SIEMENS
Ingenuity for life

Cybersecurity Model

Remote Diagnostic Service for Oil & Gas and Industrial Rotating Equipment

siemens.com/energy

Table of contents

1. Purpose of this guide

Asset availability, utilization and ultimately, operational profitability are the three core benefits of Siemens Remote Diagnostic Service (RDS) used by many of our customers worldwide who own and operate Siemens rotating equipment, such as industrial gas and steam turbines, generators and compressors.

As connected assets, Siemens rotating equipment must be protected against cyber threats at each asset's location, where machine data is collected. The data must be then protected in transit to Siemens Remote Diagnostic Centers and upon arrival and while stored at Siemens.

For these reasons, Siemens has developed and implemented an end-to-end cybersecurity model to keep out hackers, malware and other threats. But, to be effective, this cybersecurity model requires the close collaboration of our RDS customers, such as yourself – especially both IT and operational technology (OT) staffs – to ensure that its safeguards are properly deployed on your end.

To help, we developed this Operations Guide. It provides much greater detail on the Siemens RDS security model, strategy and specific defenses to assist your OT and IT professionals in understanding our approach and supporting it in their respective domains.

By working together, Siemens RDS helps you exploit the availability and utilization of your rotating equipment without compromising your overall cyber-risk posture.

2. Overview of Siemens Remote Data Service (RDS)

Siemens RDS provides operators of Siemens turbines, generators and compressors with 24/7 performance monitoring, as well as early-warning support to flag KPI variances and anomalous conditions that could indicate trouble ahead. It delivers actionable intelligence for decision support to help them understand how to manage any performance issues until their next planned maintenance outage, increase availability and reduce the cost of unplanned disruptions. Our extensive experience has shown a major upside to remote performance monitoring and diagnostics by averting trips and resulting forced outages via early detection of potential faults and preventive actions.

To support troubleshooting and remediation, our expert engineers, who can offer real-time, over-the-shoulder assistance for faster resolutions and escalate issues as needed, bring additional expertise to bear on problems. Usually it is much faster and more efficient to determine the causes of equipment issues via remote diagnosis by analyzing historical data of your equipment and, where possible, address the issue remotely. Even in cases where remote repair is not possible, the information obtained via remote diagnosis can support the Siemens service engineer in onsite repair.

Now covering a fleet of installations worldwide, RDS is employed by many Siemens customers to enact condition-based monitoring of their rotating equipment. In this approach, maintenance can be performed as needed, rather than at fixed intervals – saving labor and spare part costs. Most importantly, production can continue for longer periods between maintenance intervals as a result.

Ultimately, RDS helps operators of Siemens rotating equipment to increase the reliability of these assets across the entire train and, importantly, the profitability of the production they drive.

3. Siemens RDS security model: How it works

Siemens rotating equipment is most often deployed in the world's critical infrastructure, such as oil and gas and power generation. These industries offer big targets to hackers, who are increasingly professional and sophisticated in their methods and relentless in the frequency of their attacks.

At the same time, these industries can be subject to internal sabotage and compromised OT infrastructure. Either way, production can potentially be disrupted or, if not, OT networks can be used by intruders as routes into enterprise IT networks to exfiltrate intellectual property, private data and other digital assets of value.

Siemens recognizes these risks and has developed a rigorous, end-to-end security model that safeguards the connectivity needed by RDS to link your rotating equipment to our Remote Diagnostic Centers. Our protections are in accord with the most current global cybersecurity standards, including ISO 27001, IEC 62443 and NERC CIP.

Our goal is to wrap our RDS for Siemens rotating equipment in the most advanced, multi-layered protections available, using a defense-in-depth model that's considered the best practice everywhere in the world.

3.1. Secure data exchange

The Siemens RDS end-to-end security model uses a secure data exchange between the rotating equipment of our RDS customers and our Remote Diagnostic Centers. This joint approach enables us to work together in neutralizing potential cybersecurity threats without compromising the overall security of the environment.

To explain this model in a bit more detail, it consists of three key components:

- **Data collection:** We developed a secure data collector solution that resides on the side of your Siemens rotating equipment to collect its sensor and events data. It's located in a demilitarized zone (DMZ) outside of your OT and IT networks, separating them from external networks in a strictly managed and monitored way. The data collector solution serves as a staging point for your data's secure transmission. The system also serves as central access point for remote RDS support. It complies with the latest global security standards, as mentioned previously.
- **Data transit:** Data from your data collector solution is encrypted and sent via a secure Virtual Private Network (VPN) connection, using our common Siemens Remote Service Platform (cRSP), over the Internet to the servers in our Siemens Remote Diagnostic Centers. These servers are part of the cRSP as well.
- **Data monitoring:** On arrival at the monitoring facility, your data is decrypted, anonymized and stored in parallel redundant databases that reside behind next-generation firewalls for additional security, backup and disaster recovery. After this security processing, the data is then analyzed using sophisticated diagnostic agents, which are a custom-coded industrial software applications.

3.2. Daily monitoring

After your Siemens rotating equipment is connected, its sensor and events data are automatically and continuously sent to Siemens servers and analysed daily. Daily monitoring by the Siemens diagnostic engineers can detect critical changes in your equipment's health status, which can go undetected by its control system. By applying rules- and physics-based, data-driven analytic models, potential problems can be identified at an early stage.

If anomalies are detected, your assigned RDS engineer will alert you with a notification document, providing short-term recommendations for corrective action. Additionally, we provide periodical Monitoring Reports that show you long-term operating trends of your connected equipment. Moreover, Siemens provides you with access to myHealth, a secure portal that gives you a dashboard overview of your important operational KPIs, sensor data from key instrumentation, notifications and reports.

3.3. Operational Service Desk

Troubleshooting in response to a critical event also plays an important role in ensuring availability of your rotating equipment. The Siemens Operational Service Desk (OSD) offers engineering support and advanced remote troubleshooting in emergency cases. Our technicians can help resolve your equipment issues much faster by analyzing historical data of your equipment and then tailoring a recommended remediation.

If you need remote support, your assigned Siemens RDS engineer or another qualified Siemens technical expert can connect to your rotating equipment's control system to review equipment faults. For this real-time support, the engineer will establish a remote connection to the equipment after access has been approved and specifically activated by you. You can track the course of the remote support and, if necessary, terminate the engineer's access at any time.

3.4. Customer Remote Control via the cRSP Customer Web Portal

As an optional add-on to our remote services, we offer Customer Remote Control, as well. This is enabled through the cRSP customer web portal (CWP). It provides you with the following services:

- Remote access for your personnel and any service partners
- Online supervision
- Access to the logging information

These services enable any of your personnel, who are not onsite, to conduct online monitoring of certain critical service activities. It may also be suitable for any of your maintenance personnel who might be working from home and want to perform certain remote service activities via the Internet. You can also supervise a remote session from a Siemens technician in real time over the CWP – from anywhere you are. Since this functionality is embedded in the cRSP security infrastructure, it provides a high level of security. Additionally, you can track any access to your equipment through the access log, as further described in section 4.

3.5. Incorporating specific customer requirements for security and safety

While our Siemens RDS cybersecurity model abides by standards as IEC 62443 and NERC CIP which apply to critical infrastructure, you may have additional requirements for the security and safety of your equipment. These might spring from your business situation, technical infrastructure, specific security issues, or applicable regulations, raising additional security needs that are beyond the standard scope of our Siemens RDS offering. In all cases, Siemens will work with you to understand and accommodate your needs in ways that respect the integrity and security of your operation, while also enabling us to provide you with our remote monitoring service for your rotating equipment. The following list of customer feature requirements is typically provided by our RDS offering:

- **Comprehensive logging**
  You and/or specific regulations that govern your business may require the comprehensive and comprehensible logging of session data.

- **Audit trail**
  Energy and Industry-specific requirements and/or applicable regulations may require that remote service sessions are recorded, so that sessions are traceable in the case of future audits.

- **Online supervision**
  You may want to observe a remote session in real time. In particular, when critical parts of the equipment are being serviced, you may want to supervise actions and be able to stop the remote session at any time.

- **Selective access: comprehensive administration of user rights and data access**
  You may want to have a detailed level of gradation of user rights and access to systems and data. For highly critical components, personalized access rights may be required.

- **Protection of data privacy**
  Before connecting remotely to your equipment, there must be clarification on how data privacy protection issues are to be addressed. In addition, certain industry standards and/or applicable regulations require specific measures to ensure data privacy.

- **Using a standard solution**
  A growing number of original equipment manufacturers (OEMs) offer remote services for their products in various configurations. This can result in an increasing number and variety of remote connections between you and them, adding to your staff's administrative burden. The added administrative complexity can also increase the possibility of security gaps. At Siemens, we strive to avoid this situation by building on a certified, standards-compliant solution for all of our Siemens products, including your rotating equipment.

4. Organizational security model

Because our RDS security model is a collaborative approach between our customers and Siemens, we include you and your designated staff members in every step of the model's design and implementation as well as all operation processes, which are designed to offer a high level of traceability.

What's more, we employ ISO 27001-certified processes and service operation protocols to ensure secure cRSP operations. You therefore benefit not only from the Siemens experience on how to operate OT and IT systems securely on a global basis, but also with the backup support of a dedicated industrial cybersecurity team and supporting tools for OT and IT environments.

Based on the requirements set forth in your RDS agreement, the connections to your plant sites will be planned in cooperation with your OT and IT professional staffs, who will then verify and sign off on them. Implementation starts after you have agreed to the agreement's suggested implementation plan, which also will be documented.

Only Siemens technical engineers trained in and committed to data privacy and security issues are authorized to perform Siemens remote services.

Siemens requires cRSP users be authorized for access and that they are RDS-trained. The certification process is intended to provide them with sufficient knowledge of applicable policies and procedures for the access and use of the information. The user certification is valid for one year. After that period, users must recertify, to be allowed to connect with the cRSP. Following are measures that enhance the security of cRSP connectivity:

- **Establishing the connection**
  To authorize remote access for a Siemens service engineer, additional security mechanisms can be put into place, such as authentication servers using one-time passwords.

- **Access control permit for remote service**
  For every service activity, the service contract can ensure that the customer grants access to his plant to the cRSP customer web portal and retains control of who is permitted access to the equipment. Access is only granted to identify or correct errors. After a set period of time, during which no action has occurred, the Siemens remote session on your equipment automatically ends.

- **Remote access logging**
  Siemens records access to your equipment and applies a time stamp. In addition, the Siemens service engineer who accesses the equipment is assigned a unique user identification, which is also recorded in this log. As a result, we can tell you within a specific time period which Siemens service engineer had access to data, when and what communication activities were performed on each piece of equipment. We typically retain these log reports for two years, but can retain them for longer, if you require it.

- **Maintenance and further development**
  Maintenance and development tasks are based on dedicated processes. Suggested changes are discussed and assigned by a Change Control Board (CCB)/Change Advisory Board (CAB). After the changes are made, they are tested for failures or incompatibilities in a release environment to protect production environments. After the approval at the end of the tests, the changes are implemented in the production environment. This process is mandatory for all changes.

5. Technical security model in greater detail

5.1. Secure data collection at your site

As mentioned, all our provided RDS services are based on secure data exchange, enabling effective joint working of our two companies to neutralize potential cybersecurity threats without compromising the overall security of our joint operating environment.

Also, as referenced earlier, RDS data is collected from your site via a secure data collector solution and sent over a VPN connection, to the cRSP servers. The data collector solution is built from two industrial-grade firewall routers — one guarding ingress from the wide area network (WAN) and the other for protecting the local area network (LAN) — as well as an industrial PC. In effect, this solution provides the needed DMZ in your network topology.

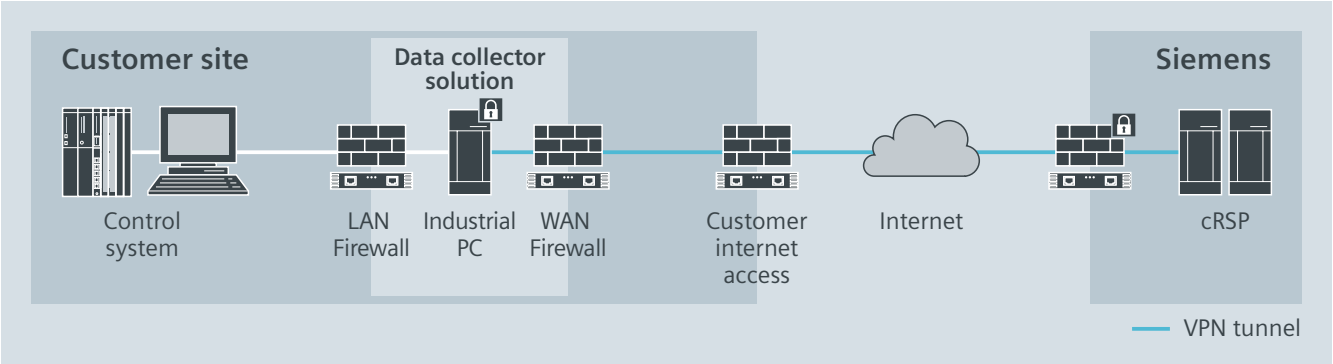

Figure 1. Data collection and transfer

The cRSP, described in more detail in the next section, is a secure central access portal inside the Siemens intranet. It requires a strong authentication method, such as PKI (Public Key Infrastructure), which can only be accessed by using a smart card.

There are different ways to connect the WAN firewall to the cRSP via a secure VPN connection, which are more fully described in the chapter standard VPN connection types. After you have selected your remote access solution, Siemens, together with you, sets up the security zone architecture and builds up the DMZ for remote access, with everything documented.

The data collector solution's LAN firewall is implemented to control IP traffic from the industrial PC to your rotating equipment's control system. As such, the industrial PC serves as a gateway between the control system and the cRSP. This way, no direct connection to your control system is possible by using the cRSP. To log into the industrial PC, a second authentication is required.

In case of an equipment failure that prompts you to request remote support from a Siemens service engineer, this person can log into your equipment's control system. However, their remote access requires your expressed approval – by changing a specific firewall rule implemented in the LAN firewall.

There are two ways for you to change the firewall rule from the control system side: (1) through an access granting software which has been installed on the control system; or (2) via a digital input such as a hardware switch that can be integrated in the LAN firewall.

Through the remote support connection you can monitor the changes in a shared session. Additionally, in case real-time support is needed instead of remote support, the service engineer can connect to the data collector of your rotating equipment. This is done via a live remote data viewer, eliminating the need for direct remote connection to the control system.

The standard firewall rule allows streaming data with OPC UA, an industrial standard communications protocol, from your equipment's control system. We stream machine data with a resolution of 1 second (maximum resolution is 100 ms) into a database that resides in the data collector solution.

OPC-UA is firewall-friendly, encrypted and needs only one open port in the LAN firewall. This industrial protocol is supported by most control systems, but if your control system supports only OPC classic, we can provide an OPC-UA gateway which converts the OPC classic protocol into OPC UA. To provide fast support in case of a critical event, we can configure the data collector solution to send an automatic notification to us at Siemens.

Additionally, we offer the possibility of using a data diode to connect the control system via OPC UA. With the implementation of the Siemens data diode and the OPC UA protocol to connect the control system, is write-protected. To support our customers remotely, we will implement an Ethernet switch at customer site to change the network.

The data collector solution is based on the most current international cybersecurity standards, including ISO 27001, IEC 62443 and NERC CIP, which cover the connectivity functions described above. As part of the solution, Siemens provides regular and mandatory firmware updates of the firewalls as well as security updates and patches of the operating system, the application software at the data collector computer and the latest virus pattern updates. All implemented hardware and software is monitored, to get knowledge about security issue, so that we can react directly to solve the issue and, if needed, provide in a short time security fixes. Additionally, end point hardening and whitelisting is used.

5.2. Security infrastructure of the cRSP

The cRSP is a secure central access portal within Siemens, using Linux servers, that provides a set of security infrastructure, as Figure 2 illustrates.

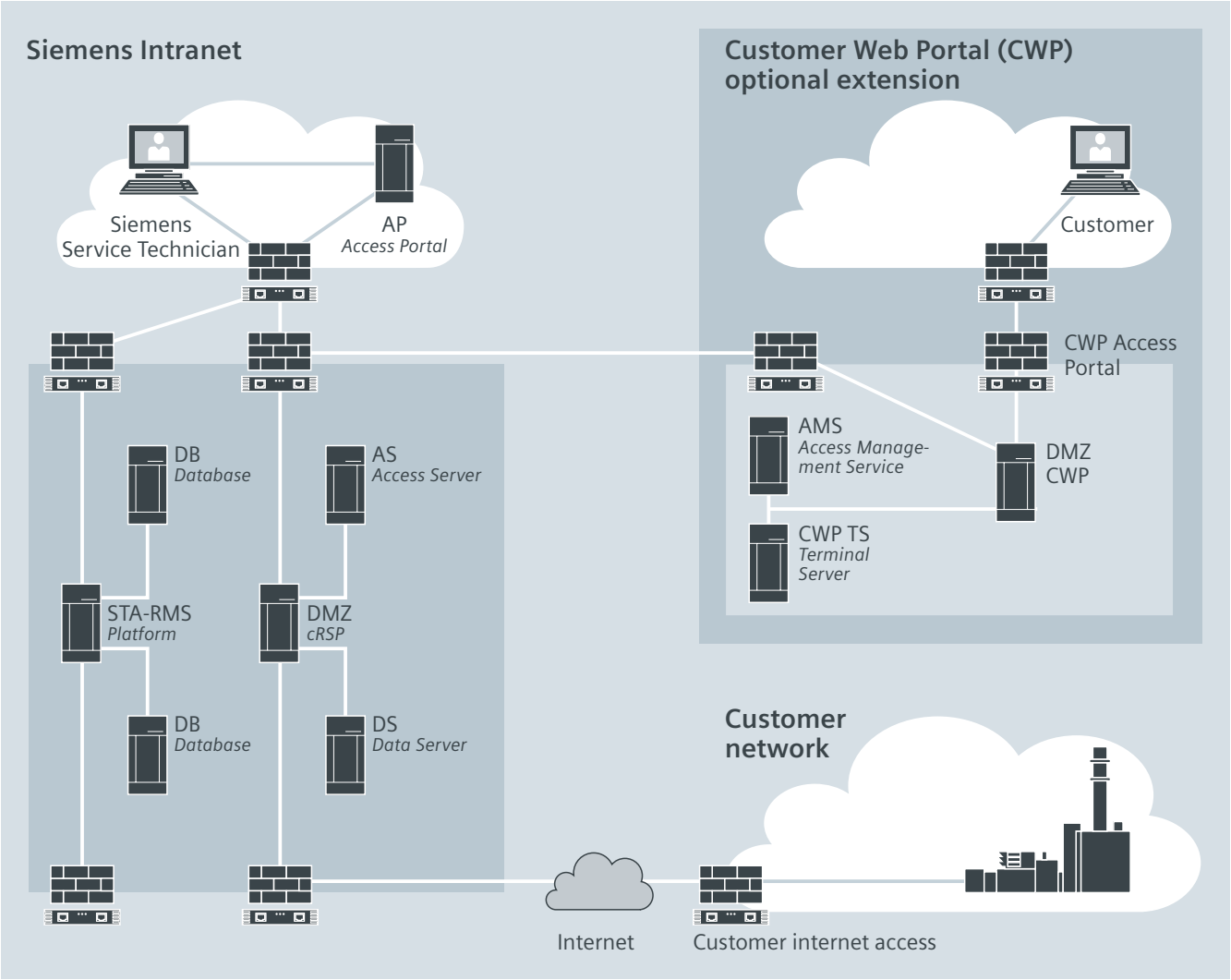

Figure 2. cRSP infrastructure

- **Authentication and authorization of Siemens service personnel**
  The cRSP central access portal is located within the Siemens intranet, in a separate network segment and requires PKI authentication using a smart card for access. We employ a multilevel service domain concept to define which users are permitted to access which equipment. This means that Siemens service engineers can only access that customer equipment for which they have been authorized. Further, only the Siemens cRSP access functions for which the engineer is explicitly authorized are released for viewing by that engineer. Other equipment in your network that is not maintained by Siemens is not configured for access by Siemens engineers.

- **Demilitarized Zone – DMZ**
  To protect your networks and the Siemens intranet from cyberattacks, the cRSP resides in a secure DMZ. Connections by the Siemens service engineer to your equipment and vice versa, are not made directly, but instead terminate in the cRSP using a reverse proxy function. This means that a connection established from the Siemens intranet is terminated in the access server.

  This server then establishes the connection to your equipment and mirrors the communication coming back to the Siemens intranet. This is configured to prevent any possibility of communication between the Siemens intranet and your network over any protocols that have not been specifically authorized. Mirroring occurs only for predefined protocols and only after successful authorization at the cRSP.

  Also, all data streams coming from and to your network or the Siemens intranet are led through firewalls featuring the latest detection methods. This architecture is designed to prevent:
  – Unauthorized access
  – Fraudulent use of secure passwords, access data and other privileged information
  – Transmission of viruses or similar harmful programs from one network to the other

  In addition, we do not store any critical data in the DMZ, especially customer access data. Within the scope of our proactive RDS, data is periodically sent by the monitored equipment. This communication is also established only after successful authorization of the equipment that is requesting the connection. Data sent through the VPN tunnels to the DMZ is then securely transferred onto the diagnostic platform.

5.3 Securing the transmission route over a VPN

We use secure encryption to protect your data from unauthorized access during transmission using Internet Protocol Security (IPsec) over a VPN between the Siemens DMZ and your network portal. This can offer the following advantages: a high level of security; optimum data transfer quality and availability; and access to all Siemens-provided services. Following offers more detail:

- **VPN with IPsec via the Internet**
  IPsec is designed to protect data against tampering and being read by others. Siemens uses this established standard with pre-shared secrets for encrypted and authenticated data transmission. Pre-shared secrets comprise at least twelve randomly selected characters. The Internet Security Association and Key Management Protocol (ISAKMP) are used to exchange encryption key information.

  The use of an Authentication Header (AH) is for data integrity by using SHA256-SHA512 hash method. Encrypted Secure Payload (ESP) provides for the confidentiality of data by AES algorithms. The Diffie-Hellmann key, with a 1024 up to 4096-bit key length, can be used as symmetrical session keys.

  Siemens can assist and provide you with the prerequisites (for instance, VPN router) to use the cRSP. The VPN endpoint on the Siemens side is a Cisco router that is configured according to your specific infrastructure and security requirements.

- **VPN with SSL via the Internet**
  In addition to the VPN via IPsec transmission mode, the cRSP offers connections using Secure Socket Layer (SSL) connections to the Siemens DMZ. For this, a Siemens-SSL client must be installed in the data collector solution.

  The client encrypts the data with certificates and sends them to the Siemens DMZ. This SSL tunnel, which uses the Transport Layer Security (TLS) protocol, provides communication privacy over the Internet to prevent man-in-the-middle eavesdropping, tampering, or message forgery between the client and the server.

- **Enhanced control capabilities through debugging (optional)**
  In case you want to receive service router SNMP or syslog messages on your router, or in case you want to see the current service router configuration, please contact your local Siemens representative.

5.4. Security measures within the customer network

- **Access to the customer network**
  In light of the security risks involved, external access to your network requires specific measures. The key security features depend on the specific concept and configuration of the customer access gateway method chosen:

  ### SSL VPN
  Our standard access gateway solution is the SSL VPN connection. For this, we provide a SSL VPN software client. This solution supports high-performance remote service solutions with low communication costs and enables value-added remote services to be added in the future. Also, the implementation process is uncomplicated.

  ### Service VPN router/Siemens-supplied access (SOA)
  In addition, we have a specified VPN-router solution with broadband Internet access, such as DSL. This solution supports also high-performance remote service solutions with lower communication costs and enables value-added remote services to be added in the future. Your specific demands for additional security measures for certain applications, network segments and requested onsite firewall features can be provided based on this access solution.

  ### Customer-supplied access (COA)
  If you already have an existing remote access solution in place, this system can, in most cases, be configured to work securely with the cRSP infrastructure. To clarify the required configuration and measures, please contact your local Siemens service representative.

- **System access**
  Once remote access to your equipment is released (either manually by the user/administrator or automatically, based on system configuration), Siemens recommends that the service engineer is authenticated at the equipment before being able to work on the equipment.

- **Protocols**
  Depending on the software capabilities in your equipment, the following can be used to service it:
  - Http – or preferably https – protocol
  - Telnet, VNC, MS Terminal Server, or SNMP
  - Other protocols (for specifics please contact your local Siemens representative)

- **Data transmission from your equipment to the STA-RMS platform**
  For our remote services, only mandatory technical data is automatically sent from your equipment to the cRSP (based on your equipment configuration). Depending on the capabilities of the software, the following services are used:
  - FTP/SFTP (file transfer protocol; secure file transfer protocol)
  - SCP (secure copy protocol)
  - cRSP Service Agent

- **Data transmission from cRSP to the data collector at customer site**
  The data collector computer will be manual or automatic updated with Anti-Virus Pattern, Microsoft Patches, Hotfixes and application updates on a regular base.

5.5. Features of Siemens equipment to protect against malicious attacks

cRSP protection
We use advanced virus protection software to protect the cRSP from infection by worms, viruses, Trojan horses, or other malware.

Vulnerability assessments related to your equipment

No direct threat from the cRSP server
The reverse proxy function and the firewalls are intended to protect against a virus infection on your equipment. Additionally, with the data collector solution, direct connections from the cRSP to your equipment and networks are not possible. Because the data collector solution is built as a DMZ at your site, only you can change the rules in the LAN firewall to allow a direct connection to your equipment's control system.

Threats from Internet connections
Since the control system is not directly connected to the Internet, but over the data collector solution, threats stemming from Internet connection are unlikely. However, as with any connection via the Internet, you must be cautious. Siemens security infrastructure contains anti-virus protection solutions, but if you use your Internet connection for other purposes, we recommend taking appropriate precautions to protect your equipment and networks.

No threat from e-mail traffic
The data collector solution sends e-mails to the cRSP and in this direction only. E-mails sent from the data collector to the cRSP are forwarded to the appropriate Siemens mail server and then sent to the recipient. The Siemens mail server scans e-mails for viruses and reacts in accordance with the Siemens established guidelines to protect the Siemens intranet. No e-mails are sent to the customer equipment, infection of the customer equipment is unlikely.

No threat from infection of serviced equipment via contact with infected equipment on your side
Infection of the cRSP through contact with infected equipment on your side is unlikely as there is no direct IP routing between their respective domains. Further, all data streams coming from and to your domain or the Siemens intranet are routed through firewalls with always updated anti-virus detection.

5.6. Security infrastructure of the cRSP Customer Web Portal

As mentioned previously in Section 3.4., the cRSP Customer Web Portal (CWP) provides optional, added functionality with these services:

- Remote access for your personnel and any service partners
- Online supervision
- Access to the logging information

The CWP is located in the cRSP DMZ and is accessible through the Internet. Users and their respective access rights are stored on the cRSP servers, in a separate network segment from Siemens intranet users. The CWP will check the state (e.g. up to date virus scanner, patch level) of all connected PCs. All CWP connections are protected with advanced encryption to protect your data from unauthorized access during transmission.

With no direct IP routing between the serviced system and the system connected to the CWP (refer to reverse proxy function), it is unlikely that a threat from infection of a serviced system through contact with an infected system happens.

The authentication of Siemens service partners and customer personnel for the CWP is realized with user ID, password and mobile PIN. When you need access to the CWP, you enter your username and your password followed by a mobile PIN that has just been sent to the mobile phone number, stored in your user profile. The PIN has to be entered within three minutes, or the authentication process has to start from the beginning. In case customer personnel are not on site, but who want to monitor certain critical service activities online, the authorization for the customer personnel can be configured in a way that certain remote service activities can be executed only if approved/confirmed by this individual.

6. Installation and configuration of the data collector solution

Once you have ordered the Siemens RDS, certain steps for installing and configuring the data collector solution will be followed. First, implementation will start with the clarification on how the connection to the equipment's control system can be established. There are two options:

- **Control system delivered by another vendor:**
  If the control system is delivered from any other vendor, we will clarify how the connection between the data collector solution and the control system can be established, as well as if an OPC UA Server is supported by the control system and available. In case no OPC UA Server is available, it has to be implemented. If an OPC classic server is available with support of OPC DA (Data Access) and OPC A&E (Alarm & Events), we can provide an OPC UA Gateway which translates the OPC classic protocol to OPC UA. To clarify which data is available from the control system, a list of all tags must be given to Siemens. Siemens will check if all needed tags can be collected to provide the needed services.
- **Control system delivered by Siemens:**
  If a Siemens control system is in place, we can recommend how a connection can best be implemented to the control system (such as using SPPA-T3000, PCS7 or WinCC).

The next step is to clarify which type of VPN connection between the data collector solution and the cRSP is to be established for implementation. You should make this decision with your IT staff, who are responsible for security, selecting one of our standard VPN connections. If you need help, please contact your Siemens contact.

The installation and pre-configuration is done on site, configuration and testing of the data collector solution is installed remotely. So, after the clarification of the remote connection, the data collector hardware will be installed at customer site in the cabinet if not already delivered. If there is no space in the cabinet, the solution should be placed near the control system. A Siemens employee will also prepare the hardware to be connected. The final router configuration (VPN implementation) is done by Siemens cRSP experts afterwards, to enable the remote connection. To ensure proper functionality of all needed applications, the remote connection will then be tested.

In the next step, the OPC UA connection is configured by our data integrity experts between the data collector solution and your control system, to ensure all needed tags for diagnostics of the equipment is collected. These steps of the implementation process are coordinated by your single Siemens contact.

At the end all implementation and configuration will be documented and stored in an encrypted folder in Siemens. Only administrative personal which supports our customers will have access to the folder. If needed all configuration files and documents can be also provided to the customer.

7. Standard VPN connection types

We offer different standard solutions to connect the data collector solution to the cRSP. All solutions are based on cRSP, which provides a VPN tunnel based on SSL or IPsec between your site and Siemens to secure the connection.

7.1. VPN situation 1: SSL – VPN via a software-based solution

The connection is established through SSL VPN software, which is installed on the industrial PC. In this case, the WAN firewall will only allow outbound connections to the cRSP via SSL. To use the VPN situation 1, we need an open port (TCP 443 – https) to connect from the WAN firewall to the Internet. The SSL VPN software can also be used over an Internet proxy and security updates are carried out automatically.

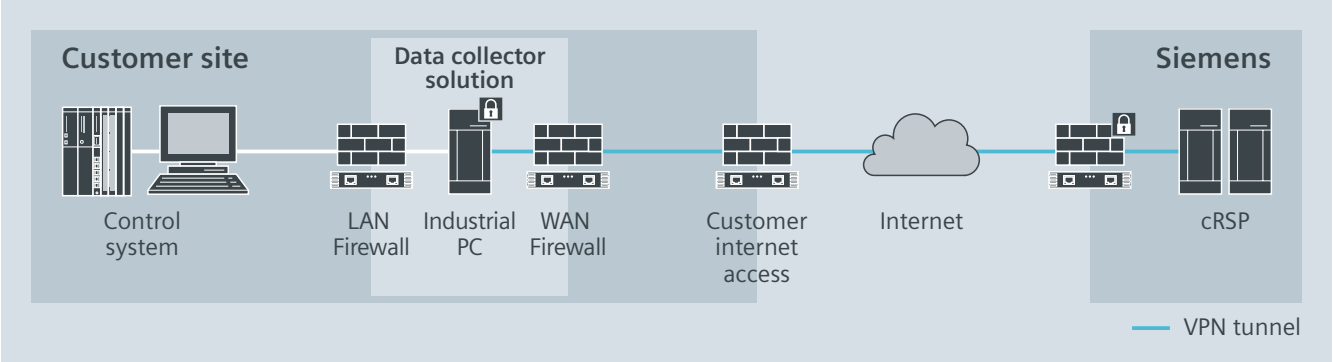

Figure 3. VPN situation 1

7.2. VPN situation 2: Siemens-owned access (SOA)

With this SOA connection, the WAN firewall terminates the VPN tunnel between your site and the cRSP. IP traffic is controlled in accordance with integrated firewall rules. Only the cRSP can connect to the WAN firewall and all other IP traffic is blocked. For all SOA VPN solutions, we need an Internet connection to build the VPN between the data collector solution and the cRSP.

- **SOA situation 2a – with direct DSL connection**
  To use this solution, you must provide direct Internet access, such as via DSL modem or router. If a router is used, please perform the Port Forwarding from this router to the WAN firewall at the data collector described in *Table 1*.

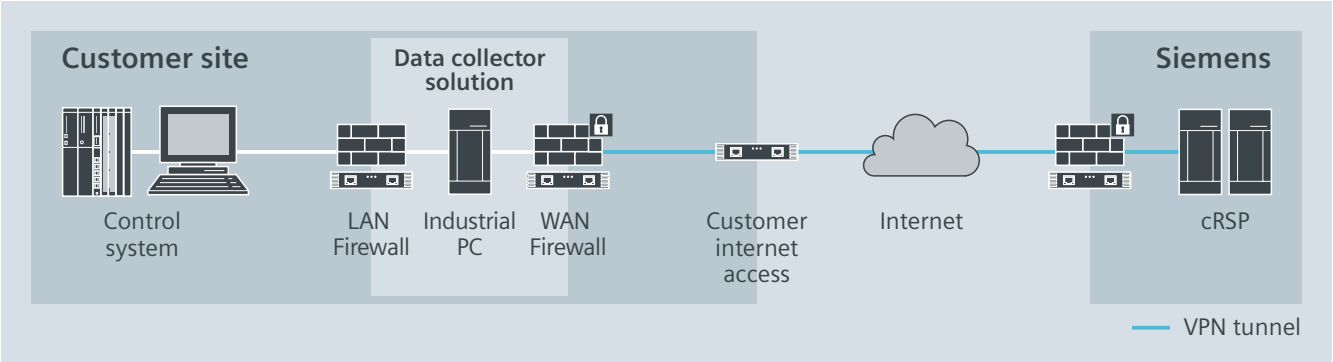

Figure 4. VPN situation 2a

- **SOA situation 2b – connection behind a customer firewall**
  If you are performing an SOA connection and the Siemens data collector solution's router is behind a firewall or border router, please perform the Port Forwarding as described in *Table 1*.

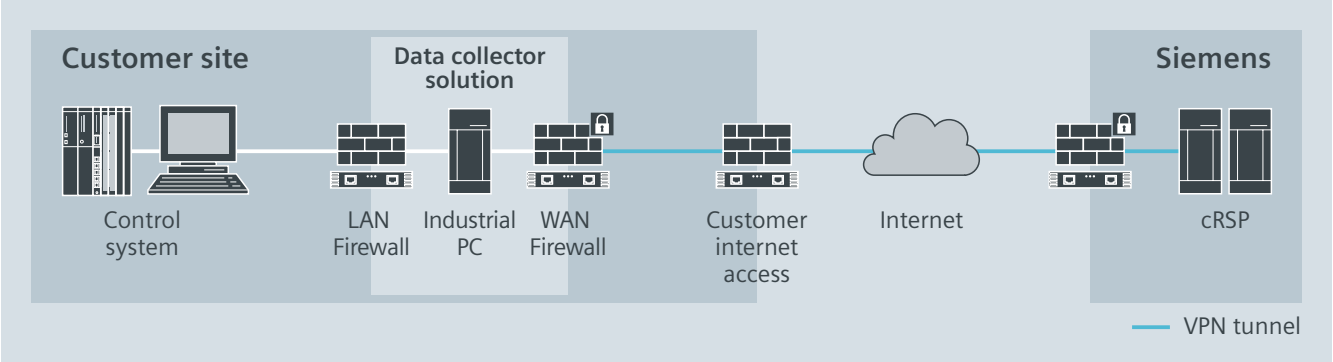

Figure 5. VPN situation 2b

- **SOA situation 2c – via central access in customer networks**
  In case more than one data collector has to be connected via IPsec, Siemens can provide a central router solution, as shown in *Figure 6* and with port forwarding information as shown in *Table 1*. The router is provided and maintained by Siemens and will forward the VPN IPsec tunnel to different VPN endpoints of the data collector solution. If this solution should be used, please contact your local Siemens representative to get more information.

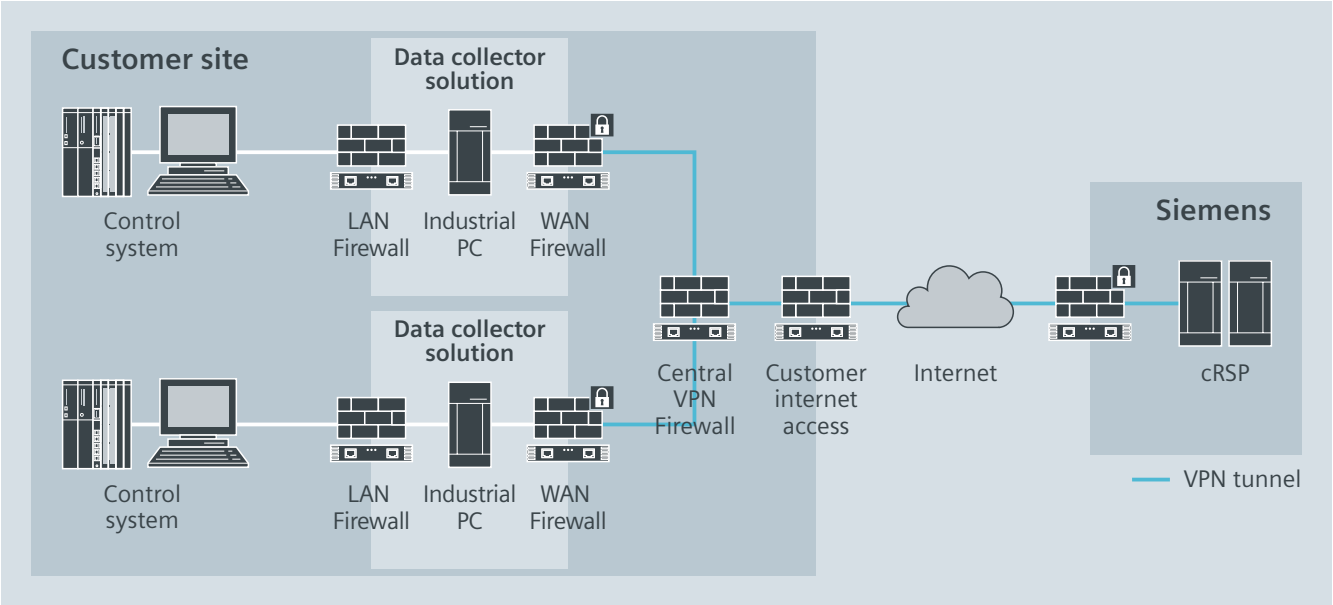

Figure 6. VPN situation 2c

Port Forwarding from customer Internet access to data collector solution's WAN firewall				
	Direction	Protocol	Port Number	Access Server
IKE	bidirectional	UDP	500	194.138.39.1 194.138.240.3 12.46.135.193
IKE NAT-Traversal	bidirectional	UDP	4500	194.138.39.1 194.138.240.3 12.46.135.193
ESP	bidirectional	IP	50	194.138.39.1 194.138.240.3 12.46.135.193
SSH	From customer access to data collector WAN firewall	TCP	22	213.146.112.253 213.146.112.254
HTTPS	From customer access to data collector WAN firewall	TCP	443	217.140.81.78

Table 1. SOA Port Forwarding information

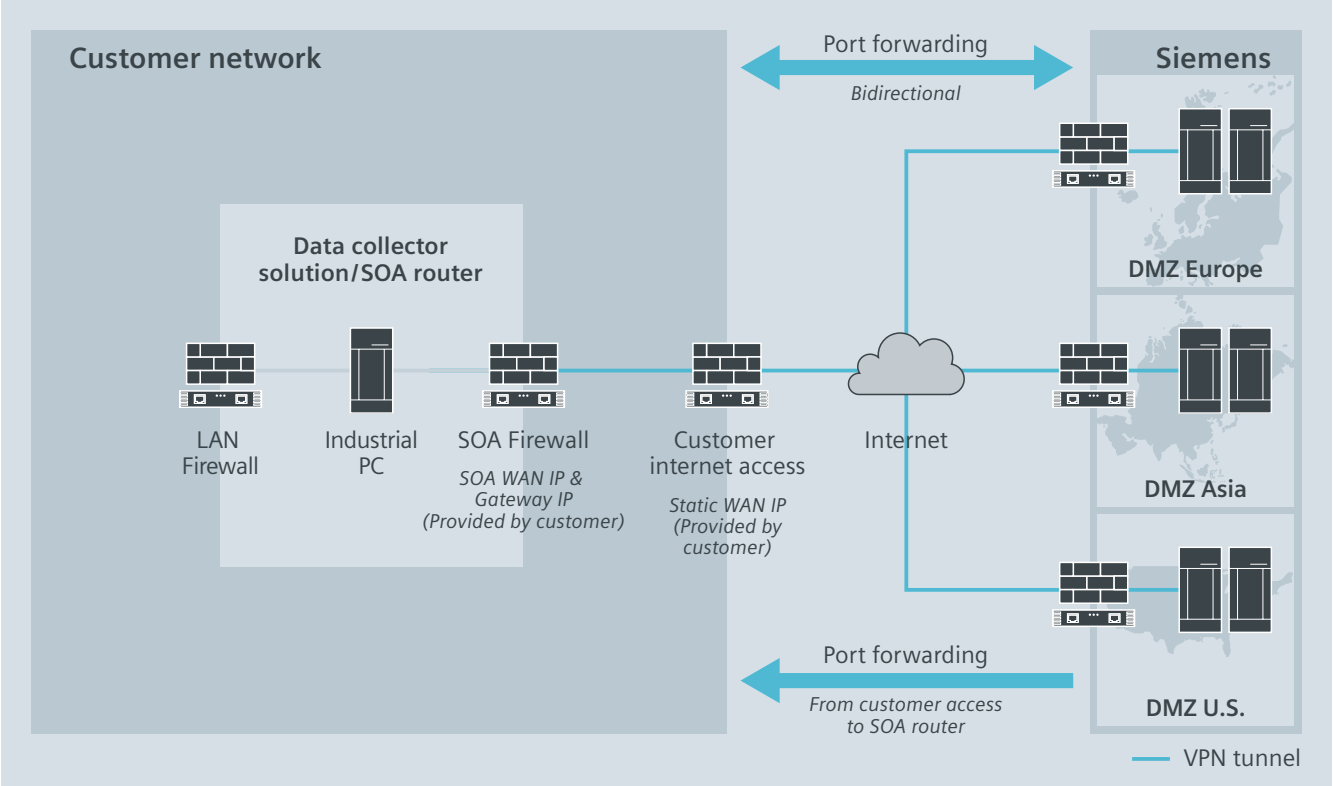

Figure 7. Implementation of SOA Port Forwarding

7.3. VPN situation 3: Customer-owned access (COA)

In case you want to use your own VPN endpoint, we can deploy the WAN firewall of the data collector solution to control IP traffic and implement specific firewall rules so that only the cRSP is connected to the solution. In this case, port forwarding is needed, which should be implemented from the VPN endpoint to the data collector solution as shown in *Figure 8*, with port forwarding information in *Table 2*.

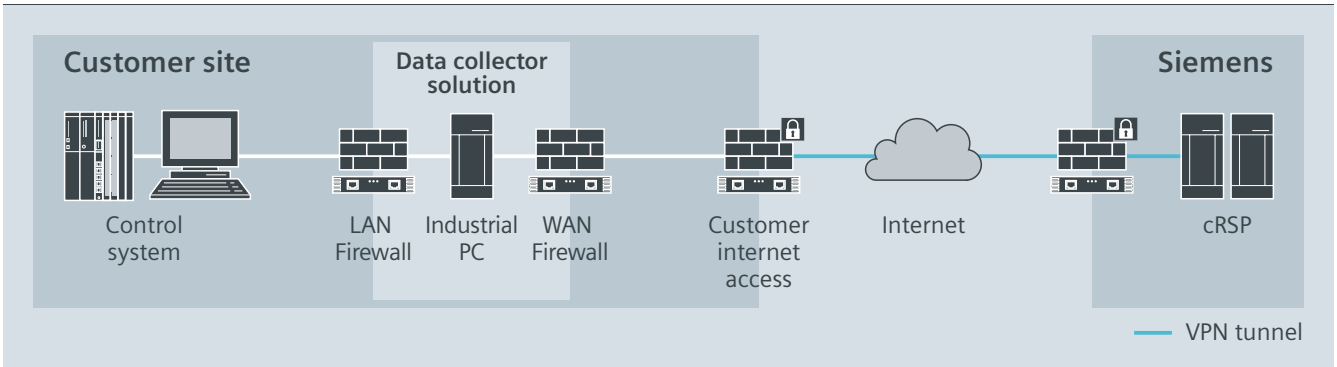

Figure 8. VPN situation 3

Port Forwarding from Customer Internet Access to data collector solution WAN firewall			
Application	Direction	Protocol	Port Number
RDP	From customer access to data collector WAN firewall	TCP	3389
VNC	From customer access to data collector WAN firewall	TCP	5900
https – Remote Trend Viewer	From customer access to data collector WAN firewall	TCP	443
Application License Manager *(transfer of engineering license if support is needed)*	From customer access to data collector WAN firewall	TCP	4410
Operation system updates	From data collector WAN firewall to customer access	TCP	8080
cRSP Service Agent *(File transfer)*	From data collector WAN firewall to customer access	TCP	943
cRSP Service Agent *(File transfer)* for software updates	From customer access to data collector WAN firewall	TCP	7783
smtp to send e-mail notifications to Siemens	From data collector WAN firewall to customer access	TCP	25
myHealth interface	From data collector WAN firewall to customer access	TCP	8010

Table 2. COA Port Forwarding information

7.4. VPN situation 4: UMTS

- **VPN UMTS situation 4a – UMTS based on IPsec**
  In a UMTS solution based on IPsec, you and Siemens, plus your Internet provider, must check if the provided IP address of the Internet connection is a public IP address, which is needed to implement the IPsec tunnel between Siemens and your site.

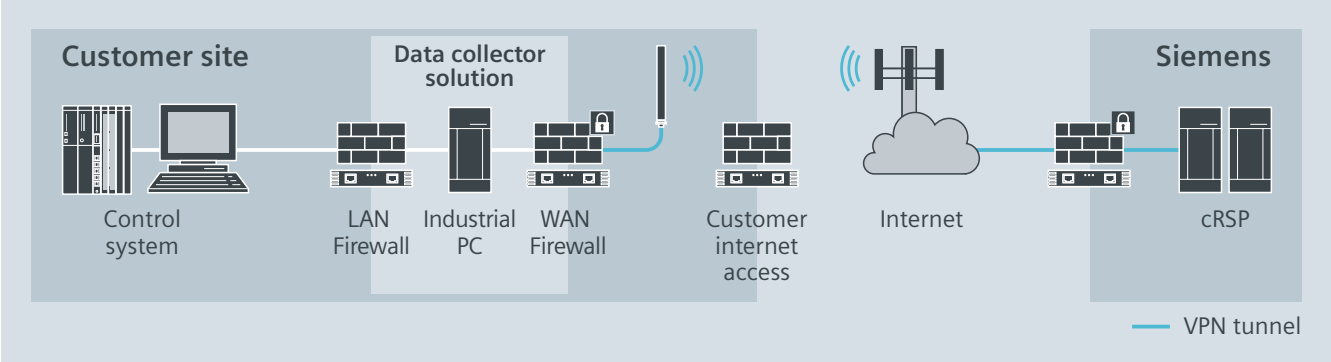

Figure 9. VPN situation 4a

- **VPN UMTS situation 4b – based on SSL**
  In this case, Siemens will install the SSL VPN client in the data collector solution and establish the VPN tunnel with SSL VPN to Siemens. The data collector solution's WAN firewall only allows SSL (TCP 443) traffic from the Siemens service portals.

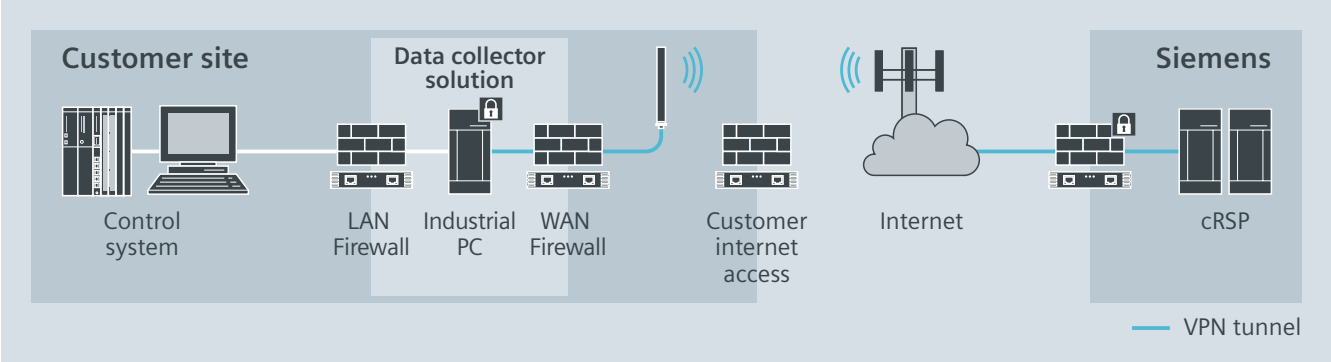

Figure 10. VPN situation 4b

7.5. cRSP VPN IPSec endpoints

cRSP VPN IPSec endpoints are shown in *Table 3*. Together, we will always need both primary and fallback portal IP addresses as cRSP VPN endpoints configured at your site.

	cRSP Portal	VPN Endpoint	cRSP Endpoint
Europe / Africa	Primary	194.138.39.1	194.138.39.0/27
	Fallback	12.46.135.193	129.73.116.64/27
Americas / Canada	Primary	12.46.135.193	129.73.116.64/27
	Fallback	194.138.39.1	194.138.39.0/27
Asia / Pacific	Primary	194.138.240.3	194.138.243.160/27
	Fallback	194.138.39.1	194.138.39.0/27

Table 3. cRSP VPN IPSec endpoints

7.6. cRSP SSL VPN endpoints

cRSP SSL VPN endpoints are shown in *Table 4*. Together, we will always need both primary and fallback portal IP addresses as cRSP SSL VPN endpoints configured at your site.

	cRSP Portal	VPN Endpoint	cRSP network
Europe / Africa	Primary	194.138.37.194	194.138.39.0/27
	Fallback	12.46.135.194	129.73.116.64/27
Americas / Canada	Primary	12.46.135.194	129.73.116.64/27
	Fallback	194.138.37.194	194.138.39.0/27
Asia / Pacific	Primary	194.138.240.119	194.138.243.160/27
	Fallback	194.138.37.194	194.138.39.0/27

Table 4. cRSP SSL VPN endpoints

8. Conclusion: Keeping your data safe and secure

More and more oil and gas customers worldwide are using Siemens RDS to gain greater asset availability and utilization as well as operational profitability. What's more, as our massive R&D investments each year generate innovations we can leverage in our RDS offering, you can gain additional benefits from them.

As valuable as the benefits of our RDS model are, in connected environments there are certain risks which have to be diminished. Siemens understands there is no way in compromising on cybersecurity, that's why we made great efforts to establish best-practice cybersecurity protocols in concert with the world's most rigorous cybersecurity standards to protect your data in motion and at rest.

This Operations Guide provides details about the Siemens RDS, its security model, strategy and specific defenses to assist you in understanding our approach in protecting your data connection. Further, it shows the process of establishing a connection, where Siemens is working closely with you to ensure that RDS is always a strong link in your overall cyber-risk model. As such, we want you to consider Siemens to be your trusted partner.

We look forward to working with you. In case of any question please contact your local Siemens Customer Support Manager.

Glossary

AH	Authentication Header
CAB	Change Advisory Board
CCB	Change Control Board
COA	Customer-owned access (i.e., customer-provided access)
cRSP	common Remote Service Platform
CWP	Customer Web Portal
DMZ	DeMilitarized Zone
ESP	Encrypted Secure Payload
ftp	file transfer protocol
IEC	International Electrotechnical Commission
IPsec	Internet Protocol security
ISO	International Organization for Standardization
ISAKMP	Internet Security Association and Key Management Protocol
IP	Internet Protocol
IT	Information Technology
KPI	Key Performance Indicator
LAN	Local Area Network
NERC CIP	North American Electric Reliability Corporation Critical Infrastructure Protection
OPC UA	Open Platform Communications Unified Architecture
OSD	Operational Service Desk
OT	Operational Technology
PKI	Public Key Infrastructure
RDS	Remote Diagnostic Service
SCP	Secure Copy Protocol
sFTP	Secure file transfer protocol
SHA	Secure Hash Algorithm
SOA	Siemens-owned access (i.e., Siemens-provided access)
SSL	Secure Socket Layer
TLS	Transport Layer Security
VPN	Virtual Private Network
WAN	Wide Area Network

Power Generation Services
Freyeslebenstraße 1
91058 Erlangen, Germany

For more information, please contact our Customer Support Center
Phone: +49 180 524 70 00
Fax: +49 180 524 24 71
(Charges depending on provider)
E-Mail: support.energy@siemens.com
siemens.com/energy

Order No: PSDG-T10085-00-7600 05.18 PF