Overview: Secure Remote Access with VPN

Industrial Security

Legal information

Use of application examples

Application examples illustrate the solution of automation tasks through an interaction of several components in the form of text, graphics and/or software modules. The application examples are a free service by Siemens AG and/or a subsidiary of Siemens AG ("Siemens"). They are non-binding and make no claim to completeness or functionality regarding configuration and equipment. The application examples merely offer help with typical tasks; they do not constitute customer-specific solutions. You yourself are responsible for the proper and safe operation of the products in accordance with applicable regulations and must also check the function of the respective application example and customize it for your system.

Siemens grants you the non-exclusive, non-sublicensable and non-transferable right to have the application examples used by technically trained personnel. Any change to the application examples is your responsibility. Sharing the application examples with third parties or copying the application examples or excerpts thereof is permitted only in combination with your own products. The application examples are not required to undergo the customary tests and quality inspections of a chargeable product; they may have functional and performance defects as well as errors. It is your responsibility to use them in such a manner that any malfunctions that may occur do not result in property damage or injury to persons.

Disclaimer of liability

Siemens shall not assume any liability, for any legal reason whatsoever, including, without limitation, liability for the usability, availability, completeness and freedom from defects of the application examples as well as for related information, configuration and performance data and any damage caused thereby. This shall not apply in cases of mandatory liability, for example under the German Product Liability Act, or in cases of intent, gross negligence, or culpable loss of life, bodily injury or damage to health, non-compliance with a guarantee, fraudulent non-disclosure of a defect, or culpable breach of material contractual obligations. Claims for damages arising from a breach of material contractual obligations shall however be limited to the foreseeable damage typical of the type of agreement, unless liability arises from intent or gross negligence or is based on loss of life, bodily injury or damage to health. The foregoing provisions do not imply any change in the burden of proof to your detriment. You shall indemnify Siemens against existing or future claims of third parties in this connection except where Siemens is mandatorily liable.

By using the application examples you acknowledge that Siemens cannot be held liable for any damage beyond the liability provisions described.

Other information

Siemens reserves the right to make changes to the application examples at any time without notice. In case of discrepancies between the suggestions in the application examples and other Siemens publications such as catalogs, the content of the other documentation shall have precedence.

The Siemens terms of use (https://support.industry.siemens.com) shall also apply.

Security information

Siemens provides products and solutions with Industrial Security functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens’ products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the Internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial security measures that may be implemented, please visit https://www.siemens.com/industrialsecurity.

Siemens’ products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer’s exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed at: https://www.siemens.com/industrialsecurity.
## Table of Contents

Legal information ........................................................................................................... 2

1 Remarks on this Document ....................................................................................... 5

1.1 Purpose and objective ......................................................................................... 5

1.2 Features and benefits ......................................................................................... 5

1.3 Structure of this document .................................................................................. 6

2 Introduction into Remote Networks ......................................................................... 7

2.1 Remote networks & industrial security ............................................................... 7

2.2 Security Integrated product portfolio ................................................................. 9

2.2.1 SINEMA Remote Connect ........................................................................... 10

2.2.2 SOFTNET Security Client .......................................................................... 11

2.2.3 SCALANCE S615, SCALANCE SC63x-2C und SC64x-2C ..................... 11

2.2.4 SCALANCE M-800 ...................................................................................... 12

2.2.5 CP ................................................................................................................ 14

2.2.6 TS Adapter IE Advanced ............................................................................ 15

2.2.7 LOGO! .......................................................................................................... 15

3 VPN with IPsec ........................................................................................................ 16

3.1 VPN tunnel between two SCALANCE SC ...................................................... 16

3.2 VPN tunnel between SCALANCE S (VPN server) and SCALANCE M81x-1 ......................................................................................... 17

3.3 VPN tunnel between SCALANCE S (VPN server) and SOFTNET Security Client ................................................................. 18

3.4 VPN tunnel between SCALANCE S (VPN server) and CP x43-1 Advanced .................................................................................. 19

3.5 VPN tunnel between SCALANCE S (VPN server) and SCALANCE M874-x .................................................................................. 20

3.6 VPN tunnel between SCALANCE S (VPN server) and a mobile client .................................................................................. 21

3.7 VPN tunnel between SCALANCE M81x-1 (VPN server) and SCALANCE M81x-1 .................................................................................. 22

3.8 VPN tunnel between SCALANCE S615 (VPN server) and SOFTNET Security Client ................................................................. 23

3.9 VPN tunnel between CP x43-1 Advanced (VPN server) and SCALANCE S .................................................................................. 24

3.10 VPN tunnel between CP x43-1 Advanced (VPN server) and SCALANCE M81x-1 .................................................................................. 25

3.11 VPN tunnel between CP x43-1 Advanced (VPN server) and SOFTNET Security Client ................................................................. 26

3.12 VPN tunnel between CP x43-1 Advanced (VPN server) and CP x43-1 Advanced .................................................................................. 27

3.13 VPN tunnel between CP x43-1 Advanced (VPN server) and SCALANCE M874-x .................................................................................. 28

3.14 VPN tunnel between CP x43-1 Advanced (VPN server) and a mobile client .................................................................................. 29

3.15 VPN tunnel between CP 1x43-1 (VPN server) and SOFTNET Security Client .................................................................................. 30

3.16 VPN tunnel between CP 1x43-1 (VPN server) and CP 1x43-1 .................................................................................. 31

3.17 VPN tunnel between CP 1543SP-1 (VPN server) and SCALANCE S615 .................................................................................. 33

4 VPN with OpenVPN .................................................................................................. 34

4.1 VPN tunnel between SINEMA Remote Connect Server and a tablet (iOS) .................................................................................. 34
Table of Contents

4.2 VPN tunnel between SINEMA RC Server and a smartphone (Android) ................................................................. 35
4.3 VPN tunnel between SCALANCE S615 and SINEMA RC client via the SINEMA RC server ........................................ 36
4.4 VPN tunnel between SCALANCE S615 and a tablet (iOS) via the SINEMA RC server ........................................... 37
4.5 VPN tunnel between SCALANCE S615 and a smartphone (Android) via the SINEMA RC server ............................. 38
4.6 VPN tunnel between two identical cells with S615 and SINEMA RC Client via the SINEMA RC Server by using the NAT function .......................... 39
4.7 JumpHost application with SINEMA RC Server .................................................. 40
4.8 VPN tunnel between LOGO! (VPN server) and a PC using a static IP address .......................................................... 41
4.9 Dedicated Remote Access with SINEMA Remote Connect ......................... 42
4.10 VPN tunnel between an PROFIBUS / MPI system and an Ethernet network .......................................................... 43

5 VPN with SSTP ......................................................................................................................................................... 45
5.1 VPN tunnel between TS Adapter IE Advanced (VPN server) and Windows SSTP client .............................................. 45
5.2 VPN tunnel between TS Adapter IE Advanced (VPN server) and TIA Portal .......................................................... 46

6 Appendix .................................................................................................................................................................. 47
6.1 Service and support ................................................................................................................................................. 47
6.2 Industry Mall ......................................................................................................................................................... 48
6.3 Links & Literature ................................................................................................................................................. 48
6.4 Change documentation ..................................................................................................................................... 48
1 Remarks on this Document

1.1 Purpose and objective

Purpose

Based on the Security Integrated product portfolio, there are numerous different ways of implementing a secure communication that are always customized to the application. For the user, looking for the perfect solution involves the following questions:

- Which solutions are available?
- What are the differences between the solutions?

Objective

The Security Integrated portfolio includes several products that can be combined with each other. This results in a large number of configuration options. This document helps you find an optimal solution for secure communication based on VPN.

1.2 Features and benefits

Properties

The document has the following features:

- Clear, compact structure
- Concisely outlines the contents and provides an overview graphic of the individual configurations
- Does not describe details; the details are provided in the individual configurations.

Benefits

The document offers the following benefits to the reader:

- Support in planning and configuration
- Quick finding of information regarding configuration options
- Short, compact overview of the features
- Reference to the individual configurations
1.3 Structure of this document

Siemens’ Security Integrated portfolio includes several products that can be combined with each other. This results in a large number of configuration options.

This document includes a choice of possible constellations. Each configuration is

- presented homogeneously in an overview graphic,
- including a list of requirements and
- the link for the detailed configuration description.

**SIMATIC independent**

The VPN solutions with the SCALANCE modules, TS Adapter or SINEMA Remote connect are **independent of SIMATIC**, i.e. the application behind the VPN tunnel does **not** have to be a SIMATIC application. Access to other applications is possible as well.

**SIMATIC-based**

The VPN solutions with the CPs are **SIMATIC-based**, since a SIMATIC CPU is required to operate the CP. However, these configurations also allow access to "non-SIMATIC" plant components via the CP.
2 Introduction into Remote Networks

2.1 Remote networks & industrial security

Remote networks

Remote networks are public or private communications infrastructures for covering wide areas or long distances, for example mobile or fixed telephone networks.

The geographical distribution of automation cells increases the demand for telecontrol (remote control) and teleservice (remote maintenance/diagnostics) in a remote network.

The comprehensive Remote Networks portfolio from Siemens offers connection to both conventional (dedicated line, telephone) and IP-based infrastructures (e.g., the Internet).

Applications

Possible remote access applications in a remote network:

- **Telecontrol**
  Connection of outstations (remote terminal units - RTUs) distributed over a wide geographical area to one or more central control systems for the purpose of operator control and monitoring.

- **Teleservice**
  Data exchange with distant technical systems such as machines, plants and computers for the purpose of error detection, diagnostics, maintenance, repair and optimization.

Integration into the industrial security concept

This document focuses on **IP-based** networks.

Since remote access to the plant is implemented via a public network (e.g., the Internet), **protection against data manipulation** and spying is particularly important. For this purpose, virtual private networks (VPN) are used.

VPN

A VPN is a private network that uses a public network (e.g., the Internet) as a transit network for transmitting data to a private destination network. The private networks and the transit network need not be compatible with one another.

Although VPN uses the addressing mechanisms of the transit network, it nevertheless uses its own network packets to separate the transport of private data packets from the others. Due to this fact, the private networks appear as a shared, logical (virtual) network.

VPN routers are required to set up a VPN.

To set up a VPN, there are several protocols available e.g. IPsec, OpenVPN, SSTP.
2 Introduction into Remote Networks
2.1 Remote networks & industrial security

VPN client and VPN server

The nodes of a secured data communication via VPN take on different roles:

- VPN server
- VPN client

The tunnel endpoint that actively starts the VPN connecting process is referred to as VPN client.
The remote end that waits for the VPN client is called the VPN server.

Note
More information on the Siemens Security Concept you find in chapter 6.1.
2.2 Security Integrated product portfolio

Through a combination of different security measures such as firewalls and VPN, the security modules protect individual devices or even entire automation cells against:

- Data espionage
- Data manipulation
- Unwanted access

The figure below shows the remote access cells.

To help you select products, the following sections describe the most important features of the respective security modules.
2.2.1 SINEMA Remote Connect

SINEMA Remote Connect is a management platform for remote networks that centrally manages secure tunnel connections. Distributed plants or machines can be conveniently and safely serviced via remote access. Even if the machines are integrated in third-party networks; for example, in the plants at the end customers of machine constructors.

Components of a solution with SINEMA Remote Connect:
- SINEMA Remote Connect as VPN server
- End device (VPN client):
  - Industrial Security appliances: SCALANCE S-600 and SC-600
  - SCALANCE M-800 mobile communication devices
  - SIMATIC RTU3030C
  - SIMATIC CP1243-1
  - SIMATIC CP1543(SP)-1
  - SINEMA Remote Connect Client

SINEMA Remote Connect Server

SINEMA Remote Connect Server is a server application and provides an integrated connection management of distributed networks via the internet. It coordinates the secure connecting process between users, distributed plants, and machines.

The following functions are handled by the SINEMA Remote Connect server:
- Management and establishing of encrypted connections with OpenVPN and IPsec.
- Verification via CA certificate or finger print.
- User management with the configuration of privileges.
- Establishing permanent or event-based connections (connecting via wake up SMS or via a signal at the digital input).
- Supporting routing and NAT for connecting subnets behind SCALANCE.
- Provision of secure remote access to subordinate networks for servicing, control and diagnostic purposes.
- Web Based Management (WBM) for configuring the server.

SINEMA Remote Connect Client

SINEMA Remote Connect Client is an OpenVPN Client software for optimal connection of programming devices, PCs and notebooks to the SINEMA Remote Connect server.

It is characterized by the following features:
- Support of VPN (OpenVPN) for secure authentication of network nodes, for data encryption and verifying data integrity.
- Simplest connection to SINEMA Remote Connect via auto configuration interface.
- Address book with all devices assigned to a user.
- Proxy server for communication with networks behind a proxy server infrastructure.
2 Introduction into Remote Networks

2.2 Security Integrated product portfolio

- Support of HTTPS and SOCKS Proxy Server.
- Selecting a device for performing teleservice within the SIMATIC environment.

2.2.2 SOFTNET Security Client

The SOFTNET Security Client allows programming devices, PCs and notebook computers access to network nodes or automation systems protected by SCALANCE S, SCALANCE M or CPs.

It is characterized by the following features:

- Secure access of programming devices or notebook computers to entire automation cells.
- Easy use on mobile PCs.
- Non-secure devices can be integrated into the secure data traffic.
- Supports the DNS client function.

2.2.3 SCALANCE S615, SCALANCE SC63x-2C und SC64x-2C

SCALANCE is a Security module for securing devices, automation cells, or network segments in Ethernet networks against external and internal dangers.

Amongst others, SCALANCE S615 or SCALANCE SC is distinguished by the following characteristics:

- Support of VPN for secure authentication of network nodes, for data encryption and verifying data integrity.
  - IPsec VPN tunnel (server and client functionality)
  - OpenVPN for connecting to SINEMA Remote Connect (client function)
- High-quality stateful inspection firewall with filtering of IP-based data traffic and communication protocols.
- Support of NAT/NAPT; also in connection with IPsec and OpenVPN.
- Supporting VLAN.
- Flexible, reaction-free and protocol-independent protection.
- Support of multiple VPN tunnels at a time.
- Simplest connection to SINEMA Remote Connect via Auto configuration interface (S615: can be enabled via KEY-PLUG SINEMA REMOTE CONNECT).
- The SCALANCE SC has 2x Combo Port electrical or optical.
2.2.4 SCALANCE M-800

SCALANCE M87x

The SCALANCE M87x routers are suited for cellular networks.
- SCALANCE M874-2
  EGPRS / GPRS (2G): 850, 900, 1800 or 1900 MHz
- SCALANCE M874-3 / M876-3
  UMTS (3G): 800, 850, 900, 1900 or 2100 MHz
- SCALANCE M876-4
  LTE (4G): 800, 900, 1800, 2100 or 2600 MHz

These modules are characterized by the following features:
- Support of VPN for secure authentication of network nodes, for data encryption and verifying data integrity.
  - IPsec VPN tunnel (server and client functionality)
  - OpenVPN for connecting to SINEMA Remote Connect (client function)
- Broad range of applications; can be used wherever a GPRS/UMTS network is available.
- Receive SMS and sending SMS.
- Support of RSTP and VRRPv3.
- Connection of stationary stations and/or mobile stations.
- Simplicity of connecting local networks by means of IP communication via WAN.
- User-specific IP firewall to distinguish and differentiate access to specific plant parts.
- Simplest connection to SINEMA Remote Connect via Auto configuration interface (can be enabled via KEY-PLUG SINEMA REMOTE CONNECT).

SCALANCE M81x-1, M826

These modules are DSL routers for cost-effective, secure connection of Ethernet-based subnets and programmable controllers to wired telephone or DSL networks. They support ADSL2+ (Asynchronous Digital Subscriber Line) or SHDSL.

These modules are characterized by the following features:
- Support of VPN for secure authentication of network nodes, for data encryption and verifying data integrity.
  - IPsec VPN tunnel (server and client functionality)
  - OpenVPN for connecting to SINEMA Remote Connect (client function)
- VPN and DSL router in a single device; therefore, it is no longer necessary to use a separate DSL router.
- Support of RSTP and VRRPv3.
- Broad range of applications due to high bandwidth, performance and speed.
- Reduced travel expenses and personnel costs due to remote programming and remote diagnostics via wired telephone or DSL networks.
- User-specific IP firewall to distinguish and differentiate access to specific plant parts.
- Simplest connection to SINEMA Remote Connect via Auto configuration interface (can be enabled via KEY-PLUG SINEMA REMOTE CONNECT).
2 Introduction into Remote Networks

2.2 Security Integrated product portfolio
2 Introduction into Remote Networks

2.2 Security Integrated product portfolio

2.2.5 CP

CP x43-1 Advanced

CP 343-1 Advanced and CP 443-1 Advanced are communications processors for connecting SIMATIC S7-CPU to PROFINET / Industrial Ethernet networks. For the SIMATIC S7-300/S7-400, they are the bridge between the field level and the MES level and integrate seamlessly with the security structures of the office and IT world.

These modules are characterized by the following features:
• Firewall, VPN gateway and communications processor in a single device
• Protection of S7-300/S7-400 controllers and their lower-level networks by IPsec tunnels

CP 1x43-x

The CP 1243-x communication processor securely connects the SIMATIC S7-1200 controller to Ethernet networks.
The CP 1543-1 communication processor securely connects the SIMATIC S7-1500 controller to Ethernet networks.
The CP 1543SP-1 communication processor securely connects the SIMATIC ET 200SP to Ethernet networks.

These modules are characterized by the following features:
• Firewall, VPN gateway and communications processor in a single device
• Protection of S7-1x00/ ET 200SP controllers and their lower-level networks by IPsec tunnels

CP 1628

CP 1628 is a communications module for securely connecting a PG/PC to Industrial Ethernet. With a dedicated processor for automation/security tasks, the CP 1628 reduces the host PC's load and provides constant, stable and secure data communication.

This module is characterized by the following features:
• Firewall, VPN gateway and communications processor in a single device.
• Simultaneous protection of multiple devices by IPsec tunnels
2 Introduction into Remote Networks

2.2 Security Integrated product portfolio

2.2.6 TS Adapter IE Advanced

In conjunction with TIA Portal (V12 SP1 or higher), the TS Adapter IE Advanced allows access, through the Internet, to all automation components of a plant (e.g., S7 controllers) that are connected to Industrial Ethernet.

This module is characterized by the following features:

- Aside from TIA Portal, no other software or hardware is required to establish the VPN connection (VPN client).¹
- Protection of S7 controllers and their lower-level networks by SSTP.

2.2.7 LOGO!

LOGO! Siemens is an intelligent logic module and ideally suitable for the realization of simple automation tasks in industry and building technology. The use of expansion modules enables LOGO! to control even complex plants without any problems.

Using LOGO! CMR in combination with the LOGO! 8 basic modules (BM) makes it possible for you to monitor and control distributed plants and systems via text messages. You can remotely access the web interface of LOGO! CMR and LOGO! BM via mobile wireless network. The remote access makes it possible, for example, to install the LOGO! BM program remotely.

¹ Internet access and a DSL modem are required to access the Internet.
3 VPN with IPsec

3.1 VPN tunnel between two SCALANCE SC

Overview

Figure 3-1

Requirements

- Static public IP address for the Internet router of the VPN server
- Internet router with port forwarding functionality (on the VPN server side)
- Standard Internet modem, router or UMTS router, for example SCALANCE M-800 (on the VPN client side)

Link to the configuration description:
3.2 VPN tunnel between SCALANCE S (VPN server) and SCALANCE M81x-1

Overview

Figure 3-2

Requirements

- Static public IP address for the Internet router of the VPN server.
- Internet router with port forwarding functionality (on the VPN server side).

Link to the configuration description:

3.3 VPN tunnel between SCALANCE S (VPN server) and SOFTNET Security Client

Overview

Requirements

- Static public IP address for the Internet router of the VPN server.
- Internet router with port forwarding functionality (on the VPN server side).
- Standard Internet modem, router or UMTS router, for example SCALANCE M873 (on the VPN client side).

Link to the configuration description:

3.4 VPN tunnel between SCALANCE S (VPN server) and CP x43-1 Advanced

Overview

Requirements

- Static public IP address for the Internet router of the VPN server.
- Internet router with port forwarding functionality (on the VPN server side).
- Standard Internet modem, router or UMTS router, for example SCALANCE M873 (on the VPN client side).

Link to the configuration description:
3.5 VPN tunnel between SCALANCE S (VPN server) and SCALANCE M874-x

Overview

Figure 3-5

Requirements

- Static public IP address for the Internet router of the VPN server.
- Internet router with port forwarding functionality (on the VPN server side).
- Mobile network operator's default APN (on the VPN client side).

Link to the configuration description:

3.6 VPN tunnel between SCALANCE S (VPN server) and a mobile client

Overview

Figure 3-6

Requirements

- Static public IP address for the Internet router of the VPN server.
- Internet router with port forwarding functionality (on the VPN server side).
- Mobile network operator's default APN (on the VPN client side).
- Smartphone with IPSec Client app and Android operating system (on the VPN client side).

Link to the configuration description:
3.7 VPN tunnel between SCALANCE M81x-1 (VPN server) and SCALANCE M81x-1

Overview

Figure 3-7

Requirements

- Static public IP address for the VPN server.

Link to the configuration description:

3.8 **VPN tunnel between SCALANCE S615 (VPN server) and SOFTNET Security Client**

**Overview**

![Diagram of VPN tunnel](image)

**Requirements**
- Static public IP address from the mobile network operator that can also be accessed from the Internet (on the VPN server side).
- Standard Internet modem, router or UMTS router, for example SCALANCE M873 (on the VPN client side).

**Link to the configuration description:**
3.9 VPN tunnel between CP x43-1 Advanced (VPN server) and SCALANCE S

Overview

Figure 3-9

Requirements

- Static public IP address for the Internet router of the VPN server.
- Internet router with port forwarding functionality (on the VPN server side).
- Standard Internet modem, router or UMTS router, for example SCALANCE M873 (on the VPN client side).

Link to the configuration description:
3 VPN with IPsec

3.10 VPN tunnel between CP x43-1 Advanced (VPN server) and SCALANCE M81x-1

3.10 VPN tunnel between CP x43-1 Advanced (VPN server) and SCALANCE M81x-1

Overview

Figure 3-10

Requirements

- Static public IP address for the Internet router of the VPN server.
- Internet router with port forwarding functionality (on the VPN server side).

Link to the configuration description:

3 VPN with IPsec

3.11 VPN tunnel between CP x43-1 Advanced (VPN server) and SOFTNET Security Client

3.11 VPN tunnel between CP x43-1 Advanced (VPN server) and SOFTNET Security Client

Overview

Figure 3-11

Requirements

- Static public IP address for the Internet router of the VPN server.
- Internet router with port forwarding functionality (on the VPN server side).
- Standard Internet modem, router or UMTS router, for example SCALANCE M873 (on the VPN client side).

Link to the configuration description:

3.12 VPN tunnel between CP x43-1 Advanced (VPN server) and CP x43-1 Advanced

Overview

Figure 3-12

Requirements

- Static public IP address for the Internet router of the VPN server.
- Internet router with port forwarding functionality (on the VPN server side).
- Standard Internet modem, router or UMTS router, for example SCALANCE M873 (on the VPN client side).

Link to the configuration description:
3 VPN with IPsec

3.13 VPN tunnel between CP x43-1 Advanced (VPN server) and SCALANCE M874-x

3.13 VPN tunnel between CP x43-1 Advanced (VPN server) and SCALANCE M874-x

Overview

Figure 3-13

Requirements

- Static public IP address for the Internet router of the VPN server.
- Internet router with port forwarding functionality (on the VPN server side).
- Mobile network operator's default APN (on the VPN client side).

Link to the configuration description:
3 VPN with IPsec

3.14 VPN tunnel between CP x43-1 Advanced (VPN server) and a mobile client

## 3.14 VPN tunnel between CP x43-1 Advanced (VPN server) and a mobile client

### Overview

Figure 3-14

![Diagram of VPN tunnel between CP x43-1 Advanced (VPN server) and a mobile client](image)

### Requirements

- Static public IP address for the Internet router of the VPN server.
- Internet router with port forwarding functionality (on the VPN server side).
- Mobile network operator's default APN (on the VPN client side).
- Smartphone with IPSec Client app and Android operating system (on the VPN client side).

### Link to the configuration description:

3.15 **VPN tunnel between CP 1x43-1 (VPN server) and SOFTNET Security Client**

**Overview**

Figure 3-15

- **Requirements**
  - Static public IP address for the Internet router of the VPN server.
  - Internet router with port forwarding functionality (on the VPN server side).
  - Standard Internet modem, router or UMTS router, for example SCALANCE M873 (on the VPN client side).

**Link to the configuration description:**

3.16 VPN tunnel between CP 1x43-1 (VPN server) and CP 1x43-1

Overview

Requirements

- Static public IP address for the Internet router of the VPN server.
- Internet router with port forwarding functionality (on the VPN server side).
- Standard Internet modem, router or UMTS router, for example SCALANCE M873 (on the VPN client side).

Link to the configuration description:

3.16 VPN tunnel between CP 1x43-1 (VPN server) and CP 1x43-1
3.17 **VPN tunnel between CP 1543SP-1 (VPN server) and SCALANCE S615**

**Overview**

Figure 3-17

**Requirements**

- Static public IP address for the Internet router of the VPN server.
- Internet router with port forwarding functionality (on the VPN server side).
- Standard Internet modem, router or UMTS router, for example SCALANCE M873 (on the VPN client side).

**Link to the configuration description:**

4 VPN with OpenVPN

4.1 VPN tunnel between SINEMA Remote Connect Server and a tablet (iOS)

**Overview**

![Network Diagram](image)

**Requirements**

- Static public IP address for the Internet router of the VPN server.
- Internet router with port forwarding functionality (on the VPN server side).
- Tablet with "OpenVPN Client" app and iOS operating system (VPN client side).
- Standard internet router with WLAN functionality (VPN client side).

**Link to the configuration description:**

4 VPN with OpenVPN

4.2 VPN tunnel between SINEMA RC Server and a smartphone (Android)

4.2 VPN tunnel between SINEMA RC Server and a smartphone (Android)

Overview

Figure 4-2

Requirements

- Static public IP address for the Internet router of the VPN server.
- Internet router with port forwarding functionality (on the VPN server side).
- Mobile network operator’s default APN (on the VPN client side).
- Smartphone with "OpenVPN Client" app and Android operating system (VPN client side).

Link to the configuration description:

4.3 VPN tunnel between SCALANCE S615 and SINEMA RC client via the SINEMA RC server

Overview

Requirements

- Static public IP address for the Internet router of the VPN server.
- Internet router with port forwarding functionality (on the VPN server side).
- Standard Internet modem, router or UMTS router, for example SCALANCE M873 (on the VPN client side).

Link to the configuration description:

4.4 VPN tunnel between SCALANCE S615 and a tablet (iOS) via the SINEMA RC server

Overview

Requirements

- Static public IP address for the Internet router of the VPN server.
- Internet router with port forwarding functionality (on the VPN server side).
- Standard Internet modem, router or UMTS router, for example SCALANCE M873 (on the VPN client side).
- Tablet with "OpenVPN Client" app and iOS operating system (VPN client side).

Link to the configuration description:

4 VPN with OpenVPN

4.5 VPN tunnel between SCALANCE S615 and a smartphone (Android) via the SINEMA RC server

4.5 **VPN tunnel between SCALANCE S615 and a smartphone (Android) via the SINEMA RC server**

**Overview**

![Diagram](image)

**Requirements**

- Static public IP address for the Internet router of the VPN server.
- Internet router with port forwarding functionality (on the VPN server side).
- Mobile network operator's default APN (on the VPN client side).
- Smartphone with "OpenVPN Client" app and Android operating system (VPN client side).

**Link to the configuration description:**

4.6 VPN tunnel between two identical cells with S615 and SINEMA RC Client via the SINEMA RC Server by using the NAT function

Overview

Requirements

- Static public IP address and port forwarding for the Internet router of the VPN server.
- Identical IP subnet in the automation cells

Link to the configuration description: http://support.automation.siemens.com/WW/view/en/109744972
4.7 JumpHost application with SINEMA RC Server

Overview

Figure 4-7

Requirements

- Static public IP address and port forwarding for the Internet router of the VPN server.
- DMZ with SINEMA Remote Connect Server and JumpHost Virtual Desktop

4.8 VPN tunnel between LOGO! (VPN server) and a PC using a static IP address

Overview

Figure 4-8

Requirements

- Static public IP address for the SIM card of the VPN server.
- Standard Internet modem, router or UMTS router, for example SCALANCE M873 (on the VPN client side).

Link to the configuration description:

4.9 Dedicated Remote Access with SINEMA Remote Connect

Overview

Requirements

- Static public IP address and port forwarding for the Internet router of the VPN server.
- SINEMA Remote Connect V2.0 or higher

Link to the configuration description:

4 VPN with OpenVPN

4.10 VPN tunnel between an PROFIBUS / MPI system and an Ethernet network

4.10 VPN tunnel between an PROFIBUS / MPI system and an Ethernet network

Overview

Abbildung 4-10

Servicezentrale

- SINEMA RC-Server

Servicetechniker

- TIA Portal Cloud Connector (Client)
- SINEMA RC-Client
- TIA Portal/STEP 7

Station

- TIA Portal Cloud Connector (Server)
- SINEMA RC-Gerät
- Zugangspunkt zu SIMATIC S7-300

Online-Verbindung zu SIMATIC S7-300
4 VPN with OpenVPN

4.10 VPN tunnel between an PROFIBUS / MPI system and an Ethernet network

Requirements

- SCALANCE M804PB on Station side
- SINEMA Remote Connect V2.0 or higher

Link to the configuration description:

5 VPN with SSTP

5.1 VPN tunnel between TS Adapter IE Advanced (VPN server) and Windows SSTP client

Overview

Requirements

- Static public IP address for the Internet router of the VPN server.
- Internet router with port forwarding functionality (on the VPN server side).
- Standard Internet modem, router or UMTS router, for example SCALANCE M873 (on the VPN client side).
- Windows 7 or Windows Server 2008 or higher.

Link to the configuration description:

5.2 VPN tunnel between TS Adapter IE Advanced (VPN server) and TIA Portal

Overview

Figure 5-2

Requirements

- Static public IP address for the Internet router of the VPN server.
- Internet router with port forwarding functionality (on the VPN server side).
- Standard Internet modem, router or UMTS router, for example SCALANCE M873 (on the VPN client side).
- TIA Portal V12 SP1 or higher.

Link to the configuration description:
6 Appendix

6.1 Service and support

Industry Online Support
Do you have any questions or need assistance?
Siemens Industry Online Support offers round the clock access to our entire service and support know-how and portfolio.
The Industry Online Support is the central address for information about our products, solutions and services.
Product information, manuals, downloads, FAQs, application examples and videos – all information is accessible with just a few mouse clicks:
support.industry.siemens.com

Technical Support
The Technical Support of Siemens Industry provides you fast and competent support regarding all technical queries with numerous tailor-made offers – ranging from basic support to individual support contracts. Please send queries to Technical Support via Web form:
www.siemens.com/industry/supportrequest

SITRAIN – Digital Industry Academy
We support you with our globally available training courses for industry with practical experience, innovative learning methods and a concept that’s tailored to the customer’s specific needs.
For more information on our offered trainings and courses, as well as their locations and dates, refer to our web page:
www.siemens.com/sitrain

Service offer
Our range of services includes the following:
- Plant data services
- Spare parts services
- Repair services
- On-site and maintenance services
- Retrofitting and modernization services
- Service programs and contracts
You can find detailed information on our range of services in the service catalog web page:
support.industry.siemens.com/cs/sc

Industry Online Support app
You will receive optimum support wherever you are with the "Siemens Industry Online Support" app. The app is available for iOS and Android:
support.industry.siemens.com/cs/ww/en/sc/2067
6.2 Industry Mall

The Siemens Industry Mall is the platform on which the entire Siemens Industry product portfolio is accessible. From the selection of products to the order and the delivery tracking, the Industry Mall enables the complete purchasing processing – directly and independently of time and location:

mall.industry.siemens.com

6.3 Links & Literature

Table 6-1

<table>
<thead>
<tr>
<th>Nr.</th>
<th>Thema</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Siemens Industry Online Support</td>
</tr>
<tr>
<td></td>
<td><a href="https://support.industry.siemens.com">https://support.industry.siemens.com</a></td>
</tr>
<tr>
<td>2</td>
<td>Link to this entry page of this application example</td>
</tr>
<tr>
<td>3</td>
<td>Topic page ”Industrial Security” - Network security</td>
</tr>
</tbody>
</table>

6.4 Change documentation

Table 6-2

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Modifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>V1.0</td>
<td>08/2014</td>
<td>First version</td>
</tr>
<tr>
<td>V1.1</td>
<td>09/2015</td>
<td>Integrating SINEMA Remote Connect as new VPN server</td>
</tr>
<tr>
<td>V2.0</td>
<td>11/2015</td>
<td>New Cluster (Merging SCALANCE M and integration of SCALANCE S615) Deleting Chapter for dynamic IP</td>
</tr>
<tr>
<td>V2.1</td>
<td>03/2017</td>
<td>New Example (chapter 5.6)</td>
</tr>
<tr>
<td>V3.0</td>
<td>05/2018</td>
<td>Update and new cluster</td>
</tr>
</tbody>
</table>