Security Configurations in LAN and WAN (DSL) with SCALANCE S61x Modules and the Softnet Security Client

Industrial Security

Application Description • March 2010

Applications & Tools

Answers for industry.

SIEMENS

Industry Automation and Drives Technologies Service & Support Portal

This article is taken from the Service Portal of Siemens AG, Industry Automation and Drives Technologies. The following link takes you directly to the download page of this document.

http://support.automation.siemens.com/WW/view/en/27043887

If you have any questions about this document, please contact us at the following e-mail address:

online-support.automation@siemens.com

S

SIMATIC
Security

Security Configurations in LAN and WAN (DSL) with SCALANCE S61x Modules and the Softnet Security Client

Warranty and Liability

Note

The application examples are not binding and do not claim to be complete regarding configuration, equipment and any eventuality. The application examples do not represent customer-specific solutions. They are only intended to provide support for typical applications. You are responsible for ensuring that the described products are used correctly. These application examples do not relieve you of the responsibility to use sound practices in application, installation, operation and maintenance. When using these Application Examples, you recognize that we cannot be made liable for any damage/claims beyond the liability clause described. We reserve the right to make changes to these Application Examples at any time without prior notice. If there are any deviations between the recommendations provided in this application example and other Siemens publications – e.g. Catalogs – the contents of the other documents have priority.

We accept no liability for information contained in this document.

Any claims against us – based on whatever legal reason – resulting from the use of the examples, information, programs, engineering and performance data etc., described in this Application Example shall be excluded. Such an exclusion shall not apply in the case of mandatory liability, e.g. under the German Product Liability Act (“Produkthaftungsgesetz”), in case of intent, gross negligence, or injury of life, body or health, guarantee for the quality of a product, fraudulent concealment of a deficiency or breach of a condition which goes to the root of the contract (“wesentliche Vertragspflichten”). However, claims arising from a breach of a condition which goes to the root of the contract shall be limited to the foreseeable damage which is intrinsic to the contract, unless caused by intent or gross negligence or based on mandatory liability for injury of life, body or health. The above provisions do not imply a change in the burden of proof to your detriment.

Table of Contents

1 Introduction

1.1 Introduction

Overview

This document gives an overview of the different practicable configurations when using the major SIMATIC NET security products.

The use case associated with each scenario is described as well as the advantages and drawbacks of this constellation.

Restriction

This document is limited to the **secure VPN communication** via local networks or the Internet with DSL.

Only the **SCALANCE S modules** and the **Softnet Security Client** from the SIMATIC NET Security product range are used.

The chapter “Scenarios” lists only a selection of practicable constellations; it does not claim to be complete.

A **complete** overview of the topic “Security with SIMATIC NET” is given in the document 27043887_Security_SIMATIC_NET.pdf located on the same html page as this document.

http://support.automation.siemens.com/WW/view/en/27043887

1.2 Communication via VPN

Communication in all scenarios takes place between one or more control center(s) and one or more manufacturing cells. The data are transmitted in encrypted form over one or more VPN tunnel(s).

Required components

Such a tunnel can be set up using either a **software-based** (**Softnet Security Client**) or a **hardware-based** (**SCALANCE S61x**) solution.

Table 1-1

Component	MLFB
Security Module S612	6GK5612-0BA00-2AA3
Security Module S613	6GK5613-0BA00-2AA3
Softnet Security Client	6GK1704-1VW01-0AA0

Process sequence

A configuration tool is used to configure the SIMATIC NET **Softnet Security Client** software and the **SCALANCE S61x module** so that each constitutes an end point of a joint VPN (Virtual Private Network) tunnel.

The security component(s) in the control center are the active nodes, i.e. they initiate that the tunnel to the other security modules on the plant side is established. This has the advantage that the current IP address of the Internet access does not have to be known **(dynamic IP address)**.

The automation network comprises a SCALANCE S612 or SCALANCE S613 which protects and terminates the IPSec tunnel. These modules are connected to the Internet. In contrast to the control center, the access point here must have a static official address, i.e. an IP address routed in the Internet (**fixed IP address**). This IP address enables the active partner in the control center to find the terminal device on the Internet.

Note

The Softnet Security Client can only be configured as active node, i.e. it initiates that the tunnel is established.

Since in this document the tunnel is established by the control center alone, the Softnet Security Client can not be used in the remote station.

Number of VPN tunnels

The Softnet Security Client can manage only one certificate for one VPN tunnel connection, i.e. the number of VPN tunnels is limited to one.

Nevertheless, it is possible to reach several end stations, provided all stations have been configured for the same VPN tunnel.

The Security Configuration Tool solves this problem with the help of the VPN group. All modules belonging to the same VPN group communicate via the same VPN tunnel and can exchange data with each other.

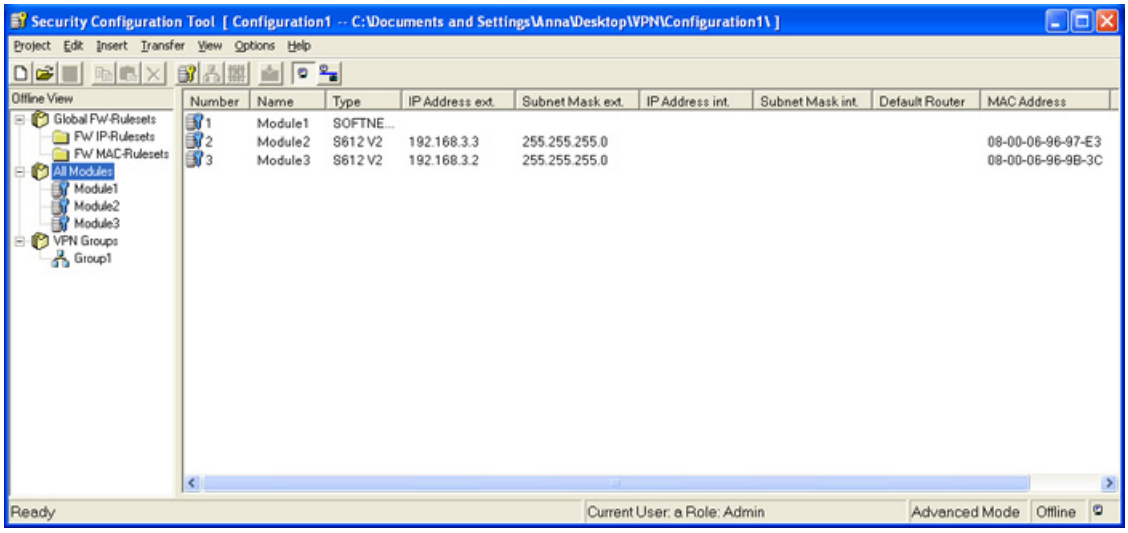
1.3 The Security Configuration Tool

Description

The Security Configuration Tool (SCT) is used to configure the SCALANCE S modules and to create the configuration files for the Softnet Security Client. All stations can be combined to groups. These assignments also define the modules that can communicate via a VPN tunnel.

The figure below shows a screenshot of the configuration tool:

Figure 1-1



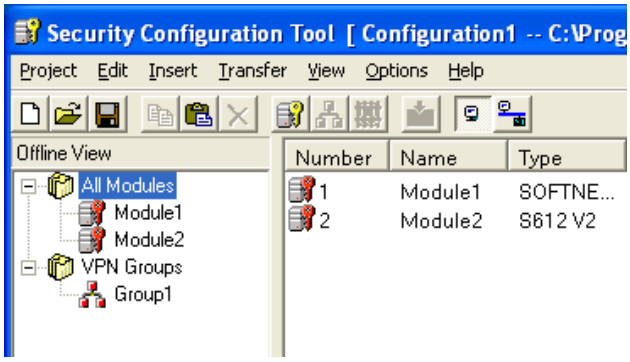
Rules for group definition

If several modules shall be combined to a VPN group in the Security Configuration Tool, the following rules with regard to the different modes are to be observed:

The first module assigned to the VPN group defines what types of further modules can be added.

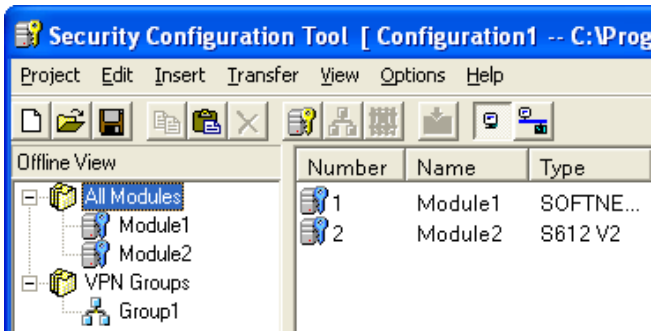
- If the first module is in routing mode, all other modules must also be operated in routing mode. The key behind the module is red.

Figure 1-2



- If the first module is operated in bridge mode, the routing mode function of all further modules assigned to this group must be deactivated. The key behind the module is blue.

Figure 1-3



Note

For the Softnet Security Client, no operating mode can be specified. It is always operated in bridge mode.

Example: If you want to specify a VPN group including a Softnet Security Client and a SCALANCE S612 in routing mode, you must draw the **S612** into the VPN group **first** and then the **Softnet Security Client**. The key behind the modules is red.

Otherwise the Softnet Security Client would define the operating mode of the VPN group – in this case the bridge mode (blue key) – and the S612 could not be assigned to this group.

2 Scenarios

2.1 General requirements for the scenarios

All scenarios must fulfill certain requirements which are listed in this section.

Note In this document the tunnel is always established from the control center. But the active components can also be configured in the remote station. All settings for the router etc. will then apply to the control center and vice versa.

Requirements for the DSL gateways

Table 2-1

Control Center	Remote Station
If the network load is high, a separated DSL connection is recommended for each security module.	Port forwarding must be activated in the router (UDP 500, 4500 on the same port as the subsequent module).
Unless the ports in the router of the control center are open without restrictions from inside to outside (proxy, firewall), port forwarding is necessary (UDP 500, 4500) here, too.	A separate DSL connection must be available for each SCALANCE S module.
	All DSL connections must have a static IP address.
	The router must have the following properties: • VPN pass-through • No VPN client • No modem

General requirements

In order for the communication via VPN to proceed smoothly, the following additional requirements must be met:

- No other VPN client is allowed to run on the computer besides the Softnet Security Client.
- If the Softnet Security Client is running on the PC, any firewall installed on the computer should be disabled or the corresponding ports should be open.

2.2 Introducing the displayed scenarios

In the following chapters, the different scenarios are illustrated. Each scenario is briefly described, the respective Use Case is displayed and the advantages or disadvantages of the solution are listed, finished by an overview image of the introduced constellation.

In detail these are the following scenarios:

- One remote station and one control center
  - One SCALANCE S ←→ One Softnet Security Client
  - One SCALANCE S ←→ One SCALANCE S
  - One SCALANCE S ←→ Several Softnet Security Clients
- One remote station and several branch control centers
  - One SCALANCE S ←→ One Softnet Security Client
  - One SCALANCE S ←→ One SCALANCE S
  - One SCALANCE S ←→ Several Softnet Security Clients
  - One SCALANCE S ←→ Several SCALANCE S
- Several plant cells and one control center
  - Several SCALANCE S ←→ One Softnet Security Client
  - Several SCALANCE S ←→ One SCALANCE S
  - Several SCALANCE S ←→ Several Softnet Security Clients
  - Several SCALANCE S ←→ Several SCALANCE S
- Several plant cells and several central stations
  - Several SCALANCE S ←→ One Softnet Security Client
  - Several SCALANCE S ←→ One SCALANCE S
  - Several SCALANCE S ←→ Several Softnet Security Clients
  - Several SCALANCE S ←→ Several SCALANCE S

3 One Remote Station and one Control Center

3.1 One SCALANCE S ←→ One Softnet Security Client

Description

The Softnet Security Client (SSC) in the control center establishes a VPN tunnel to a **SCALANCE S61x** in the remote station.

Configuration notes

For this scenario **one** VPN group is required in the Security Configuration Tool. Nodes are the Softnet Security Client and the SCALANCE S61x.

Use Case

This scenario shows an easy and secure remote access to a plant.

This configuration is optimally suited for a service technician who connects to a production network from a remote location in order to obtain access to the stations (e.g. S7 etc.) connected in the network.

On the technician's PC, the Softnet Security Client runs as the active node, i.e. it initiates that the tunnel to the SCALANCE S module on the plant side is established.

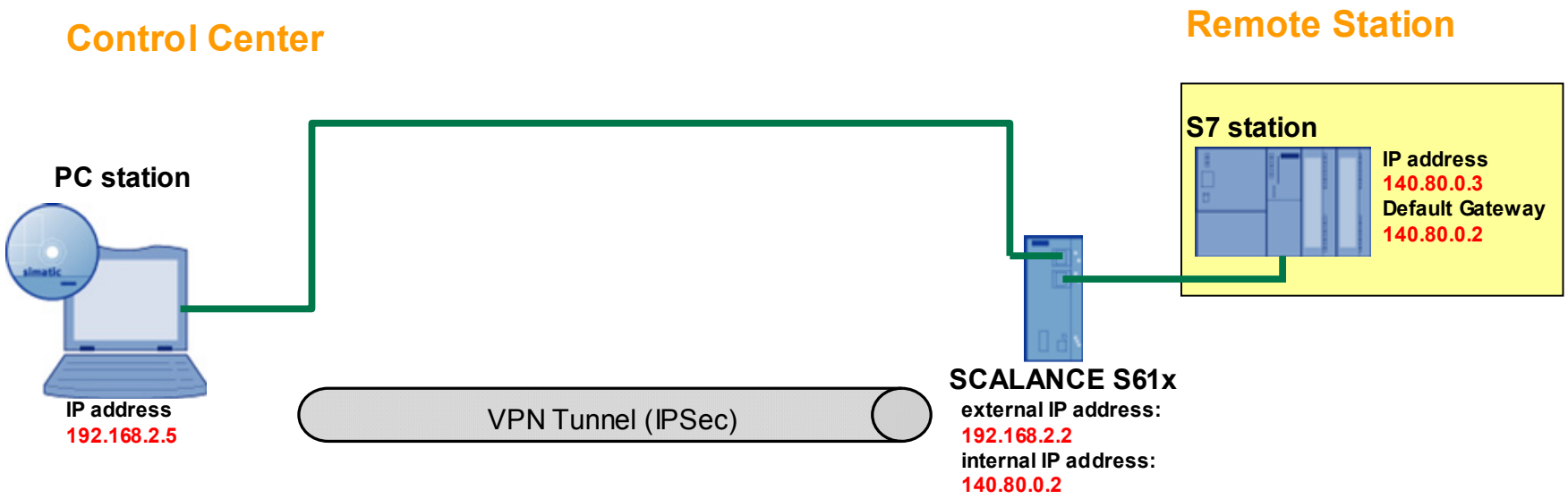
Advantages and disadvantages

Table 3-1

Advantage	Disadvantage
The control center is not bound to a location.	SSC can only manage one VPN tunnel.
Software-based VPN end point	VPN software runs directly on one PC. Only this PC has access to the remote station.
The router in the control center only needs a dynamic IP address.	

Configuration

Figure 3-1



3.2 One SCALANCE S ←→ One SCALANCE S

Description

The **SCALANCE S61x (SEM)** in the control center opens a VPN tunnel to the **SCALANCE S61x** in the remote station.

Configuration notes

For this scenario **one** VPN group is required in the Security Configuration Tool. Nodes are the two SCALANCE S61x.

Use Case

This scenario shows an easy and secure remote access to a plant.

This configuration is optimally suited for several service technicians who connect to a production network from a remote location in order to obtain access to the stations (e.g. S7 etc.) connected in the network.

The SCALANCE S module in the control center initiates a VPN tunnel to the remote station. An internal network is located behind the SCALANCE in the control center. All PCs connected to the SCALANCE can exchange data with the remote station via the VPN tunnel.

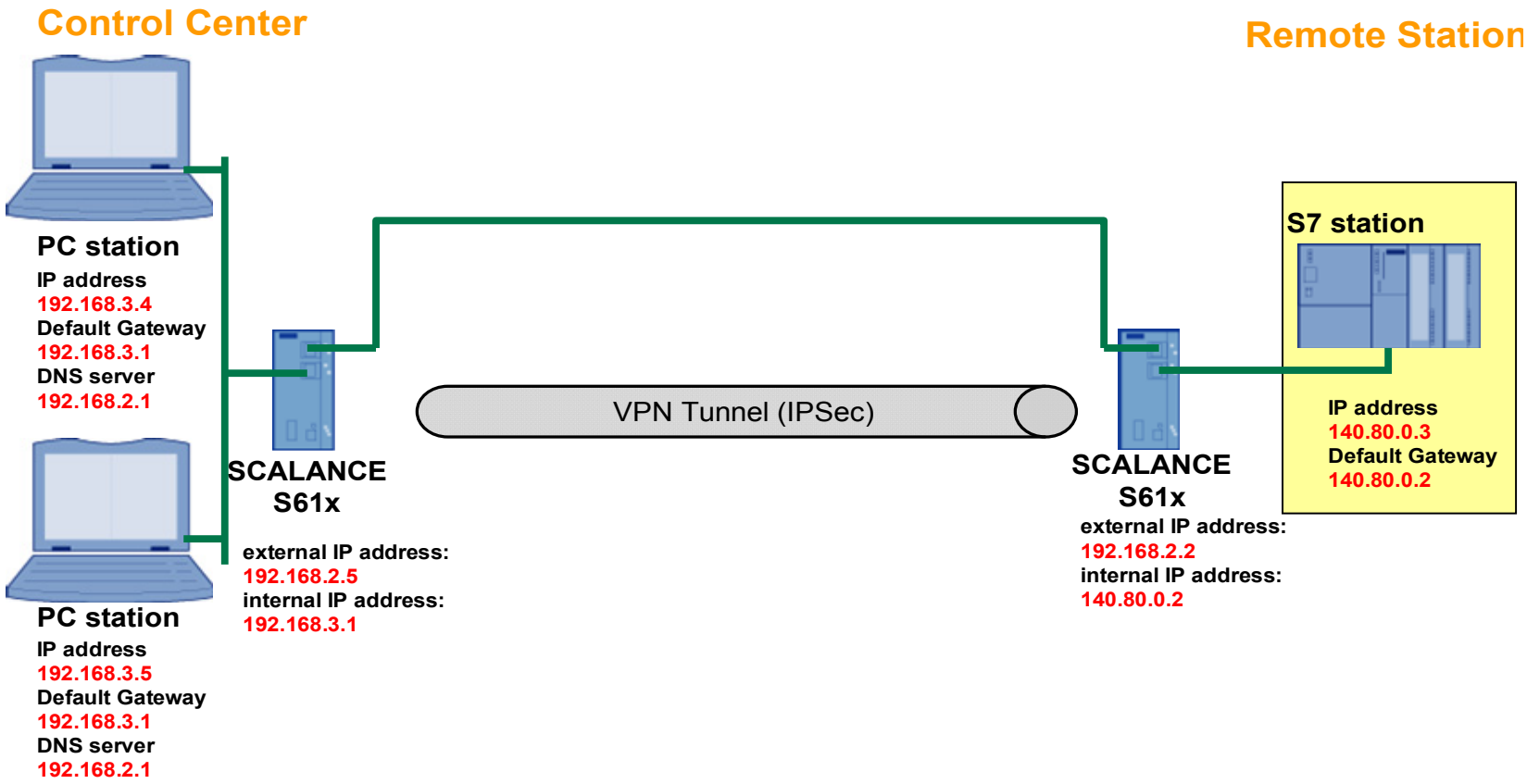
Advantages and disadvantages

Table 3-2

Advantage	Disadvantage
Several nodes (PCs) can send data through the VPN tunnel.	The software solution ties the service mechanics to a certain location.

Configuration

Figure 3-2



3.3 One SCALANCE S ←→ Several Softnet Security Clients

Description

There are **several Softnet Securit Clients** installed in the control center. **One SCALANCE S** is located in the remote station. Each Softnet Security Client establishes a separate VPN tunnel to the remote station.

Configuration notes

For this scenario **several** VPN groups are required in the Security Configuration Tool. Nodes of the group are **one** Softnet Security Client each and the SCALANCE S61x of the remote station.

Use Case

This solution is optimally suited for several service technicians who connect to a production network simultaneously from a remote location to access the different machines etc. connected in the network.

On each technician's PC, the Softnet Security Client runs as the active node, i.e. it initiates its own tunnel to the SCALANCE S module on the plant side.

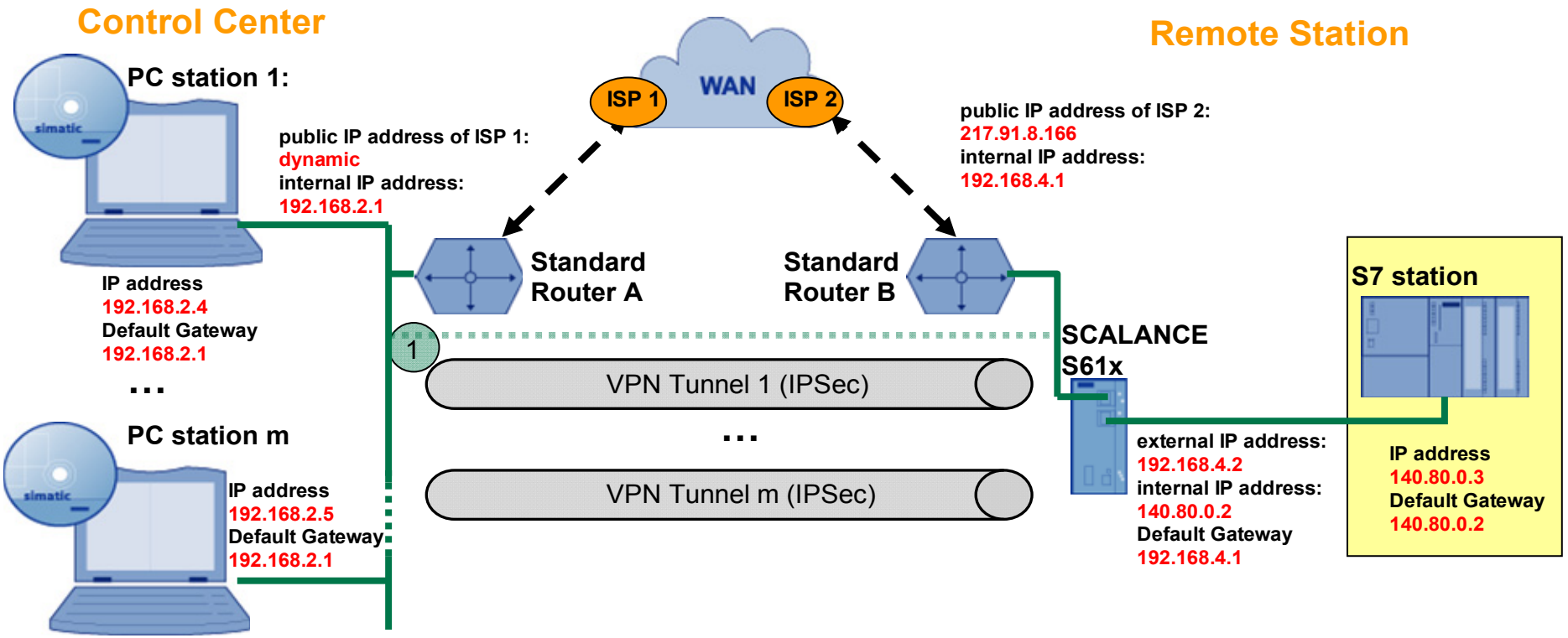
Advantages and disadvantages

Table 3-3

Advantage	Disadvantage
The control center is not bound to a location.	SSC can only manage one VPN tunnel.
Software-based VPN end point	Each PC needs a separate software.
The PCs in the control center are independent of each other since each is a separate VPN end point.	
Different machines can be serviced by several technicians at the same time.	
The router in the control center only needs a dynamic IP address.	

Configuration

Figure 3-3



1 The connection between control center and remote station can also be made via an internal LAN

4 One Remote Station and several Branch Control Centers

4.1 One SCALANCE S ←→ One Softnet Security Client

Description

There are **several control centers** with **one Softnet Security Client** each. **One SCALANCE S** is located in the remote station. Each Softnet Security Client establishes a separate VPN tunnel to the remote station.

Configuration notes

For this scenario **several** VPN groups are required in the Security Configuration Tool. Nodes of the group are the Softnet Security Client of **one** control center and the SCALANCE S61x of the remote station.

Use Case

A production network is monitored and serviced in several locations. A programmer, technician or mechanic in each branch control center can connect to the remote station from his PC by opening a VPN tunnel and remote service it.

On each technician's PC, the Softnet Security Client runs as the active node, i.e. it initiates the tunnel to the SCALANCE S module on the plant side to be established.

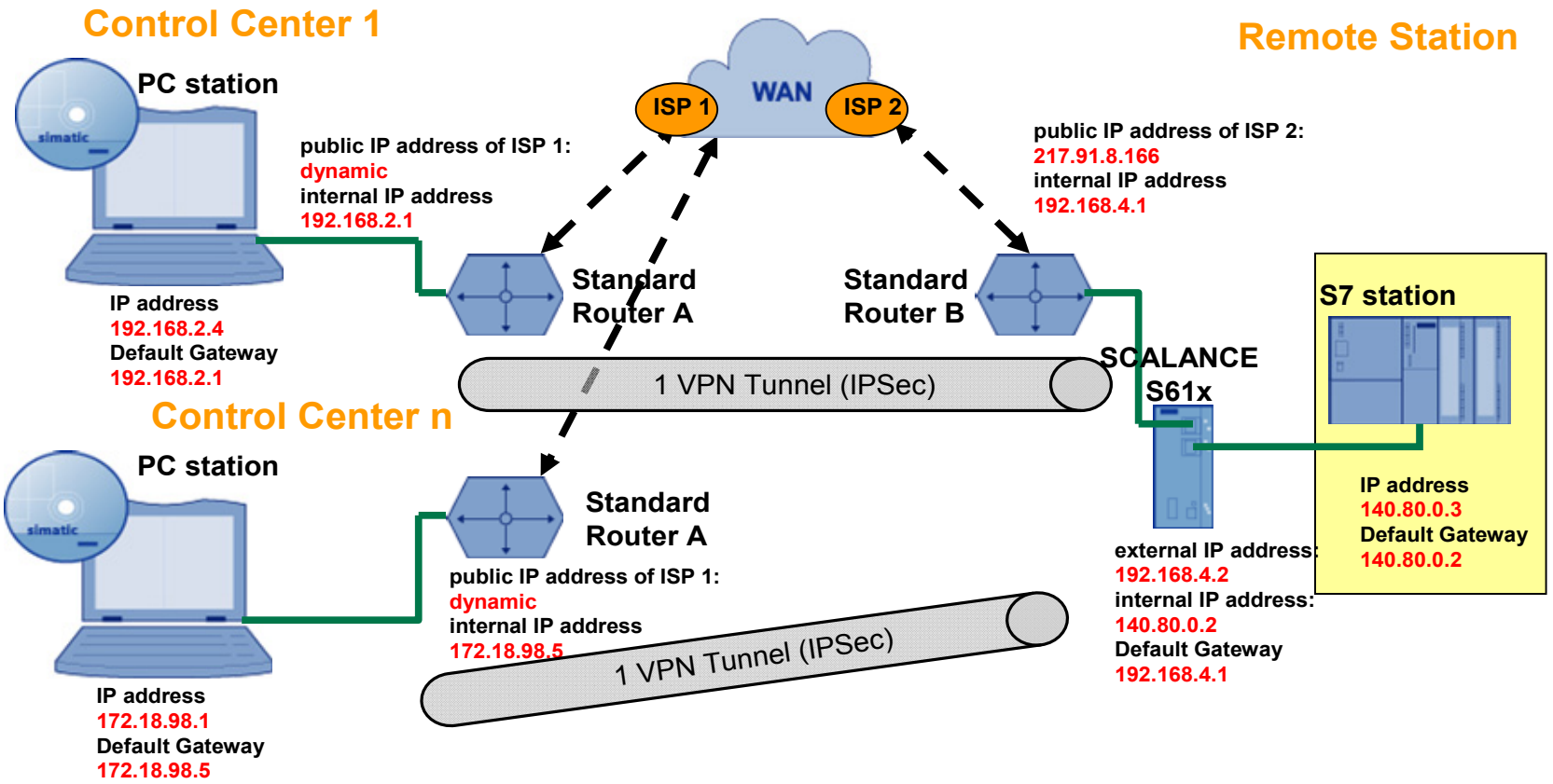
Advantages and disadvantages

Table 4-1

Advantage	Disadvantage
Branch control centers are not tied to one place.	SSC can only manage one VPN tunnel.
Software-based VPN end point	Each PC needs a separate software.
Branch control centers are independent of each other since each is an autonomous VPN end point.	Only one VPN tunnel is possible in each subordinate central station.
Different machines can be maintained by several technicians from different locations at the same time.	Only one PC per subordinate central station can have remote access to the plant.
Total of up to 128 VPN connections to remote station possible.	
Each branch control center can have its own subnet.	
The routers in the branch control center only needs a dynamic IP address.	

Configuration

Figure 4-1



4.2 One SCALANCE S ←→ One SCALANCE S

Description

There are **several control centers** with **one SCALANCE S61x module** each. **One SCALANCE S** is located in the remote station. Each branch control center establishes one ore more VPN tunnels to the remote station via the VPN client.

Configuration notes

For this scenario **several** VPN groups are required in the Security Configuration Tool. Nodes of the group are the SCALANCE S61x of **one** control center and the remote station.

Use Case

A production network is monitored and serviced in several locations. Each branch control center accommodates several programmers, technicians or mechanics who can remote service the remote station simultaneously from their PC via the VPN tunnel.

The SCALANCE S module initiates a VPN tunnel to the remote station. An internal network is located behind the SCALANCE in the control center. All PCs connected to the SCALANCE can exchange data with the remote station via the VPN tunnel.

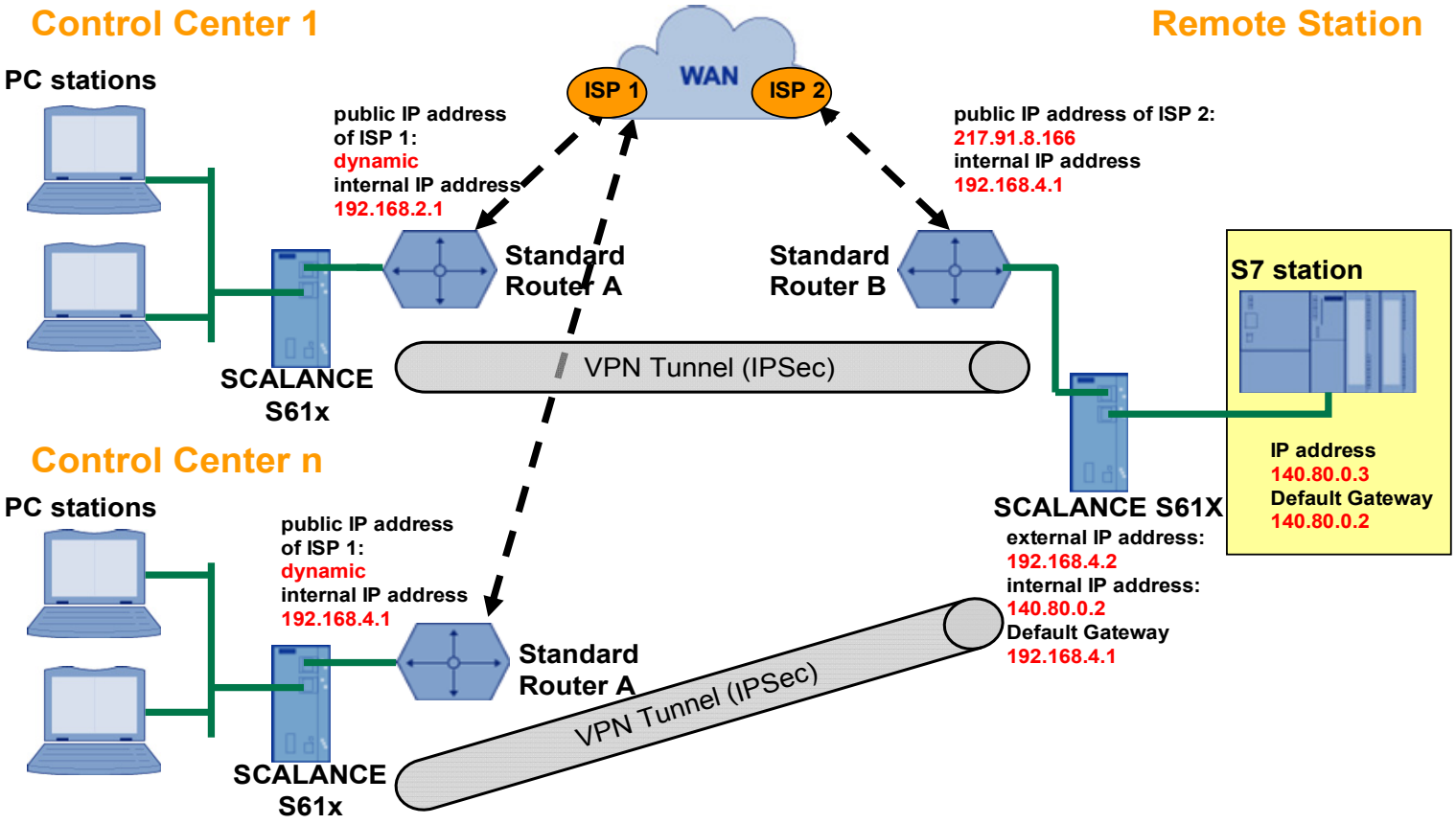
Advantages and disadvantages

Table 4-2

Advantage	Disadvantage
Several nodes (PCs) can send data through the VPN tunnel.	The software solution ties the service mechanics to a certain location.
Total of up to 128 VPN connections to remote station possible.	If there are many branch control centers, the data rate performance to the remote station can decrease.
Each branch control center can have its own subnet.	
Different machines can be serviced by several technicians simultaneously from one and from different locations.	

Configuration

Figure 4-2



4.3 One SCALANCE S ←→ Several Softnet Security Clients

Description

There are **several control centers** with several **Softnet Security Clients** each. **One SCALANCE S** is located in the remote station. Each Softnet Security Client establishes a separate VPN tunnel to the remote station.

Configuration notes

For this scenario **several** VPN groups are required in the Security Configuration Tool. Nodes of the group are **one** Softnet Security Client each of **one** control center and the SCALANCE S61x of the remote station.

Use Case

A production network is monitored and serviced in several locations. Several programmers, technicians or mechanics in each branch control center can connect to the remote station from their PC by establishing a VPN tunnel and remote service it.

On each technician's PC, the Softnet Security Client runs as the active node, i.e. it initiates the tunnel to the SCALANCE S module on the plant side to be established.

Advantages and disadvantages

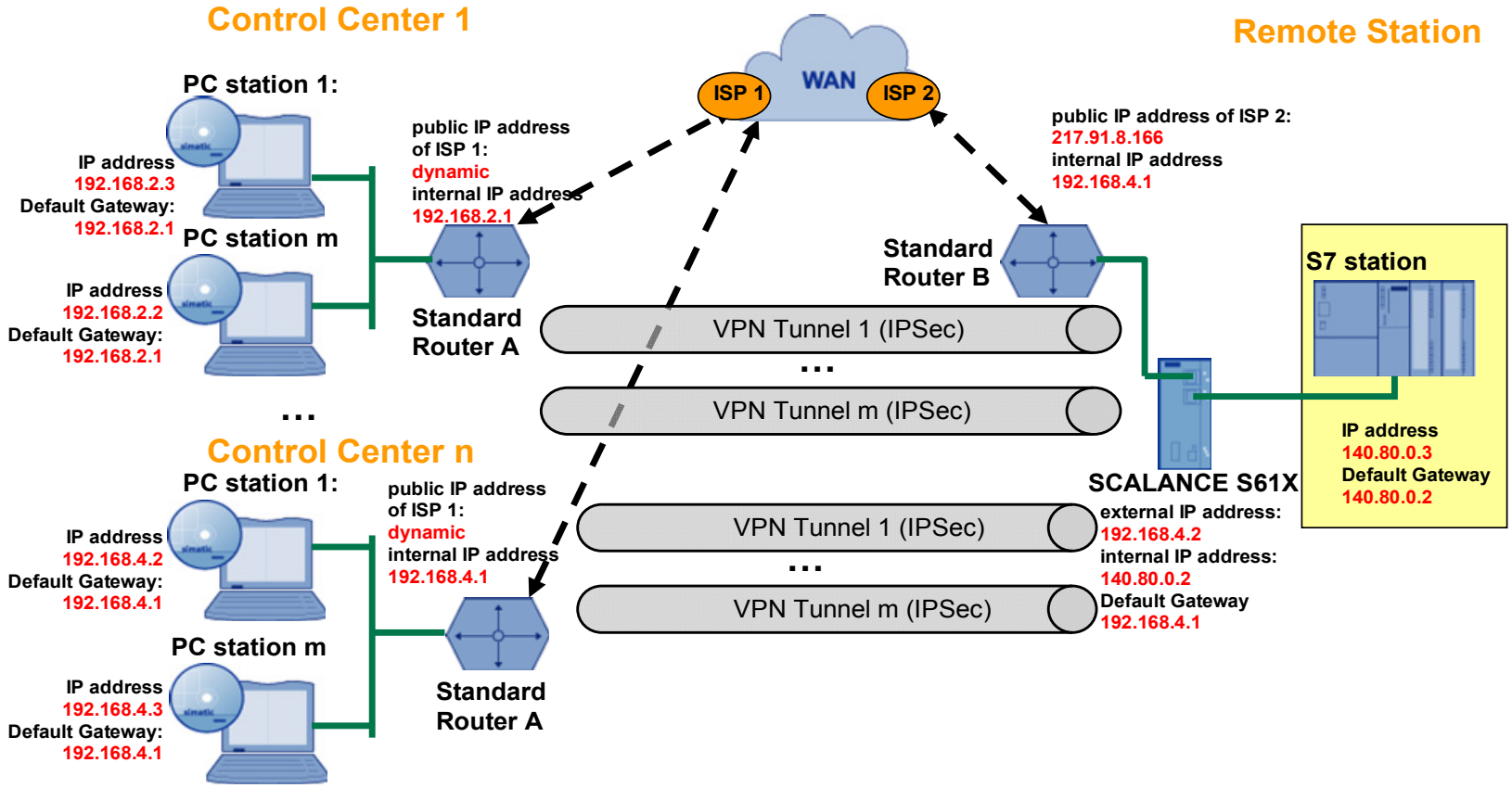
Table 4-3

Advantage	Disadvantage
Branch control centers are not tied to one place.	SSC can only manage one VPN tunnel.
Software-based VPN end point	Each PC needs a separate software.
Branch control centers are independent of each other since each is an autonomous VPN end point.	Only one PC can send data through its own VPN tunnel.
Different machines can be serviced by several technicians simultaneously from different locations.	
Total of up to 128 VPN connections to remote station possible.	

Security27043887

Configuration

Figure 4-3



4.4 One SCALANCE S ←→ Several SCALANCE S

Description

There are **several control centers** with several **SCALANCE S61x modules** each. **One SCALANCE S** is located in the remote station. Each branch control center establishes one ore more VPN tunnels to the remote station via its VPN clients.

Configuration notes

For this scenario there are two configuration options in the Security Configuration Tool:

- **All** SCALANCE S16x of a control center and the SCALANCE S61x of the remote station are nodes of a VPN group.
- **One** SCALANCE S16x **each** of a control center and the SCALANCE S61x of the remote station are nodes of a VPN group.

Use Case

A production network is monitored and serviced in several locations. Each branch control center accommodates several programmers, technicians or mechanics who can remote service the remote station simultaneously from their PC by establishing a VPN tunnel.

The SCALANCE S modules initiate a VPN tunnel to the remote station. An autonomous network is located behind each SCALANCE in the branch control center. All PCs behind it can exchange data with the remote station via the VPN tunnel.

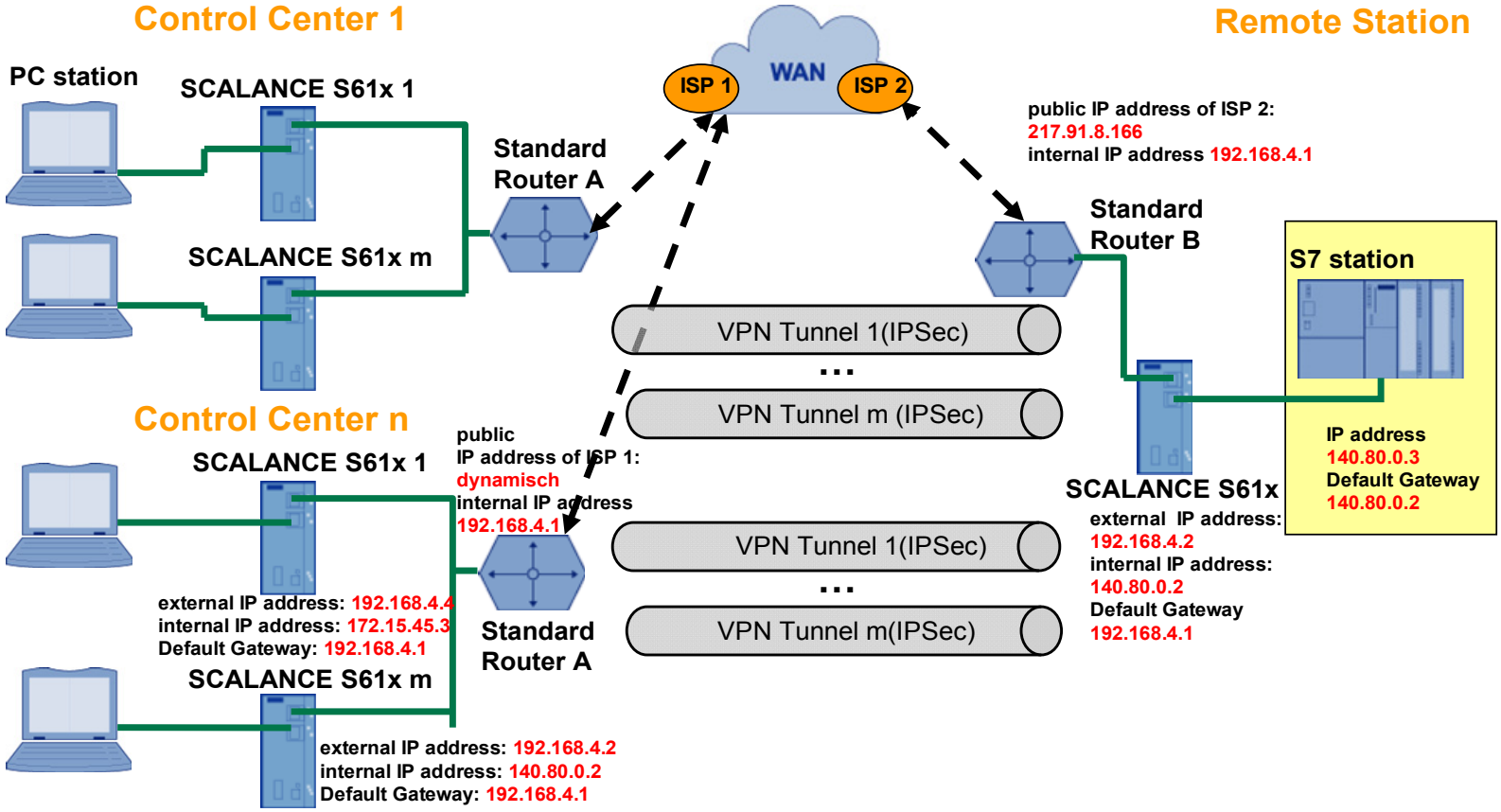
Advantages and disadvantages

Table 4-4

Advantage	Disadvantage
Several nodes (PCs) can send data through the VPN tunnel.	The software solution ties the service mechanics to a certain location.
Total of up to 128 VPN connections to remote station possible.	If there are many branch control centers, the data rate performance to the remote station can decrease.
There can be a different subnet behind each SCALANCE.	

Configuration

Figure 4-4



5 Several Plant Cells and one Control Center

5.1 Several SCALANCE S ←→ One Softnet Security Client

Description

There is **one Softnet Security Client** in the control center and **several SCALANCE S** modules in the remote station. The Softnet Security Client establishes a VPN tunnel to one or several of the SCALANCE S61x modules in a plant cell.

Configuration notes

For this scenario there are two configuration options in the Security Configuration Tool:

- The Softnet Security Client and **one** SCALANCE S61x of a plant cell are nodes of **one** VPN group.
- The Softnet Security Client and **several** SCALANCE S61x of different plant cells are nodes of **one** VPN group.

Use Case

A plant network is divided into different cells. Each cell has its own SCALANCE S and thus a different internal subnet.

These secured cells are monitored and serviced by a programmer, technician etc. in one location.

On the technician's PC in the control center, the Softnet Security Client runs as active node, i.e. it initiates that the tunnel to a secured cell is established. This VPN tunnel gives access to the stations (e.g. S7, etc.) connected in the network.

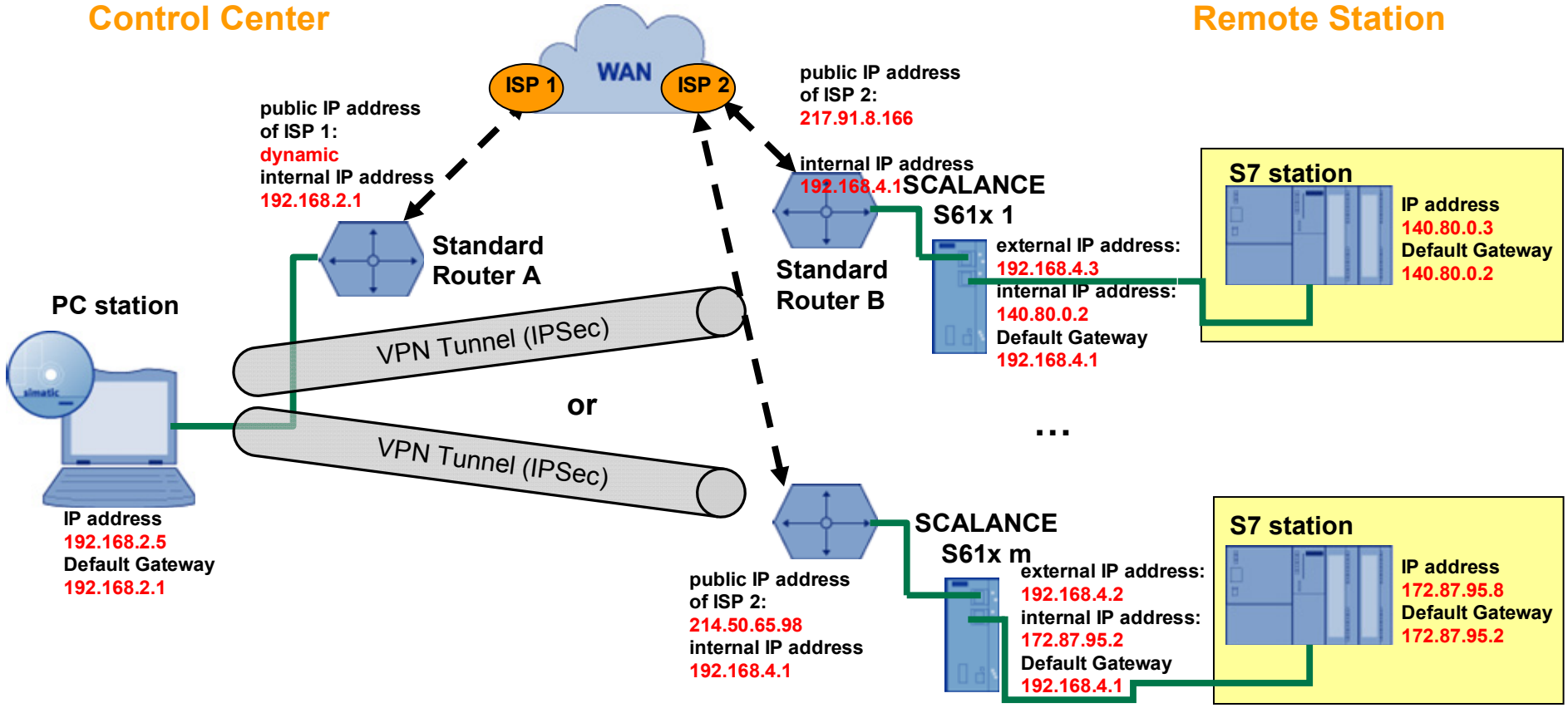
Advantages and disadvantages

Table 5-1

Advantage	Disadvantage
The control center is not bound to a location.	SSC can only manage one joint VPN tunnel.
Each cell in the remote station can be located in a different subnet.	It is not possible to establish several different VPN tunnels to several cells simultaneously.
	Only one PC can send data through the VPN tunnel.

Configuration

Figure 5-1



5.2 Several SCALANCE S ←→ One SCALANCE S

Description

There is **one SCALANCE S** in the control center and **several SCALANCE S** modules in the remote station. The control center establishes one or more VPN tunnels to the remote station.

Configuration notes

For this scenario there are two configuration options in the Security Configuration Tool:

- The SCALANCE S61x of the control center and **one** SCALANCE S61x of the remote station are nodes of **one** VPN group.
- The SCALANCE S61x of the control center and **several** SCALANCE S61x of the remote station are nodes of **one** VPN group.

Use Case

A plant network is divided into different cells. Each cell has its own SCALANCE S and thus a different internal subnet.

These secured cells are monitored and serviced by several programmers, technicians etc. in one location.

In the control center, one SCALANCE S module initiates that a tunnel to the manufacturing cells is established. All PCs located behind the SCALANCE in the control center have simultaneous access to all plant units.

Advantages and disadvantages

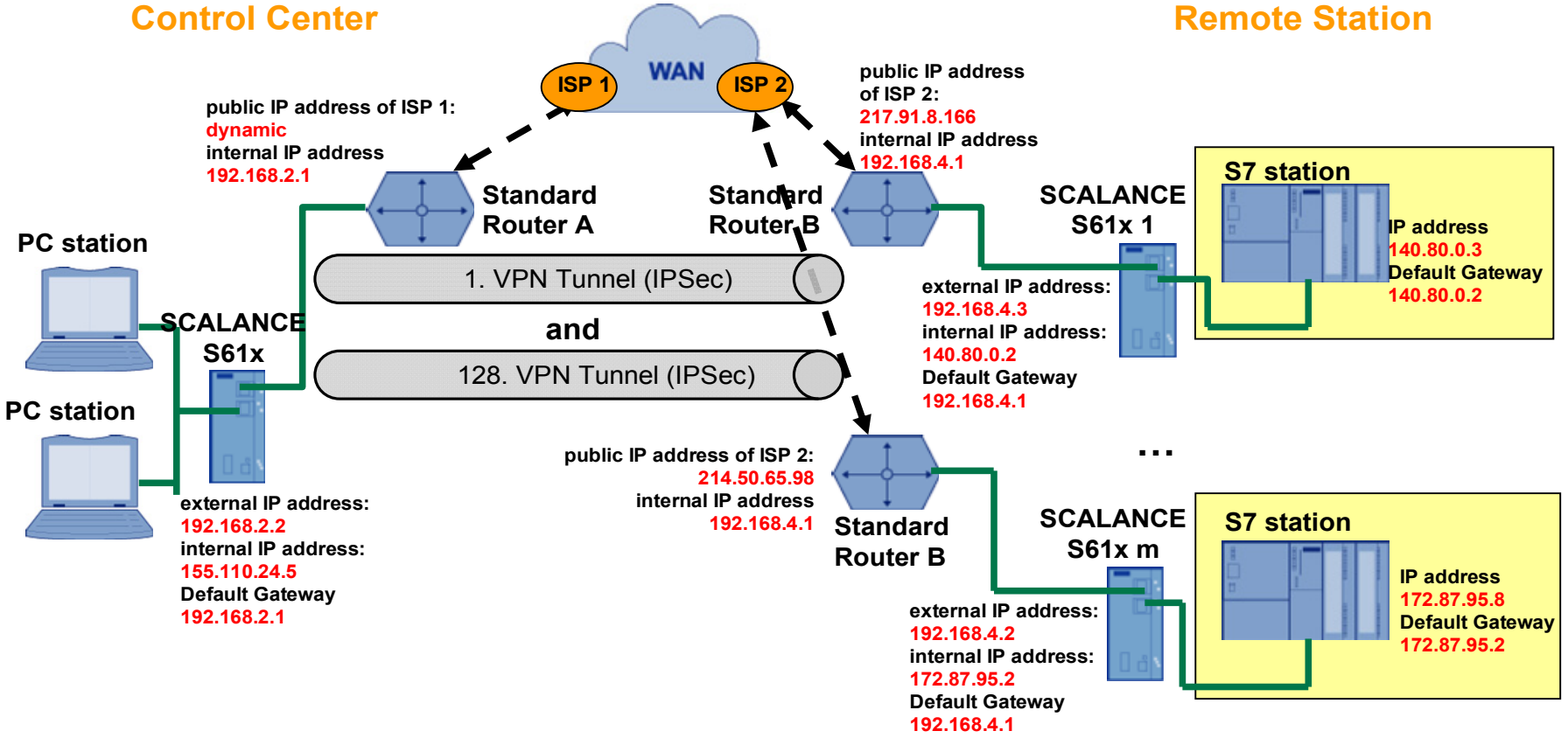
Table 5-2

Advantage	Disadvantage
Several nodes (PCs) can send data through the VPN tunnel.	The software solution ties the service mechanics to a certain location.
Each SCALANCE can manage up to 128 VPN connections simultaneously.	If there are many cells, the data rate performance to the control center can decrease.
Each cell can have a different subnet.	All PCs behind the SCALANCE in the control center have access to the cells connected by the VPN tunnel.
SCALANCE in the control center can establish a VPN tunnel to several cells simultaneously.	
Several secured cells can be remote serviced from one PC.	

Security27043887

Configuration

Figure 5-2



5.3 Several SCALANCE S ←→ Several Softnet Security Clients

Description

There are **several Softnet Security Clients** in the control center and **several SCALANCE S modules** in the remote station. Each Softnet Security Client establishes its own VPN tunnel to one or several of the SCALANCE S61x of a cell.

Configuration notes

For this scenario there are two configuration options in the Security Configuration Tool:

- **One each** Softnet Security Client of the control center and **one each** SCALANCE S61x of a plant cell are nodes of **one** VPN group.
- **One each** Softnet Security Client of the control center and **several** SCALANCE S61x of different plant cells are nodes of **one** VPN group.

Use Case

A plant network is divided into different cells. Each cell has its own SCALANCE S and thus a different internal subnet.

These secured cells are monitored and serviced by several programmers, technicians etc. in one location.

On each of the technicians' PC in the control center, the Softnet Security Client runs as active node, i.e. it initiates that the tunnel to a secured cell is established. This connection gives access to all stations (e.g. S7) located in the network behind the SCALANCE S module.

Advantages and disadvantages

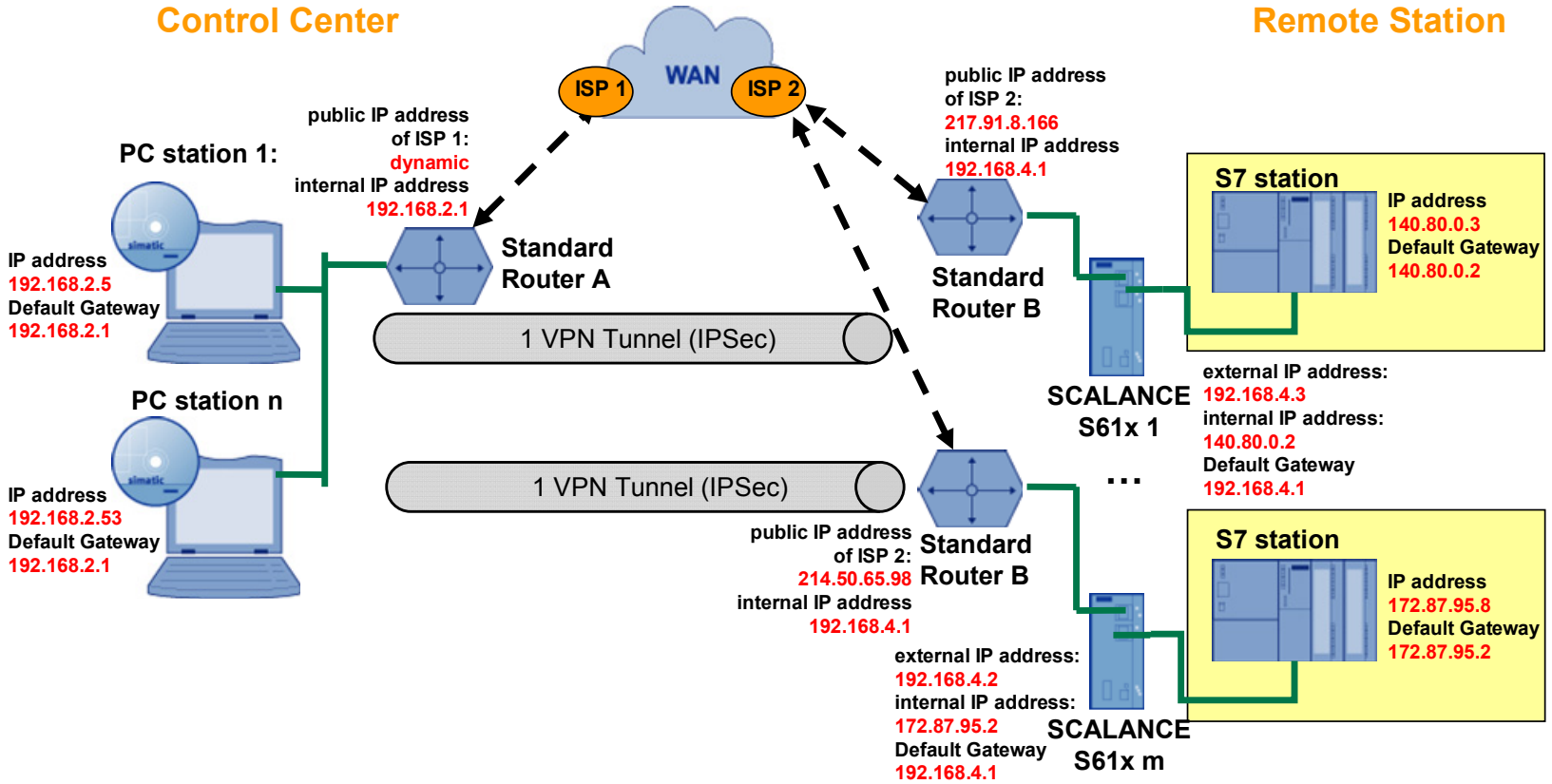
Table 5-3

Advantage	Disadvantage
The control center is not bound to a location.	SSC can only manage one joint VPN tunnel.
Each cell can have a different subnet.	Each PC needs a separate software.
Several secured cells can be remote serviced from several PCs.	
Depending on the competence of the service technicians, access can be given to a certain cell only.	

Security27043887

Configuration

Figure 5-3



5.4 Several SCALANCE S ←→ Several SCALANCE S

Description

There are **several SCALANCE S modules** in the control center and in the remote station. Each SCALANCE S in the control center can establish one ore more VPN tunnels simultaneously to the remote station.

Configuration notes

For this scenario there are two configuration options in the Security Configuration Tool:

- One SCALANCE S16x each of the control center and one SCALANCE S61x of a plant cell are nodes of **one** VPN group.
- One SCALANCE S16x each of the control center and **several** SCALANCE S61x of **different** plant cells are nodes of **one** VPN group.

Use Case

A plant network is divided into different cells. Each cell has its own SCALANCE S and thus a different internal subnet.

These secured cells are monitored and serviced by several programmers, technicians etc. in one location.

In the control center, the SCALANCE S modules initiate that a tunnel to one or more secured cells is established. All PCs located behind the SCALANCE in the control center have simultaneous access to these cells.

Advantages and disadvantages

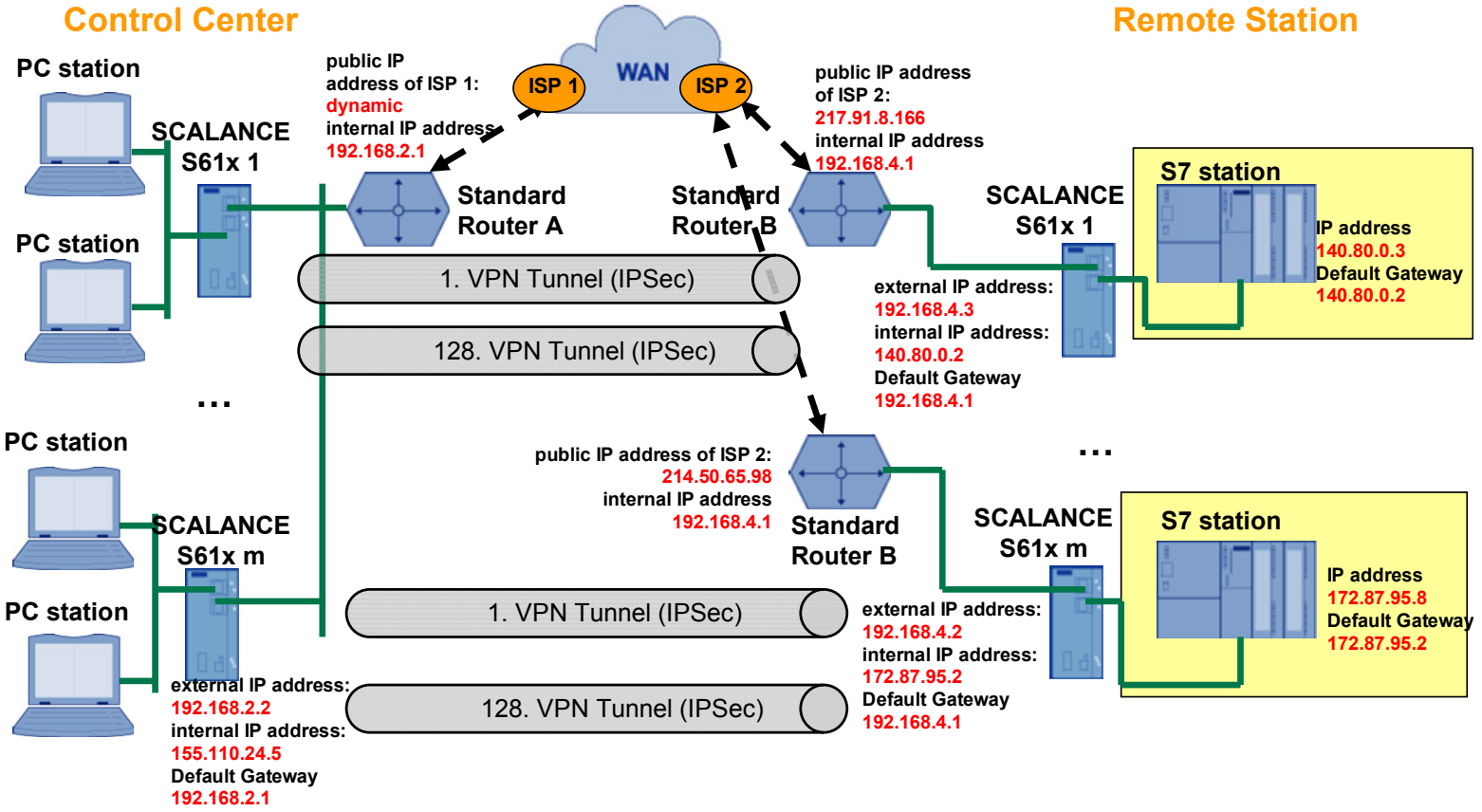
Table 5-4

Advantage	Disadvantage
Several nodes (PCs) can send data through the VPN tunnel.	The software solution ties the service mechanics to a certain location.
Total of up to 128 VPN connections to remote station are possible for each SCALANCE.	If there are many cells, the data rate performance to the control center can decrease.
Each cell can have a different subnet.	All PCs behind a SCALANCE in the central station have access to all cells connected by the VPN tunnel.
There can be a different subnet behind each SCALANCE in the central station.	
Several secured cells can be remote serviced from one PC.	

Security27043887

Configuration

Figure 5-4



6 Several Plant Cells and several Central Stations

6.1 Several SCALANCE S ←→ One Softnet Security Client

Description

There are **several control centers** with **one Softnet Security Client** each. There are **several SCALANCE S modules** in the remote station. Each VPN client of a branch control center establishes its own VPN tunnel to a SCALANCE S in a plant cell.

Configuration notes

For this scenario there are two configuration options in the Security Configuration Tool:

- The Softnet Security Client of **one** control center and the SCALANCE S61x of **one** plant cell are nodes of **one** VPN group.
- The Softnet Security Client of a control center and **several** SCALANCE S61x of **different** plant cell are nodes of **one** VPN group.

Use Case

A plant network is divided into different cells. Each cell has its own SCALANCE S and thus a different internal subnet.

These cells are monitored and serviced in several locations. A programmer, technician or mechanic in each branch control center can connect to a secured cell from his PC by opening a VPN tunnel.

On each technician's PC, the Softnet Security Client runs as the active node, i.e. it initiates that the tunnel to one SCALANCE S module on the plant side is established.

Advantages and disadvantages

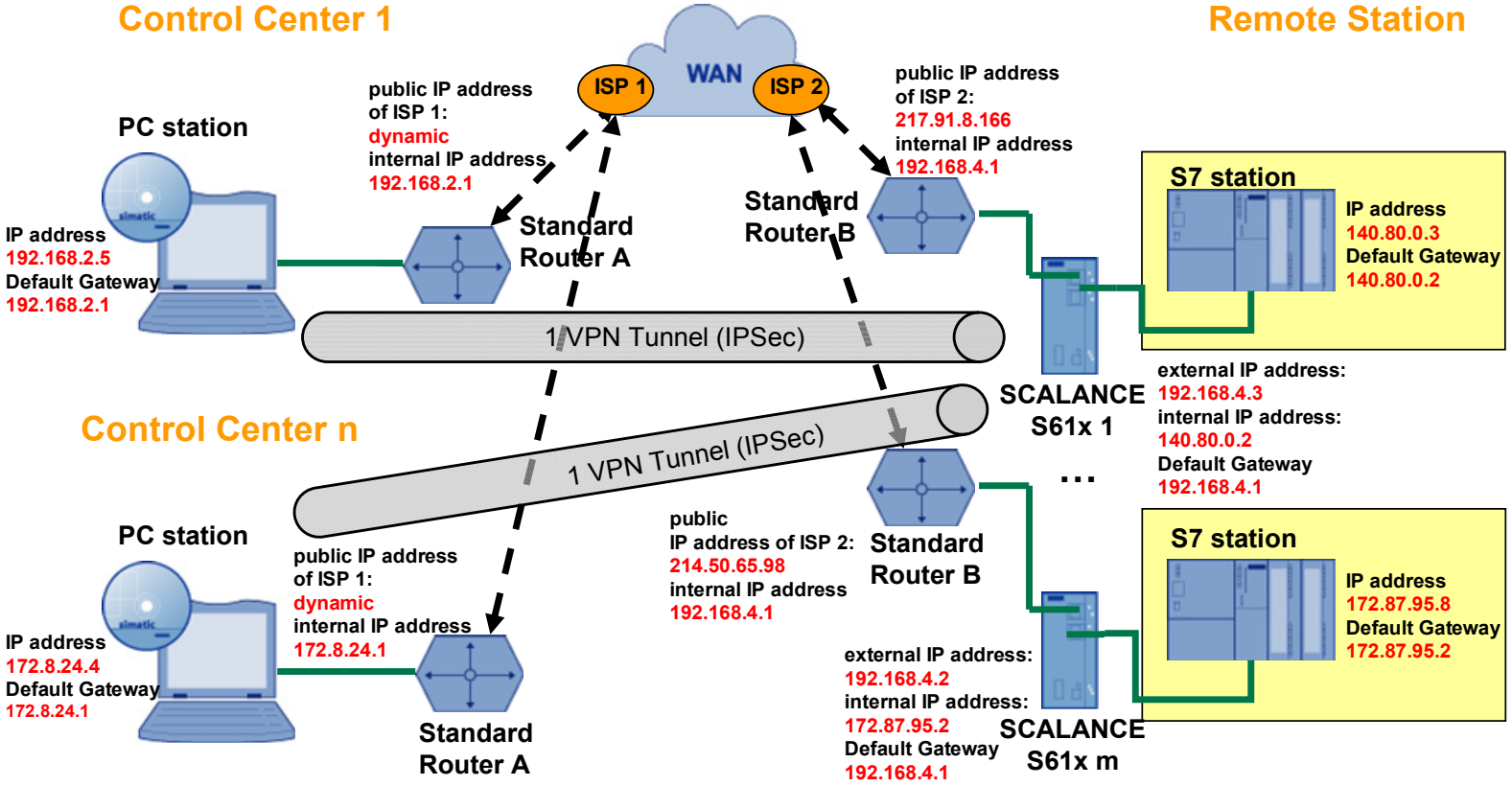
Table 6-1

Advantage	Disadvantage
The subordinate central station is not bound to a location.	SSC can only manage one VPN tunnel.
Each subordinate central station can be assigned to a certain secured cell and access is granted to this cell only.	One PC can not teleservice several secured cells simultaneously.
Each secured cell in the plant has a separate subnet.	Each PC needs a separate software.

Security27043887

Configuration

Figure 6-1



6.2 Several SCALANCE S ←→ One SCALANCE S

Description

There are **several control centers** with **one SCALANCE S** each. There are **several SCALANCE S modules** in the remote station. Each branch control center establishes one ore more VPN tunnels to the remote station.

Configuration notes

For this scenario there are two configuration options in the Security Configuration Tool:

- The SCALANCE S16x of **one** control center and **the** SCALANCE S61x of a plant cell are nodes of **one** VPN group.
- The SCALANCE S16x of **one** control center and **several** SCALANCE S61x of **different** plant cells are nodes of **one** VPN group.

Use Case

A plant network is divided into different cells. Each cell has its own SCALANCE S and thus a different internal subnet.

These secured cells are monitored and serviced by several programmers, technicians etc. in several locations.

In each branch control center, the SCALANCE S modules initiate that the tunnel to one or more plant cells is opened. All PCs located behind the SCALANCE in the control center have simultaneous access to all secured manufacturing cells.

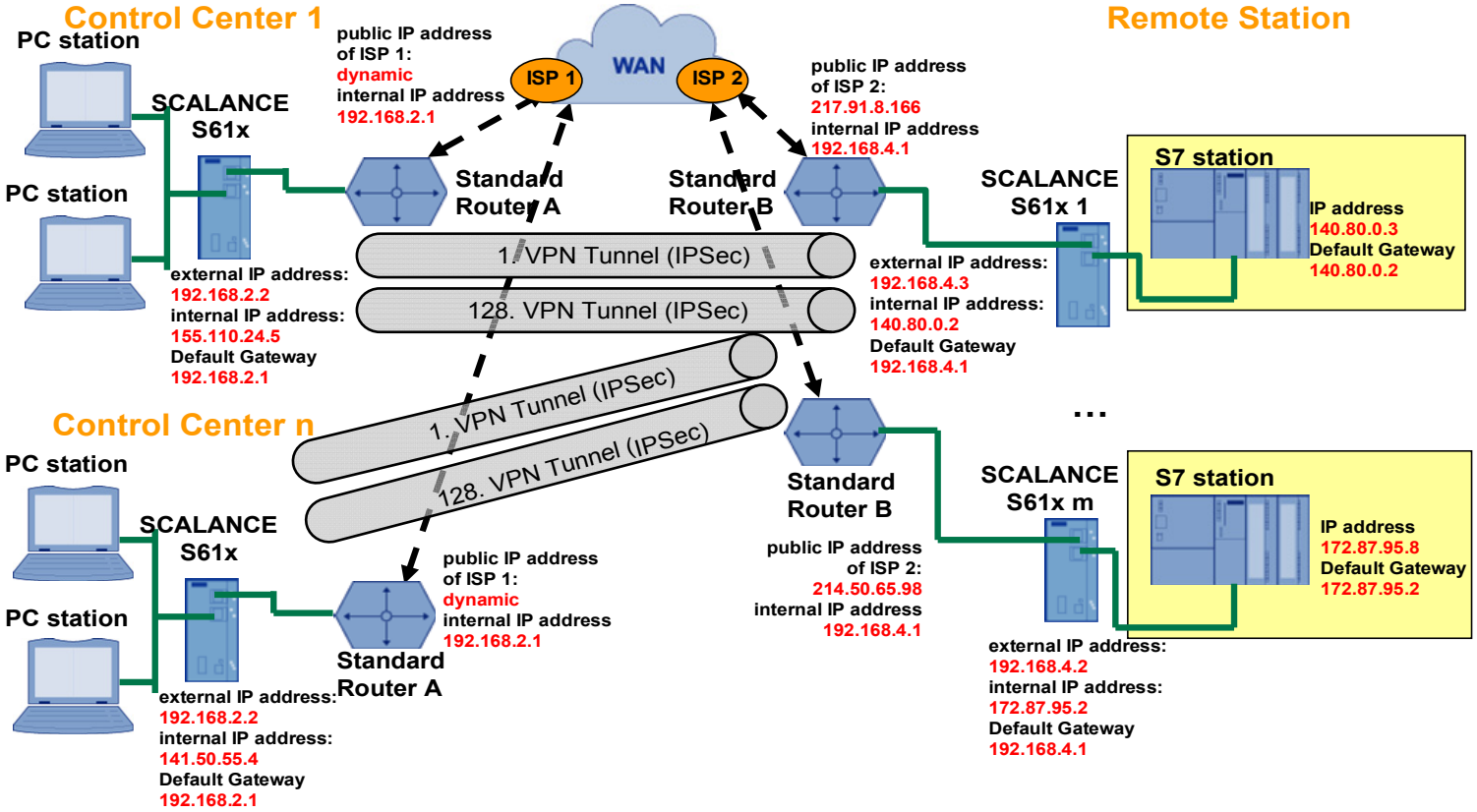
Advantages and disadvantages

Table 6-2

Advantage	Disadvantage
Several nodes (PCs) can send data through the VPN tunnel.	The software solution ties the service mechanics to a certain location.
Each SCALANCE of a cell can manage up to 128 VPN tunnels simultaneously.	If there are many cells, the data rate performance to the control center can decrease.
Each cell in the remote station can have a different subnet.	All PCs behind a SCALANCE in the subordinate central station have access to all cells connected by the VPN tunnel.
There can be a different subnet behind each SCALANCE in the subordinate central station.	
Several cells can be remote serviced from one PC.	

Configuration

Figure 6-2



6.3 Several SCALANCE S ←→ Several Softnet Security Clients

Description

There are **several control centers** with **several Softnet Security Clients**. There are **several SCALANCE S modules** in the remote station. All VPN clients in the branch control centers establish their own VPN tunnel to a SCALANCE S module in the plant cell.

Configuration notes

For this scenario there are two configuration options in the Security Configuration Tool:

- **One** Softnet Security Client **each** of one control center and the SCALANCE S61x of **one** plant cell are nodes of **one** VPN group.
- **One** Softnet Security Client **each** of a control center and **several** SCALANCE S61x of **different** plant cells are nodes of **one** VPN group.

Use Case

A plant network is divided into different cells. Each cell has its own SCALANCE S and thus a different internal subnet.

These secured cells are monitored and serviced in several locations. Programmers, technicians or mechanics in each branch control center can connect to a cell from their PCs by establishing a VPN tunnel.

On each technician's PC, the Softnet Security Client runs as the active node, i.e. it initiates that the tunnel to one SCALANCE S module on the plant side is established.

Advantages and disadvantages

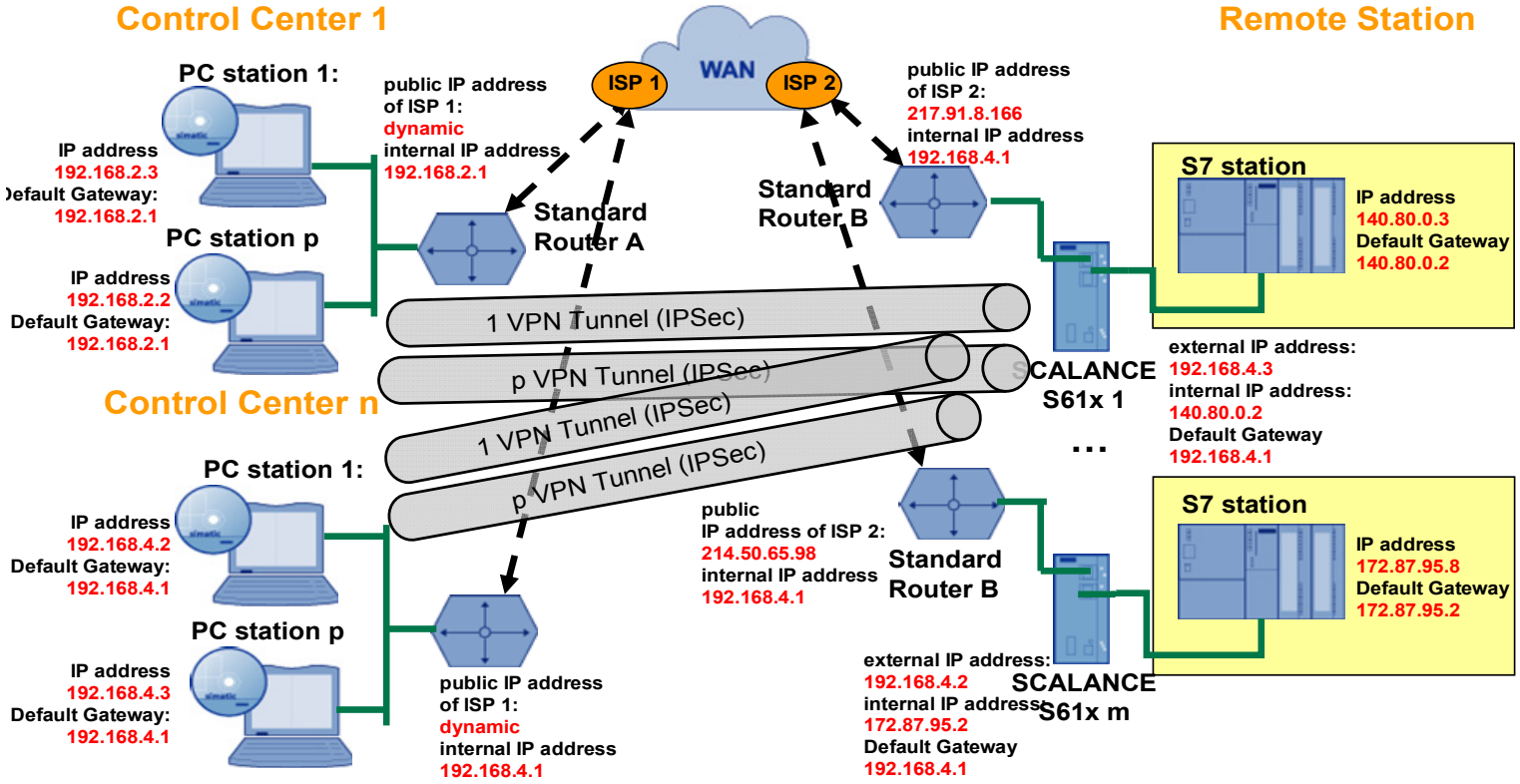
Table 6-3

Advantage	Disadvantage
Each PC can be assigned a certain secured cell and access is granted to this cell only.	One PC can not teleservice several secured cells simultaneously.
Each secured cell in the plant has a separate subnet.	Each PC needs a separate software.
Each SCALANCE of a cell can manage up to 128 VPN tunnels simultaneously.	
The subordinate central station is not bound to a location.	SSC can only manage one VPN tunnel.

Security27043887

Configuration

Figure 6-3



6.4 Several SCALANCE S ←→ Several SCALANCE S

Description

There are **several control centers** with **several SCALANCE S**. There are **several SCALANCE S modules** in the remote station. All VPN clients of the branch control centers establish one ore more VPN tunnels to the remote station.

Configuration notes

For this scenario there are four configuration options in the Security Configuration Tool:

- **One** SCALANCE S16x of **one** control center and the SCALANCE S61x of **one** plant cell are nodes of **one** VPN group.
- **Several** SCALANCE S16x of **one** control center and the SCALANCE S61x of **one** plant cell are nodes of **one** VPN group.
- **One** SCALANCE S16x of **one** control center and **several** SCALANCE S61x of **different** plant cells are nodes of **one** VPN group.
- **Several** SCALANCE S16x of **one** control center and **several** SCALANCE S61x of **different** plant cells are nodes of **one** VPN group.

Use Case

A plant network is divided into different cells. Each cell has its own SCALANCE S and thus a different internal subnet.

These secured cells are monitored and serviced by several programmers, technicians etc. in several locations.

In each branch control center, the SCALANCE S modules initiate that a tunnel to one or more manufacturing cells is established. All PCs located behind the SCALANCE in the control center have simultaneous access to all secured cells.

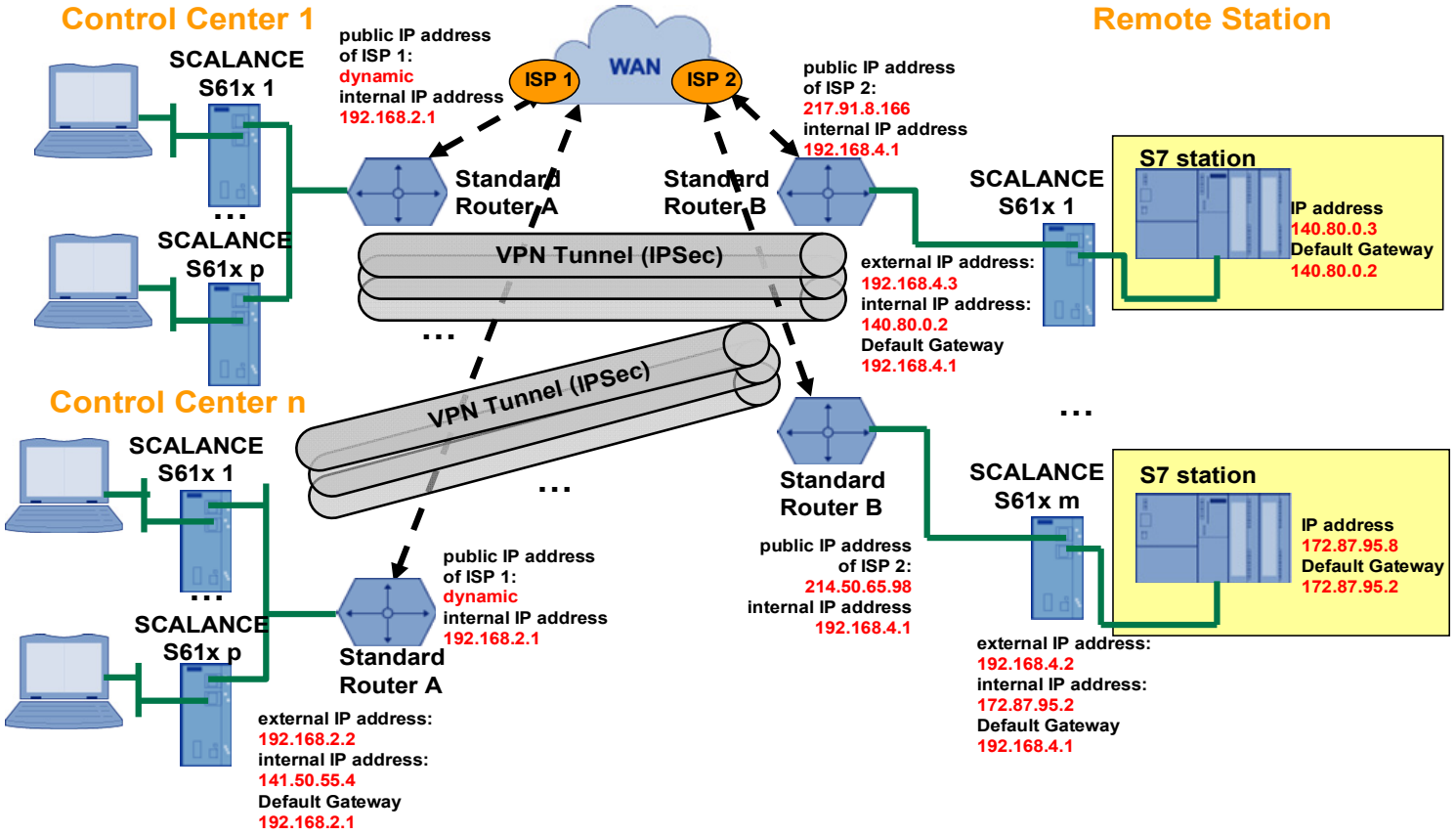
Advantages and disadvantages

Table 6-4

Advantage	Disadvantage
Several nodes (PCs) can send data through the VPN tunnel.	The software solution ties the service mechanics to a certain location.
Each SCALANCE of a cell can manage up to 128 VPN tunnels simultaneously.	If there are many cells, the data rate performance to the control center can decrease.
Each cell can be located in a different subnet.	All PCs behind a SCALANCE in the subordinate central station have access to all cells connected by the VPN tunnel.
There can be a different subnet behind each SCALANCE in the central station.	
Several plant components can be remote serviced from one PC.	

Configuration

Figure 6-4



7 Complex Remote Control System

Description

There is **one control center** with **one SCALANCE S**. There is **one SCALANCE S module** each in the remote stations. Each **service technician** has a **Softnet Security Client**. The VPN clients of the service technicians and in the remote stations set up one VPN tunnel each to the control center.

Configuration notes

For this scenario **two** VPN groups are required in the Security Configuration Tool. Nodes of the first group are the Softnet Security Client and the SCALANCE S61x in the control center. Nodes of the second group are the SCALANCE S61x of the control center and the remote station.

Use Case

There exist several plant cells or remote stations which have their own SCALANCE S and thus have a different internal subnet.

These secured cells are monitored and serviced by several programmers, technicians etc. in several locations.

The control center as central point of the plant is also secured with a SCALANCE S. Remote servicing PCs and a data base with the necessary configuration data for the remote station are available here.

In each remote station the SCALANCE S module initiates the tunnel setup to the control center at the service technicians of the Softnet Security Client. This makes the control center the end point of two **different** VPN tunnels.

A remote servicing software on the PG of the service technician enables remote control of the remote servicing PC in the control center. (e.g. the operation of STEP 7) Via this remote maintenance PC the required configuration data are loaded to the remote station (e.g. loading the hardware configuration into the controller).

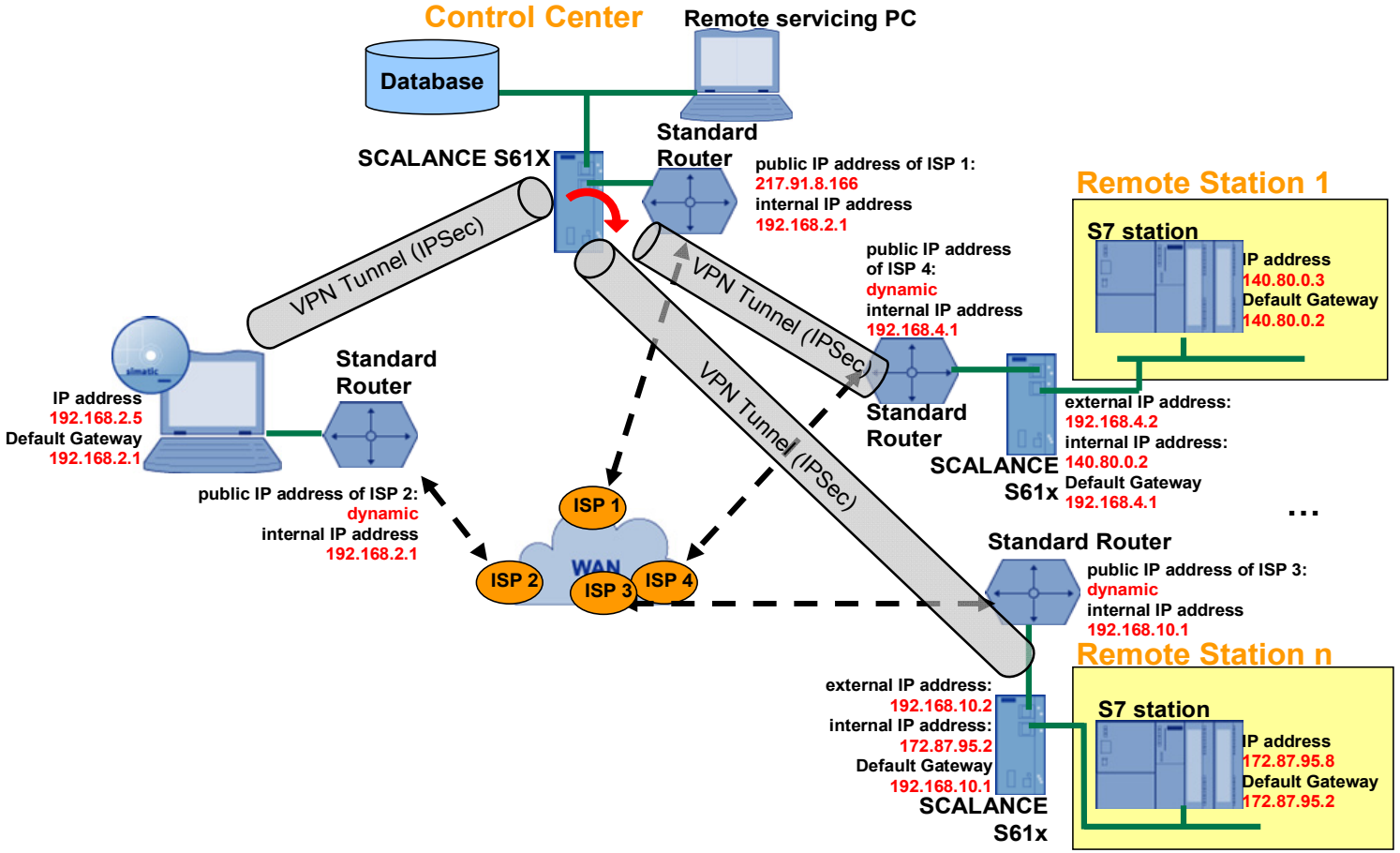
Advantages

- Minimizing wrong configurations/settings since all service technicians can download the required configuration data from the central database.
- The control center can manage up to 128 VPN tunnels simultaneously.
- Each tunnel end point can be located in a different subnet.
- Securing all project-relevant files in a central database.
- Several plant components / remote stations can be remote serviced from one PC.
- Access to the remote station can be limited to particular service technicians.

Security27043887

Configuration

Figure 7-1



8 Appendix and List of Further Literature

Internet Links

	Topic	Title
\1\	Reference to this document	http://support.automation.siemens.com/WW/view/en/27043887
\2\	Siemens A&D Customer Support	http://support.automation.siemens.com

9 History

Table 9-1 History

Version	Date	Changes
V1.0	31.10.2007	First issue
V2.0	19.02.2010	Inserting a general overview chapter. Extension by complex remote servicing system. Using the new .dot-template.