Port Forwarding on the VPN Server Side

SINEMA Remote Connect

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

Siemens Industry Online Support

This entry is from the Siemens Industry Online Support. The general terms of use (http://www.siemens.com/terms_of_use) 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 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

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 in the router 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 server side.

2 Port Forwarding on the VPN Server Side

In order for the SINEMA Remote Connect Server to be accessible from the internet side you have to forward a number of ports to the SINEMA Remote Connect Server in the internet router (on the VPN server side).

Note For this your router must support port forwarding and you have to configure corresponding incoming rules.

You must forward the following ports to the SINEMA Remote Connect Server:

- Port forwarding of the https port (modifiable, preset: 443)
- Port forwarding of the UDP port to set up the OpenVPN tunnel (modifiable, preset: 1194)

  or

- Port forwarding of the TCP port to set up the OpenVPN tunnel (modifiable, preset: 5443)
- Port forwarding of Port 6220 for the certificate update
  (SINEMA Remote Connect Server <V1.3: set fixed at 6220;
  SINEMA Remote Connect Server V1.3 or 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