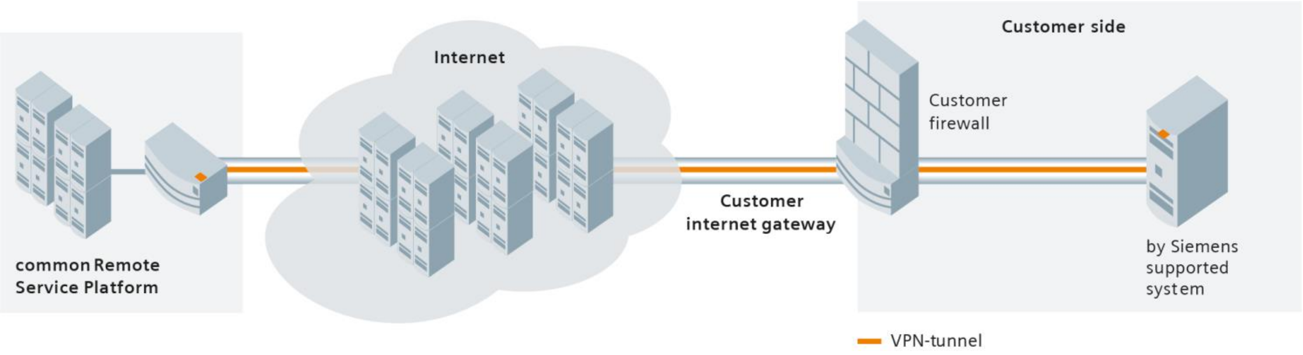
Customer Offered Access (COA)

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.


Internet
Customer side
Customer internet gateway
common Remote Service Platform
Customer router or firewall, at which tunnel ends
by Siemens supported system
VPN-tunnel

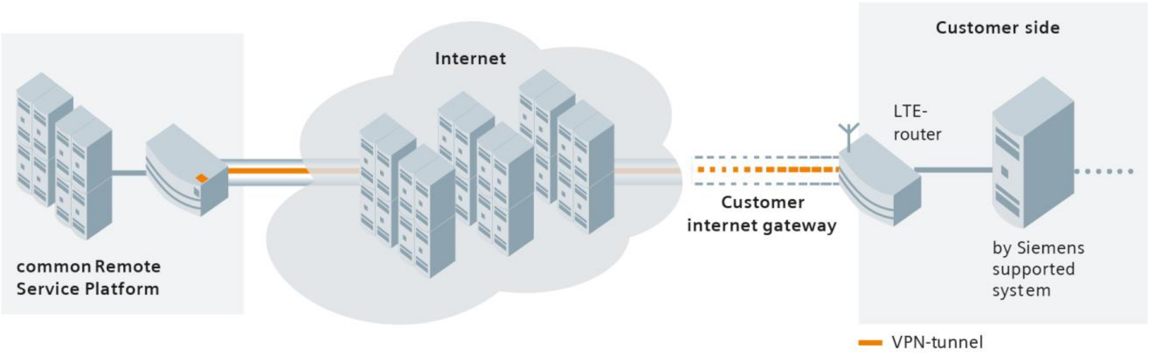
SSL VPN client

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


Internet
Customer side
Customer firewall
Customer internet gateway
common Remote Service Platform
by Siemens supported system
VPN-tunnel

Connection via mobile network

In this case, the customer does not have an Internet connection. A connection is established via UMTS (3G) or LTE (4G) router. After initial startup, it can be easily adapted to the changing project circumstances. The workflow for integration into the cRSP platform is similar to the SOA connection option.



Published by
Siemens AG 2019

MindSphere Product Management
E-mail: remoteaccessservices.industry@siemens.com

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.

Unrestricted