SIEMENS
Ingenuity for life

Port Release on the VPN Client Side

SINEMA Remote Connect

https://support.industry.siemens.com/cs/ww/en/view/ 109745584

Siemens
Industry
Online
Support

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 only form one element of such a concept.
The customer is responsible to prevent unauthorized access to its plants, systems, machines and networks. Systems, machines and components should only be connected to the enterprise network or the internet if and to the extent necessary and with appropriate security measures (e.g. use of firewalls and network segmentation) in place.
Additionally, Siemens' guidance on appropriate security measures should be taken into account. For more information about industrial security, please visit http://www.siemens.com/industrialsecurity.

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends to apply product updates as soon as available and to always use the latest product versions. Use of product versions that are no longer supported, and failure to apply latest updates may increase the customer's exposure to cyber threats.
To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under http://www.siemens.com/industrialsecurity.

Contents

1 Overview 3
2 Port Release on the VPN Client Side 4

1 Overview

Devices that can be connected to SINEMA RC by autoconfiguration (SCALANCE S615 and SCALANCE SC-600, for example) and the SINEMA Remote Connect Server are to establish a secured connection via OpenVPN.

To enable a secured connection you have to make appropriate settings on the VPN client side and on the VPN server side. These are the settings:

- Port forwarding on the VPN server side (ports used in the server)
- Port release in the firewall on the VPN client side (connection to the internet)

This document shows the settings to be made on the VPN client side.

2 Port Release on the VPN Client Side

You have to make the following settings in order to connect devices that can be connected to SINEMA RC by autoconfiguration (SCALANCE S615 and SCALANCE SC-600, for example) to the SINEMA Remote Connect Server via OpenVPN:

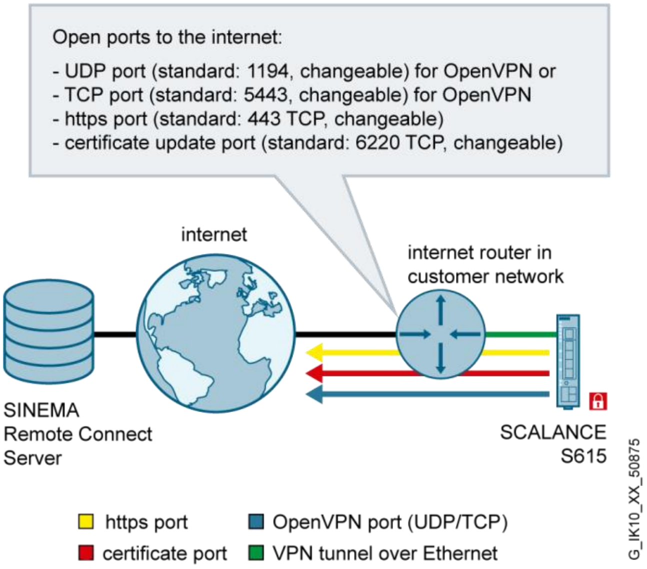
- All devices that can be connected to SINEMA RC by autoconfiguration (SCALANCE S615 and SCALANCE SC-600, for example) need an IP address with gateway via DHCP (alternatively also static) at the WAN port (external network).
- The following ports must be released in the firewall / proxy of the client in the direction of the internet (outgoing rule in the firewall):
  - https port for the autoconfiguration interface (modifiable, preset: 443; this can be set as required by the owner of the SINEMA RC server)
  - UDP port to set up the OpenVPN tunnel (modifiable, preset: 1194; this can be set as required by the owner of the SINEMA RC server)

    or

  - TCP port to set up the OpenVPN tunnel (modifiable, preset: 5443; this can be set as required by the owner of the SINEMA RC server)
  - TCP port 6220 for the certificate update
    (SCALANCE S615/M-800 firmware version V4.3.1/ V5 and higher and SCALANCE SC-600 firmware version V1.1 and higher:
    modifiable, preset: 6220)

The ports that are not preset fixed can be modified in the configuration of SINEMA Remote Connect Server.

Figure 2-1


Open ports to the internet:
- UDP port (standard: 1194, changeable) for OpenVPN or
- TCP port (standard: 5443, changeable) for OpenVPN
- https port (standard: 443 TCP, changeable)
- certificate update port (standard: 6220 TCP, changeable)
internet
internet router in customer network
SINEMA Remote Connect Server
SCALANCE S615
🟨 https port
🟦 OpenVPN port (UDP/TCP)
🟥 certificate port
🟩 VPN tunnel over Ethernet
G_IK10_XX_50875