NAT with SCALANCE SC-600 / M-800 / S615

Security / NAT / SCALANCE

https://support.industry.siemens.com/cs/ww/en/view/109744660

Siemens Industry Online Support

Legal Information

Use of Application Examples

The application examples show solutions to automation tasks with the interaction of multiple components in the form of texts, graphics and/or software blocks. The application examples are provided free of charge by Siemens AG and/or a subsidiary of Siemens AG ("Siemens"). They are non-binding and are not claimed to be complete with regard to configuration and equipment. The sample applications do not constitute customer-specific solutions, they merely provide assistance with typical tasks. The responsibility rests entirely with you for ensuring the proper and safe operation of the products in compliance with the valid regulations and for checking the function of each application example and adapting it accordingly to your plant.
Siemens grants you the non-exclusive, non-sublicensable and non-transferable right to have the application examples implemented by appropriately skilled and trained personnel. The responsibility rests entirely with you for any modifications made to the application examples. Forwarding to third parties and the reproduction of the application examples or excerpts thereof is permitted only in combination with your own products. The application examples are not necessarily subject to the usual tests and quality inspections of a purchased product and might have function and/or performance defects and other faults. You are obligated to ensure that during implementation of the said application examples any faults that might occur do not cause damage or injury to persons.

Liability Disclaimer

Siemens accepts no liability, regardless of the legal grounds, in particular for the usability, availability, completeness and the freedom from defects of the application examples as well as associated instructions, configuration and performance data and any damages that might arise. This does not apply where Siemens is statutorily liable, under the Product Liability Act, for example, in the event of willful intent, gross negligence due to loss of life, injury or damage to health through the non-observance of a warranty for the condition of an object, due to the malicious non-disclosure of a defect or due to the violation of important contractual duties. However, claims for damages for the violation of important contractual duties are limited to foreseeable losses which are typically associated with this contract unless willful intent or gross negligence exists or if statutory liability is undertaken due to loss of life, injury or damage to health. The foregoing provisions shall not involve a change in the burden of proof to your detriment. Insofar as Siemens is not statutorily liable you shall indemnify Siemens from any claims in this respect from third parties.
By using sample applications you acknowledge that no claims for damages can be asserted against Siemens over and above the liability described.

Further Information

Siemens reserves the right to modify application examples at any time without notice. Where the proposals contained in application examples are inconsistent with other Siemens publications, such as catalogs, the information contained in the other documentation shall take precedence. The Siemens conditions of use shall also apply (https://support.industry.siemens.com).

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.
Customers are responsible to prevent unauthorized access to their 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. Further information about Industrial Security is available here:
https://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: https://www.siemens.com/industrialsecurity.

Contents

1 Introduction

Initial situation

The SCALANCE modules can protect industrial networks and automation systems against unauthorized access.

Thanks to its multi-layered properties, the security module can be used to protect different network topologies and flexibly implement security concepts.

- The possibility of VLAN structuring offers protection against DoS access and unauthorized access.
- Access to the device and the adjacent network can be protected by a firewall and VPN.
- By configuring as NAT router, the IP addresses of industrial networks or automation systems can be hidden from the outside. In addition, the IP address range can be used by multiple connected private networks without any address collisions.

Motivation of this documentation

By using the SCALANCE modules as routers and simultaneously supporting common NAT mechanisms, there is a wide range of possibilities for accessing the internal network or automation system to be protected:

- Static routing
- NAPT
- NAT
- NETMAP
- IP masquerading

In principle, static routing is preferable to all NAT variants. NAT requires - depending on the use case - a considerable additional effort in configuration and handling.

However, some constellations cannot be solved with routing, if no gateway is desired, for example. In these cases an appropriate NAT must be used.

Content of this document

This document describes the different options based on selected use cases. In each case, the initial situation is described and the prerequisites addressed, but the advantages and disadvantages are also highlighted.

The aim is to give an overview of the existing options and to provide an adequate solution for the most common use cases.

The following constellations are considered in detail:

Table 1-1

	Use Case	Mechanism
1.	Bidirectional communication with gateway	Standard routing
2.	Web server access without gateway (PC active, CPU passive)	NAPT
3.	PG functions on multiple CPUs without gateway	Destination NAT
4.	NATs of complete subnets	Destination NAT
5.	PG functions on all CPUs without gateway	Destination NAT
6.	Cross communication of CPUs in series machine construction	Destination NAT
7.	Connection to control systems without gateway (CPU as active part)	Source NAT
8.	Non-reactive communication via VPN tunnel for existing plants	Source NAT
9.	Non-reactive S7 communication for existing systems	Source and destination NAT

Note

The functions described in this document require firmware V06.02 in SCALANCE S615 and SCALANCE M-800 and V02.00.01 for SCALANCE SC-600. Make sure that you have at least this firmware installed on the module (see section 5).

The following descriptions apply equally for the SCALANCE M-800, SCALANCE SC-600 and SCALANCE S615 series.

2 The Use Cases at a Glance

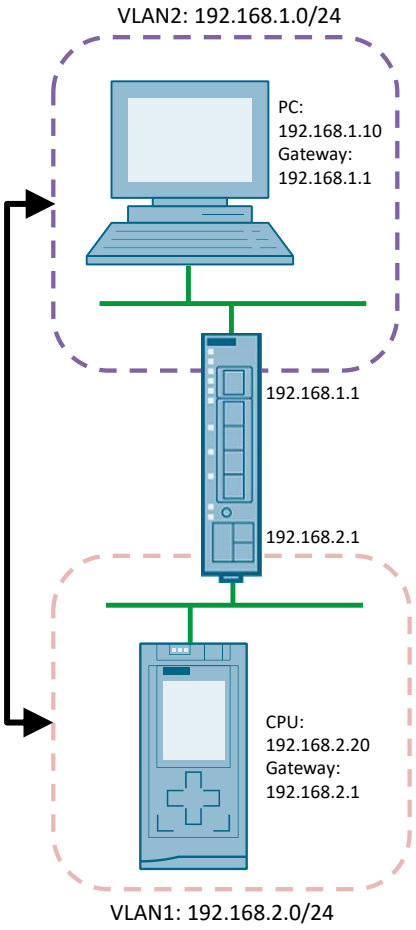
Note Basics about the mechanisms used in this document and further information about using NAT can be found in chapter 3.

2.1 Static Routing

Outset

The following constellation allows bidirectional communication between PC and CPU. The direction in which the connection is established can be freely selected.

Figure 2-1



Requirements

For network separation, SCALANCE S615 has two VLANs with different network IDs. Consequently, the device has a separate IP address for each VLAN (in this document: VLAN1: 192.168.2.1 and VLAN2: 192.168.1.1).

Depending on the VLAN assignment, this IP address of the SCALANCE S615 must be entered as gateway in the terminal device (in this document: PC or CPU).

All subnets and IP addresses are used only once in the entire network.

If additional routers are present in VLAN2 and must also communicate with VLAN1, the subnet of VLAN1 must also be made known or configured there.
In general, all subnets must be known to the routers.

Procedure (active setup CPU to PC)

The IP address 192.168.1.10 cannot be reached locally. The packet is sent to the gateway.

The SCALANCE S615 has an interface in the subnet 192.168.2.0 and forwards the packet directly to the PC.

From the PC point of view, the IP address 192.168.2.20 is not local. The response packets are also sent to the gateway.

Advantages

The advantages of this scenario are:

- All nodes can establish connections in any direction.
- Each node can be reached via a unique address.

Firewall rules

The bidirectional communication between the two VLANs is enabled in the firewall of SCALANCE S615.

Figure 2-2

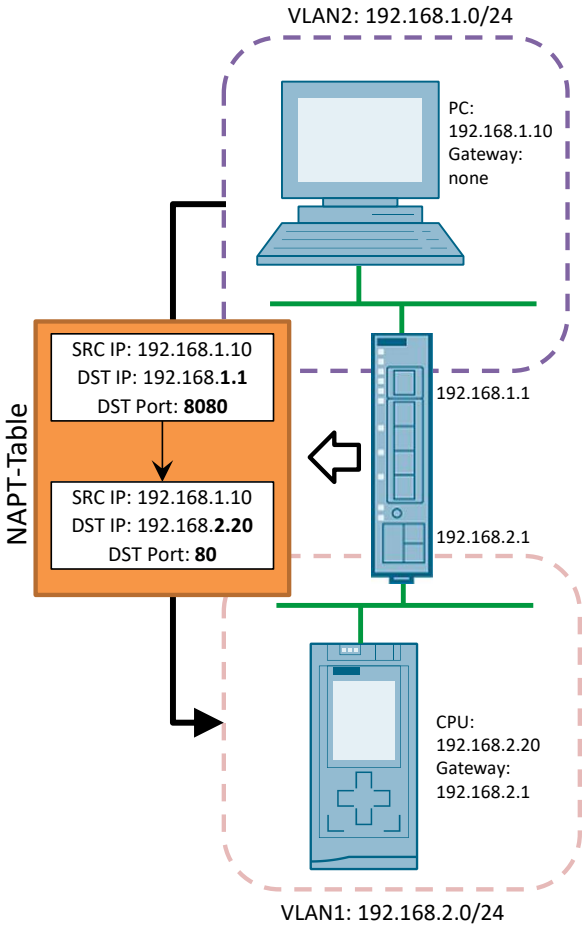
Action	From	To	Source (Range)	Destination (Range)	Service
Accept	Vlan2	Vlan1	192.168.**1.10**/32	192.168.**2.20**/32	Destination Port **X**
Accept	Vlan1	Vlan2	192.168.**2.20**/32	192.168.**1.10**/32	Destination Port **X**

2.2 Web Server Access via NAPT

Outset

The PC should be able to access the web server of the CPU without gateway. The destination port is not fixed and can be adjusted during setup.

Figure 2-3



Requirements

For network separation, SCALANCE S615 has two VLANs with different network IDs. Consequently, the device has a separate IP address for each VLAN (in this document: VLAN1: 192.168.2.1 and VLAN2: 192.168.1.1).

In addition, a NAPT table is defined in SCALANCE S615 to rewrite the messages of the PC to another IP address.

So that the response packets of the CPU find their way into VLAN2, the IP address of SCALANCE S615 (VLAN1) must be entered in the CPU as gateway.

Procedure (active setup PC to CPU)

The PC addresses as destination the local IP address of the SCLANCE S615 (192.168.1.1) including a port specification instead of the IP address of the CPU 192.168.2.20.

Based on the definition in its NAPT table the SCALANCE S615 replaces the destination IP address and optionally a port and sends the packet to the CPU.

The source IP address (in this document: 192.168.1.10) is not changed, from the CPU point of view the packet comes from a different subnet. Therefore the CPU

requires an additional entry for the gateway (IP address of the SCALANCE S615 for VLAN1).

In all response packets that are sent from the CPU to the PC, the source IP address 192.168.2.20 is automatically replaced by 192.168.1.1.

Advantages

The advantage of this scenario is that no additional gateway entry is required in the PC. The already used IP address of the SCALANCE S615 of the local network serves as destination address. No additional IP is required in VLAN 2.

Disadvantages

The disadvantage is that only one active setup from PC to CPU is possible. Each port can only be forwarded once. Via protocols with a fixed destination port (S7 protocol, for example), only one single node in VLAN1 can be addressed.

Forwarded ports can no longer be used by SCALANCE S615 (for example: http, IPSec, SNMP etc.)

NAPT and firewall rules

In the NAPT table of SCALANCE S615, packets from VLAN2 with the destination IP address 192.168.1.1:8080 are translated to the IP address of the CPU 192.168.2.20:80. Port 80 is used because this is a web server access.

Figure 2-4

Source Interface	Traffic Type	Interface IP	Destination IP	Destination Port	Translated Destination IP	Translated Destination Port
vlan2	TCP	☑	192.168.1.1	8080	192.168.2.20	80

Communication between PC (VLAN2) and CPU (VLAN1) must be allowed in the firewall.

Figure 2-5

Action	From	To	Source (Range)	Destination (Range)	Service
Accept	vlan2	vlan1	192.168.1.10/32	192.168.2.20/32	Destination Port 80 TCP

Notes

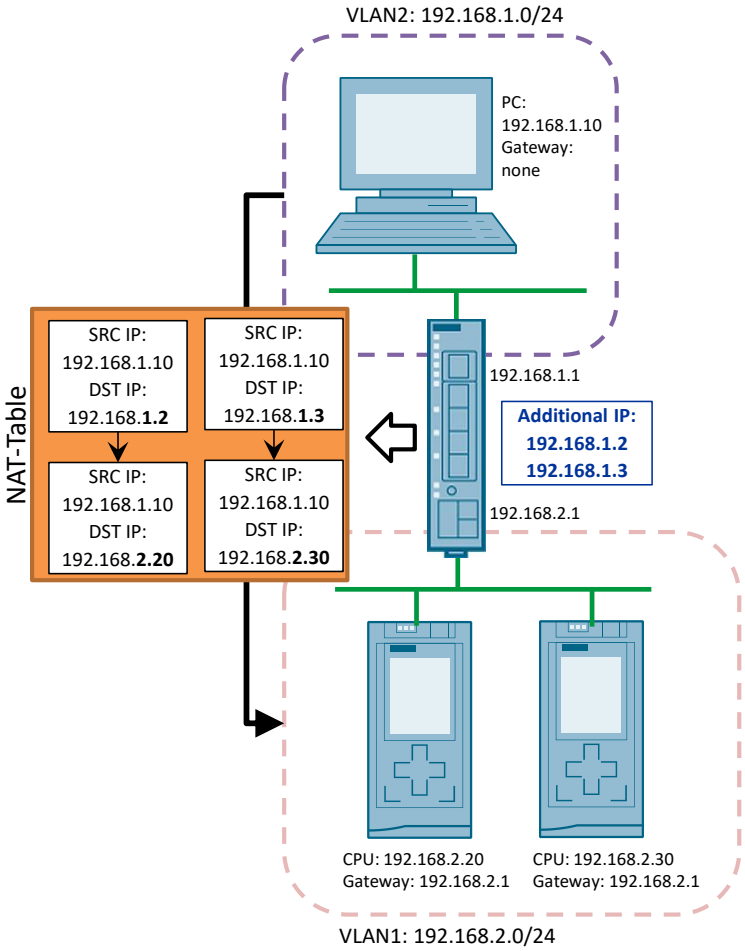
- Address translation with NAPT was done before the firewall, so the translated addresses and ports must be used for address translation.
- From the PC point of view the web server of the CPU is thus accessible via http://192.168.1.1:8080.
- Further CPUs can be made equally accessible by using a different destination port and destination IP address, 192.168.1.1:8081 -> 192.168.2.30:80, for example.
- To completely enable VLAN2 to access the CPU, the firewall rule for the source must be changed as follows: 192.168.1.0/24.
- The more common term for NAPT is port forwarding.

2.3 PG Functions with NETMAP and Destination NAT

Outset

The PC is to use STEP 7 PG functions on several CPUs without gateway. STEP 7 PG functions run on an S7 connection with an unchangeable destination port TCP 102.

Figure 2-6



Requirements

For network separation, SCALANCE S615 has two VLANs with different network IDs. Consequently, the device has a separate IP address for each VLAN (in this document: VLAN1: 192.168.2.1 and VLAN2: 192.168.1.1).

To rewrite the messages of the PC to another IP address, a NAT table is additionally defined in SCALANCE S615. This requires two additional, unused IP addresses from the subnet of VLAN2.

So that the response packets of both CPUs find their way into VLAN2, the IP address of SCALANCE S615 (VLAN1) must be entered as gateway in both CPUs.

Procedure (active setup PC to CPU)

The additional NAT IP addresses 192.168.1.2 and 192.168.1.3 are occupied by SCALANCE S615.

The PC addresses as destination the local IP address 192.168.1.2 or 192.168.1.3.

The SCALANCE S615 uses the definition in its NAT table to replace the destination IP address and sends the packet to CPU1 or CPU2.

The source IP address (in this document: 192.168.1.10) is not changed, from the CPU point of view the packet comes from a non-local subnet.
Therefore the CPU requires an additional entry for the gateway (IP address of the SCALANCE S615 for VLAN1).

The source IP address 192.168.2.20 (or 192.168.2.30) is automatically replaced by 192.168.1.2 (or 192.168.1.3) in all response packets from the CPU to the PC.

Advantages

The advantage of the NAT table is that by using additional addresses per CPU, all ports can be forwarded or used.

Disadvantages

The disadvantage is that only one active setup from PC to CPU is possible. Additional IP addresses from the subnet of VLAN2 are also required per CPU, each of which must be configured accordingly.

NAT and firewall rules

In the NAT table of SCALANCE S615, packets from VLAN2 with the destination IP address 192.168.1.2:1.3 (or 192.168.1.3) are translated to the IP address of the CPU 192.168.2.20:2.30 (or 192.168.2.30).

Figure 2-7

Type	Source Interface	Destination Interface	Source IP Subnet	Destination IP Subnet	Trans. Destination IP Subnet
Destination	vlan2	vlan1	192.168.**1.10**/32	192.168.**1.2**/32	192.168.**2.20**/32
Destination	vlan2	vlan1	192.168.**1.10**/32	192.168.**1.3**/32	192.168.**2.30**/32

Communication between PC (VLAN2) and both CPUs (VLAN1) must be allowed in the firewall. The service is limited to port 102 because only PG functions are permitted via an S7 connection.

Figure 2-8

Action	From	To	Source (Range)	Destination (Range)	Service
Accept	vlan2	vlan1	192.168.**1.10**/32	192.168.**2.20**/32	Destination Port **102** TCP
Accept	vlan2	vlan1	192.168.**1.10**/32	192.168.**2.30**/32	Destination Port **102** TCP

NETMAP Bidirectional / Auto firewall rules

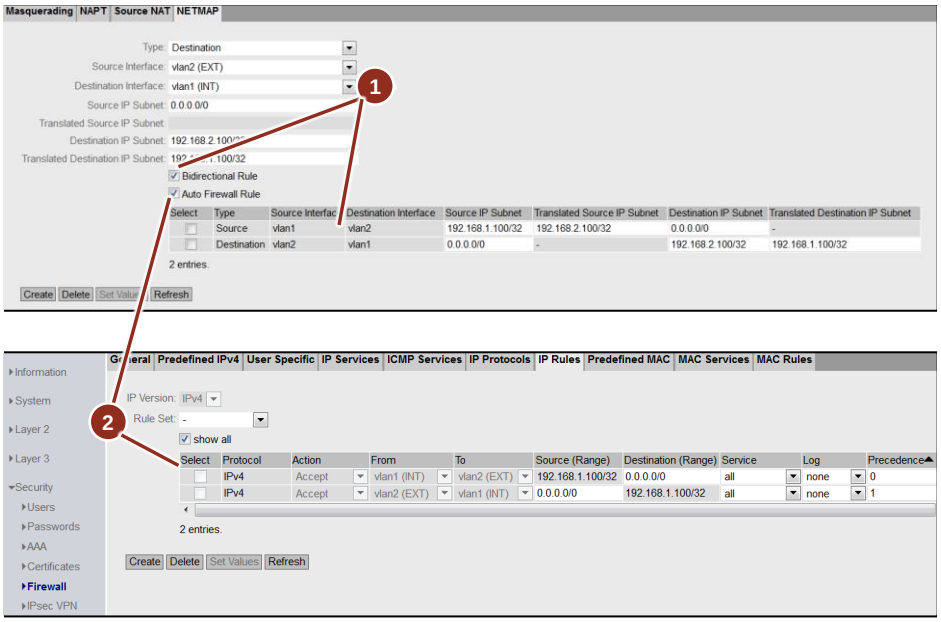
NETMAP offers two additional options to simplify configuration:

- With the **Bidirectional rule**, a corresponding NAT entry is automatically generated in the opposite direction, with reversed IP addresses.
- With the **Auto firewall rule**, firewall rules are also automatically generated for the NAT entries. The IP addresses are automatically taken from the NAT. Depending on the NAT type, either the source or destination IP can be manually restricted.

  If the user changes the IP addresses in the NAT entry, the firewall rule automatically applies the change.
  The firewall rules cannot be deleted, the corresponding NAT entry has to be removed.

Note "Bidirectional" and "Auto" firewall rules make configuration considerably easier. It is recommended to use these options.

Figure 2-9



Notes

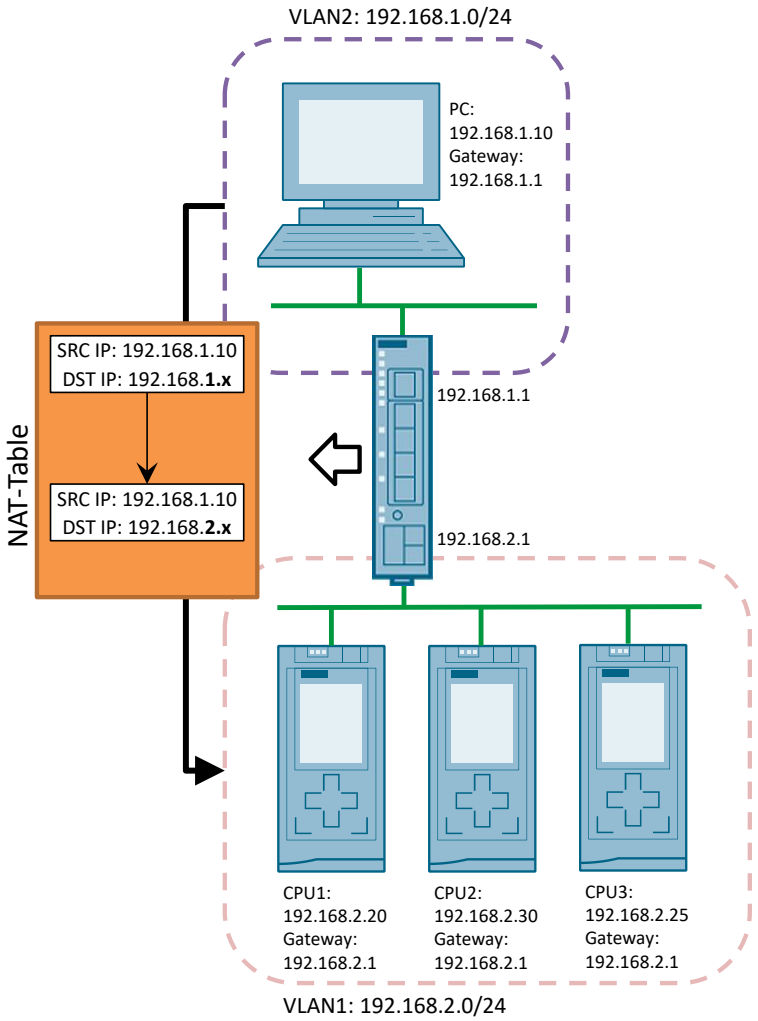
- Address translation with NAT was done before the firewall, so the translated addresses must be used in the firewall.
- From the PC (or STEP 7) point of view the two CPUs are accessible via the IP addresses 192.168.1.2 and 192.168.1.3 respectively.
- To completely enable VLAN2 to access the CPU, the firewall rule and the NAT rule for the source must be changed as follows: 192.168.1.0/24.
- NAPT could also be used for a single CPU (see section 2.2).
- With NETMAP, x addresses are always translated into x other addresses - also called 1:1 NAT.
- The columns "Trans.Destination IP Subnet" in SCALANCE S615 may only be configured with a single IP address - i.e. /32. Only then does SCALANCE S615 also answer ARP requests for the additional IP addresses.

2.4 NATs of Complete Subnets with NETMAP and Destination NAT

Outset

The PC is to communicate with several or all devices in an automation network. The destination port is not fixed and can be adjusted during setup.

Figure 2-10



Requirements

For network separation, SCALANCE S615 has two VLANs with different network IDs. Consequently, the device has a separate IP address for each VLAN (in this document: VLAN1: 192.168.2.1 and VLAN2: 192.168.1.1).

To rewrite the messages of the PC to another IP address, a NAT table is additionally defined in SCALANCE S615. This requires another free subnet (in this document: 172.16.1.0/24). The additional, virtual subnet exists only within the SCALANCE S. It is freely selectable and completely independent of the subnet on VLAN 1.

Depending on the VLAN assignment, this IP address of the SCALANCE S615 must be entered as gateway in the terminal device (in this document: PC or automation device).

Procedure (active setup PC to CPU)

The additional subnet 172.16.1.0/24 is occupied by SCALANCE S615. SCALANCE S615 uses NETMAP for address translation. With NETMAP it is possible to translate complete subnets into another subnet. The addresses are translated 1:1.

The following translations result for the example:

Table 2-1

Target IP address	Virtual NAT IP address
192.168.2.20	172.16.1.20
192.168.2.30	172.16.1.30
192.168.2.25	172.16.1.25

The PC addresses the destination via routing, the IP address 172.16.1.20, for example.

Based on the definition in its NAT table the SCALANCE S615 replaces the destination IP address with 192.168.2.20 and sends the packet to the CPU1.

The source IP address (in this document: 192.168.1.10) is not changed, from the CPU point of view the packet comes from a non-local subnet.
Therefore the CPU requires an additional entry for the gateway (IP address of the SCALANCE S615 for VLAN1).

The source IP address 192.168.2.x (or 2.2.30) is automatically replaced by 172.16.1.x in all response packets from the CPU to the PC.

Advantages

The advantage of the NAT table is that by using additional addresses per CPU, all ports can be forwarded or used. The 1:1 address translation simplifies the NAT configuration, because only one line in the NAT table is required.

Disadvantages

The route to the virtual subnet must be known. The virtual NAT IP addresses cannot be addressed directly.

NAT and firewall rules

In the NAT table of SCALANCE S615, packets with the target IP address from the translation network 172.16.1.0/24 are translated to VLAN 1. The translation is done on the basis of a 1:1 relationship.

Figure 2-11

Type	Source Int.	Dest. Int.	Source IP	Destination IP	Trans. Destination IP
Destination	vlan2	vlan1	192.168.**1.10/32**	172.16.1.0/**24**	192.168.**2.0/24**

Communication between PC (VLAN2) and the automation devices (VLAN1) must be allowed in the firewall.

Figure 2-12

Action	From	To	Source (Range)	Destination (Range)	Service
Accept	vlan2	vlan1	192.168.**1.10**/32	192.168.**2.0/24**	Dest. Port **X**

Notes

- Address translation with NAT was done before the firewall, so the translated addresses must be used in the firewall.
- To completely enable VLAN2 to access the automation devices, the firewall rule and the NAT rule for the source must be changed as follows: 192.168.1.0/24.
- No ARP requests are answered on 172.16.1.x.
  Consequently, these addresses are only accessible via routing.
- NAPT could also be used for a single CPU (see section 2.2).
- With NETMAP, x addresses are always translated into x other addresses - also called 1:1 NAT.
- The subnets of the objects participating in NETMAP must all have the same size, for example all /24.

2.4.1 Virtual Subnets with NETMAP

Requirements

- The SCALANCE S IP address (192.168.1.1) is entered as gateway in the terminal device (the CPU, for example).
- The virtual subnets must be made known via routing (as default gateway in the PC, for example).
- The virtual subnet must have the same size as the physical one, which corresponds to a 1:1 translation.

Procedure (active setup in both directions)

- The PC addresses the virtual subnet 172.16.1.X via routing and sends the packet to the SCALANCE.
- Usable without restrictions, the S615 translates the virtual IP to the physical one in VLAN1.
  1.1 > 1.1 1.2 > 1.2 1.X > 1.X
- Translation the same in reverse direction if the CPU sets up actively.

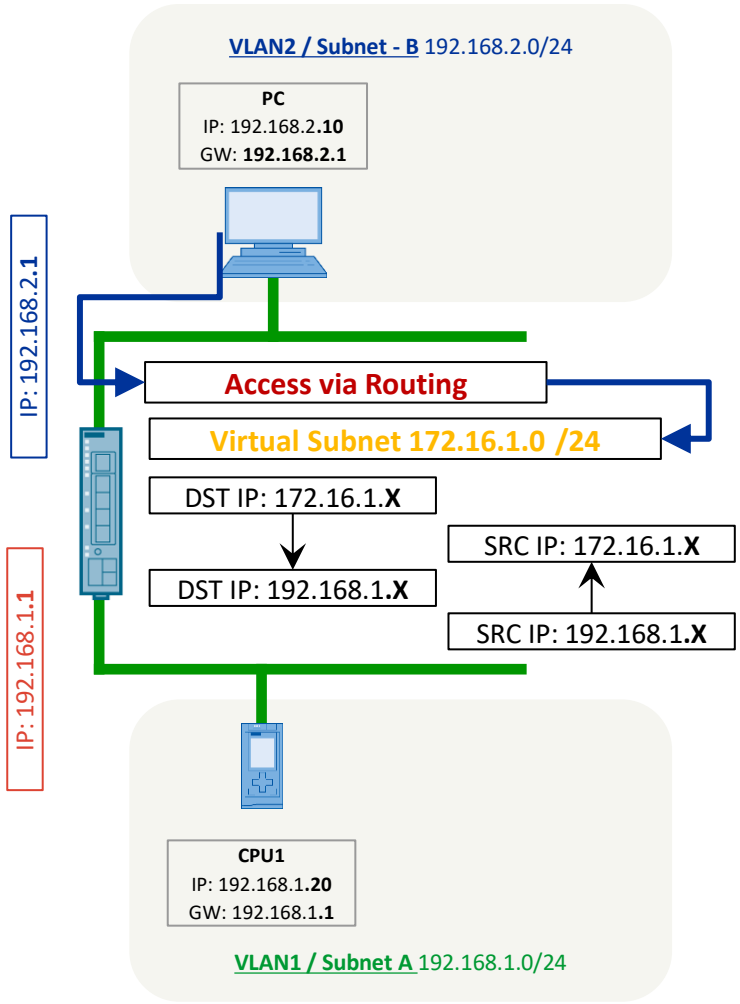
Advantages

- No other addresses are required in VLAN2.
- The virtual network is freely selectable. Without routing, the virtual addresses are not visible on the network.
- One line in the NETMAP configuration is enough to translate the complete subnet.
- Since the addresses are not physically occupied, the NAT can be combined with VRRP / redundancy.

Disadvantages

The virtual subnets must be accessible via routing.

Figure 2-13

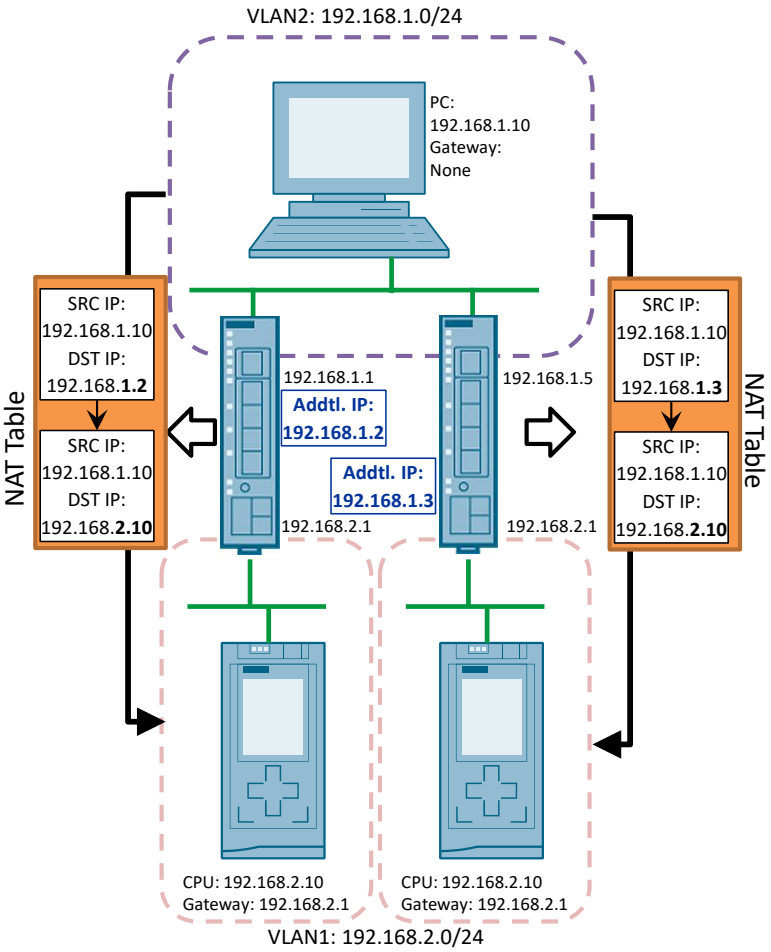


2.5 Series Machines with NETMAP and Destination NAT

Outset

In this case, several identical plant sections are to be reached by one PC. Consequently, the same subnet (in this document: 192.168.2.x) is used in all plant sections.

The PC is to communicate without gateway with each CPU from the plant sections and execute any functions.



Requirements

A SCALANCE S615 is connected upstream of each plant section.

For network separation, SCALANCE S615 has two VLANs with different network IDs. Consequently, the device has a separate IP address for each VLAN (in this document: VLAN1: 192.168.2.1 and VLAN2: 192.168.1.1 or 192.168.1.5).

The SCALANCE S615 and the PC are connected via VLAN2.

This setup requires NAT and cannot be solved with pure routing, because the subnet from VLAN1 could not be clearly assigned, independent of the direction of the connection setup and gateway in the PC.
One SCALANCE S615 module is required per identical, internal subnet. It is not possible to connect multiple, identical subnets to a single SCALANCE S615.

This means that a NAT table is additionally defined in SCALANCE S615 in order to rewrite the messages of the PC to another IP address. This requires another IP address from the subnet of VLAN2.

So that the response packets of both CPUs find their way back into VLAN2, the IP address of SCALANCE S615 (VLAN1) must be entered as gateway in both CPUs.

Procedure (active setup PC to CPU)

The additional NAT IP addresses 192.168.1.2 and 192.168.1.3 are occupied by the two SCALANCE S615s.

The PC addresses as destination the local IP address 192.168.1.2 or 192.168.1.3.

The associated SCALANCE S615 uses the definition in its NAT table to replace the destination IP address and sends the packet to CPU1 or CPU2.

The source IP address (in this document: 192.168.1.10) is not changed, from the CPU point of view the packet comes from a non-local subnet.
Therefore the CPU requires an additional entry for the gateway (IP address of the associated SCALANCE S615 for VLAN1).

The source IP address 192.168.2.10 is automatically replaced by 192.168.1.2 or 192.168.1.3 in all response packets from the CPU to the PC.

Advantages

The advantage of the NAT table is that by using an additional address all ports can be forwarded or used.

Disadvantages

The disadvantage is that only one active setup from PC to CPU is possible. Furthermore, one additional IP address from the subnet of VLAN2 is required per plant section, each of which must be configured accordingly.

NAT and firewall rules

In the NAT table of SCALANCE S615 for the first plant section, packets from VLAN2 with the destination IP address 192.168.1.2 are translated to the IP address of the CPU 192.168.2.10.

Figure 2-14

Type	Source Interface	Destination Interface	Source IP Subnet	Destination IP Subnet	Trans. Destination IP Subnet
Destination	vlan2	vlan1	192.168.**1.10**/32	192.168.**1.2**/32	192.168.**2.10**/32

The NAT table of SCALANCE S615 for the second plant section is configured accordingly.

Figure 2-15

Type	Source Interface	Destination Interface	Source IP Subnet	Destination IP Subnet	Trans. Destination IP Subnet
Destination	vlan2	vlan1	192.168.**1.10**/32	192.168.**1.3**/32	192.168.**2.10**/32

The firewall rule is identical for both SCALANCE S615s, because both use the same subnet in VLAN1.
Communication between PC (VLAN2) and CPU (VLAN1) must be allowed in the firewall. Since all functions may be executed, there is no port restriction.

Figure 2-16

Action	From	To	Source (Range)	Destination (Range)	Service
Accept	vlan2	vlan1	192.168.**1.10**/32	192.168.**2.10**/32	Ports **Beliebig** = *

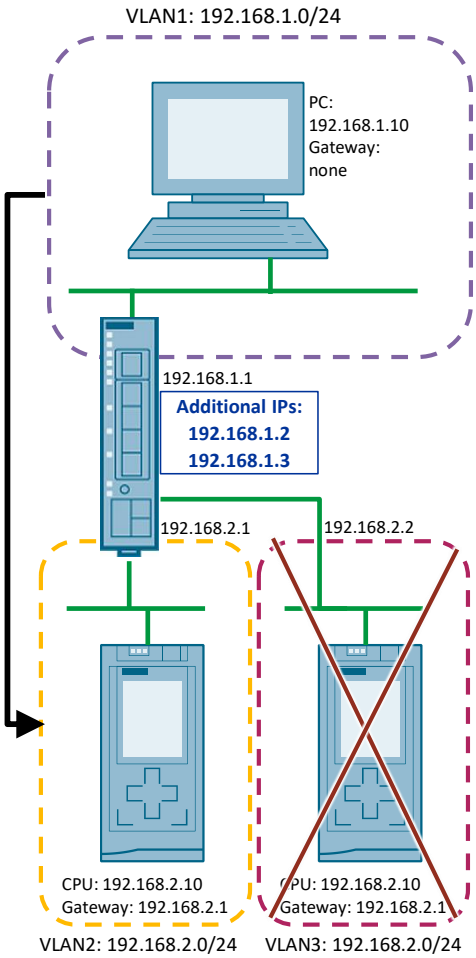
Notes

- Address translation with NAT was done before the firewall, so the translated addresses must be used in the firewall.
- From the PC (or STEP 7) point of view the two CPUs are therefore accessible via 192.168.1.2 and 192.168.1.3 respectively. This ensures the association of the CPUs despite identical subnets in VLAN1.
- To completely enable VLAN2 to access the CPU, the firewall rule and the NAT rule for the source must be changed as follows: 192.168.1.0/24.
- With NETMAP, x addresses are always translated into x other addresses - also called 1:1 NAT.
- The columns "Trans.Destination IP Subnet" in SCALANCE S615 may only be configured with a single IP address - i.e. /32. Only then does SCALANCE S615 also answer ARP requests for the additional IP addresses.

Restriction

It is not possible to connect the same subnet twice to a single SCALANCE S. There is no way to distinguish between 192.168.2.10 in VLAN2 and 192.168.2.10 in VLAN3.

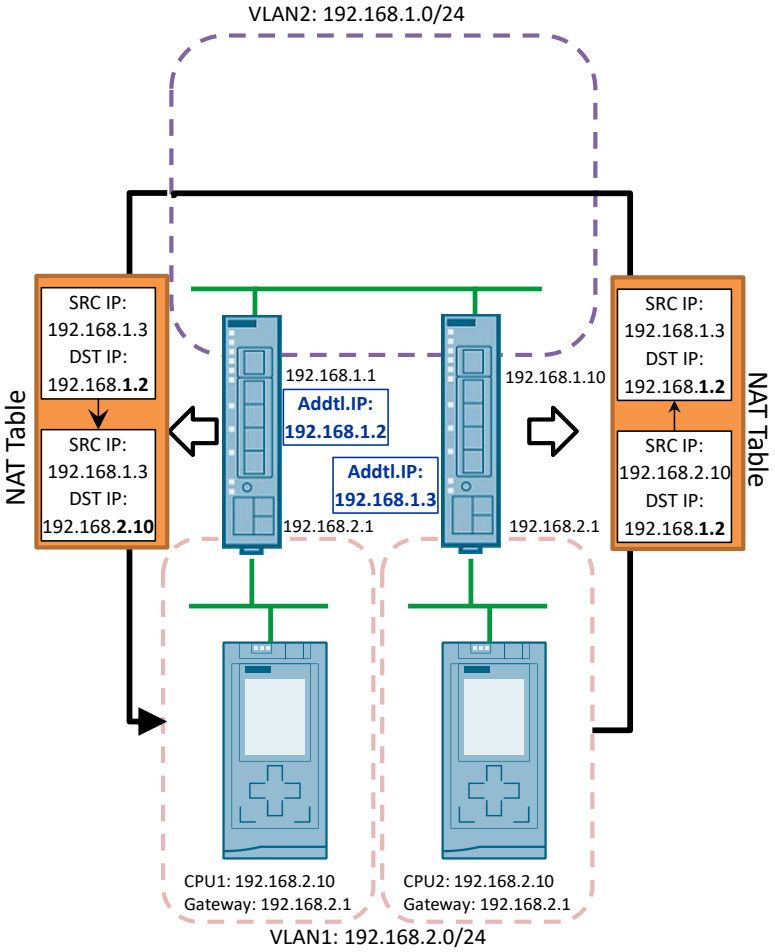
During the routing process the decision must be made to which IP interface the outgoing packet is to be transferred. Since the IP address 192.168.2.10/24 exists twice, there should be two identical entries in the routing table. In this case, only one entry is processed, while the second remains unused.



2.6 Cross Communication with Series Machines with NETMAP and Destination NAT

Outset

In this case, multiple identical plant sections are to communicate with each other (in this document: CPU2 and CPU1). The same subnet (in this document: 192.168.2.x) is used in all plant sections.



Requirements

A SCALANCE S615 is connected upstream of each plant section.

For network separation, SCALANCE S615 has two VLANs with different network IDs. Consequently, the device has a separate IP address for each VLAN (in this document: VLAN1: 192.168.2.1 and VLAN2: 192.168.1.1 or 192.168.1.10).

The SCALANCE S615s are connected via VLAN2.

This setup requires NAT and cannot be solved with pure routing, because the subnet from VLAN1 could not be clearly assigned, independent of the direction of the connection setup and gateway in the PC.
One SCALANCE S615 module is required per identical, internal subnet. It is not possible to connect multiple, identical subnets to a single SCALANCE S615.

This means that a NAT table is additionally defined in SCALANCE S615 in order to rewrite the messages of the PC to another IP address. This requires another IP address from the subnet of VLAN2.

The destination NAT is used in the left SCALANCE S615 (first plant section), the source NAT is used in the right SCALANCE S615 (second plant section).

So that the response packets of both CPUs find their way back into VLAN2, the IP address of SCALANCE S615 (VLAN1) must be entered as gateway in both CPUs.

Procedure (active setup CPU2 to CPU1)

The additional NAT IP addresses 192.168.1.2 and 192.168.1.3 are occupied by the two SCALANCE S615s.

The CPU2 addresses as destination the local IP address 192.168.1.2.

Based on the definition in its NAT table the associated SCALANCE S615 from the second plant section replaces the source IP address with 192.168.1.3 and sends the packet to CPU1.

Based on the definition in its NAT table the associated SCALANCE S615 from the first plant section replaces the destination IP address with 192.168.2.10 and sends the packet to CPU1.

The source IP has been changed, from the CPU1 point of view the packet comes from a non-local subnet. It is necessary to change the source IP address for the following reason: CPU1 and CPU2 use the same IP address internally (in this document: 192.168.2.10). Without changing the source IP address, for CPU1 it would look as if the packet came from its own IP address.

Advantages

Although both CPUs use the same IP address and subnet, direct CPU-CPU communication is possible.

Disadvantages

The disadvantage is that only one active setup from CPU2 to CPU1 is possible. For a bidirectional CPU-CPU communication the same rules must be additionally configured in the opposite direction.
An additional IP address from the subnet of VLAN2 is required per plant section, each of which must be configured accordingly.

NAT and firewall rules

In the NAT table of SCALANCE S615 for the first plant section, packets from VLAN2 with the destination IP address 192.168.1.2 are translated to the IP address of the CPU1 192.168.2.10.

Figure 2-17

Type	Source Int.	Dest. Int.	Source IP	Destination IP	Trans. Destination IP
Destination	vlan2	vlan1	192.168.**1.3/32**	192.168.**1.2/32**	192.168.**2.10/32**

In the NAT table of SCALANCE S615 for the second plant section, packets from VLAN1 with the source IP address 192.168.2.10 are translated to their own additional VLAN2 IP address 192.168.1.3.

Figure 2-18

Type	Source Int.	Dest. Int.	Source IP	Trans. Source IP	Destination IP
Source	vlan1	vlan2	192.168.**2.10/32**	192.168.**1.3/32**	192.168.**1.2/32**

In the firewall of both SCALANCE S615s the communication between CPU1 (VLAN1) and CPU2 (VLAN1) via VLAN2 must be allowed as per the NAT table. The CPU-CPU communication is based on an S7 communication. The services are therefore limited to port 102.

In the firewall of SCALANCE S615 from the first plant section, communication between VLAN2 (additional IP address in the right SCALANCE S615) and CPU1 (VLAN1) must be allowed.

Figure 2-19

Action	From	To	Source (Range)	Destination (Range)	Service
Accept	vlan2	vlan1	192.168.**1.3**/32	192.168.**2.10**/32	Dest. Port **102**

In the firewall of SCALANCE S615 from the second plant section, communication between CPU2 (VLAN1) and VLAN2 (additional IP address in the left SCALANCE S615) must be allowed.

Figure 2-20

Action	From	To	Source (Range)	Destination (Range)	Service
Accept	vlan1	vlan2	192.168.**2.10**/32	192.168.**1.2**/32	Dest. Port **102**

Notes

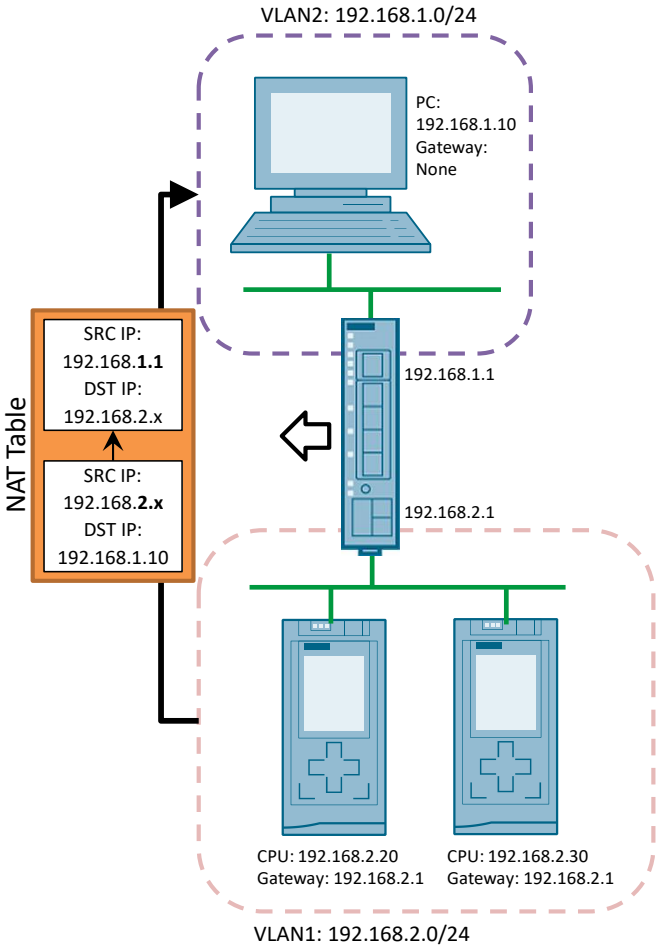
- In SCALANCE S615 from the first plant section, the address translation with NAT (destination NAT) was done before the firewall, so the translated addresses must be used in the firewall.
- In SCALANCE S615 from the second plant section, the address translation with NAT (source NAT) is done only after the firewall, so the physical addresses must be used in the firewall.
- The columns "Trans.Destination IP Subnet" and "Trans.Source IP Subnet" in SCALANCE S615 may only be configured with a single IP address - i.e. /32. Only then does SCALANCE S615 also answer ARP requests for the additional IP addresses.
- To translate all internal nodes from the second plant section into the IP address of the SCALANCE S615 IP in VLAN2, source NAT or masquerading can be used as an alternative to NETMAP → Source NAT.

2.7 Connection to the Control System with Source NAT

Outset

Multiple CPUs are to actively establish a connection to the PC. The PC itself has no gateway entered.
The destination port can be fixed or adjustable (S7 connection or TCP/UDP native).

Figure 2-21



Requirements

For network separation, SCALANCE S615 has two VLANs with different network IDs. Consequently, the device has a separate IP address for each VLAN (in this document: VLAN1: 192.168.2.1 and VLAN2: 192.168.1.1).

In addition, a NAT table is defined in SCALANCE S615 to rewrite the messages of the CPUs to another IP address.

So that the messages of both CPUs find their way into VLAN2, the IP address of SCALANCE S615 (VLAN1) must be entered as gateway in both CPUs.

Procedure (active setup CPU to PC)

The destination IP address 192.168.1.10 is not located in the local subnet of VLAN1. All messages are sent to the gateway (IP address of SCALANCE S615 (VLAN1)).

Based on the definition in its NAT table the SCALANCE S615 replaces the source IP address with its own IP address (192.168.1.1) and sends the packet to the destination IP address.

From the PC point of view, all packets of the CPUs come from the local subnet VLAN2. It is therefore possible to respond directly. The subnet of VLAN1 is not visible to the outside.

In all response packets from the PC to the CPU the destination IP address is automatically replaced with the respective CPU IP address.
The assignment is based on the already existing state in the firewall. A manual assignment as with the destination NAT is not necessary.

Advantages

The advantage of this NAT table is that no additional IP address is required. The source IP address is the one already used by SCALANCE S615 for VLAN2.

Disadvantages

The disadvantage is that only one active setup from CPU to PC is possible. Due to the identical source IP addresses, it is no longer possible to tell from which CPU the packets come.

NAT and firewall rules

In the NAT table of SCALANCE S615, packets from VLAN1 with the source IP address 192.168.2.x are translated to their own VLAN2 IP address 192.168.1.1.

Figure 2-22

Source Interface	Destination Interface	Source IP Address(es)	Use Interface IP	Translated Source IP Address	Destination IP Address(es)
vlan1	vlan2	192.168.2.0/24	☑	192.168.1.1	0.0.0.0/0

Communication between CPU (VLAN1) and PC (VLAN2) must be allowed in the firewall. The services are limited to TCP.

Figure 2-23

Action	From	To	Source (Range)	Destination (Range)	Service
Accept	vlan1	vlan2	192.168.2.0/24	192.168.1.10/32	Destination Port X TCP

Notes

- Address translation with source NAT is done only after the firewall, so the physical addresses must be used here.
- To enable any source or destination IP addresses, the firewall rule must be changed as follows: 0.0.0.0/0.
- The Source NAT tab translates multiple arbitrary IPs into a single IP, i.e. N:1 NAT.
- The NETMAP: Source NAT translates multiple IPs into multiple IPs, i.e. 1:1 NAT.
- In the reverse direction the setup works correspondingly if the two CPUs have no gateway entry.
- With Source NAT, the translation shown here is usually sufficient, since the source IP address of a connection is usually not checked. Otherwise, use a corresponding "NETMAP > Source NAT" (see section 2.5) to translate to individual addresses.

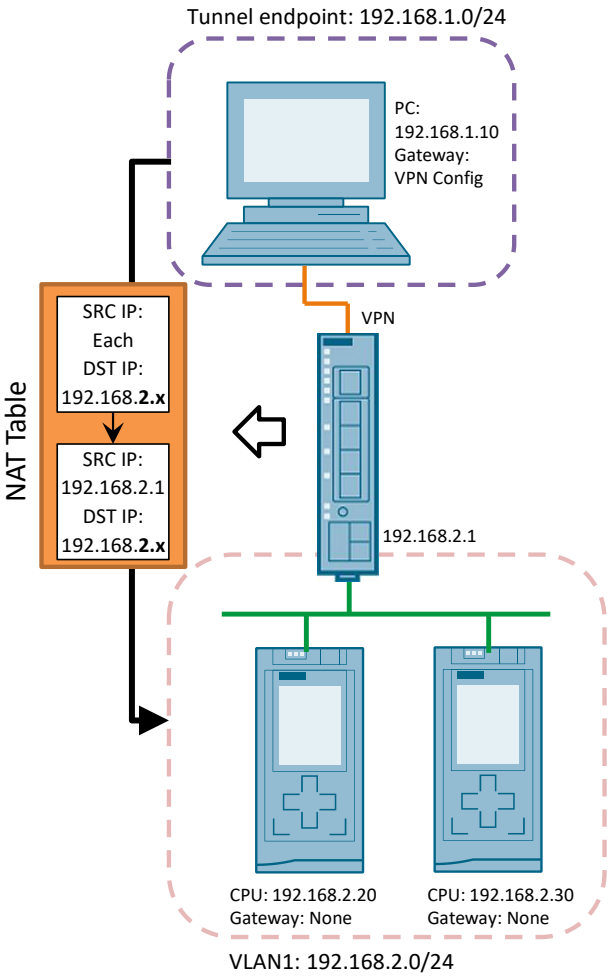
- Since multiple IP addresses are translated into a single IP address, the source port of a connection request may also change in the course of the source NAT. This is unavoidable if two nodes use the same source port.

2.8 Source NAT from VPN Tunnel

Outset

The PC is to be able to use any functions on the S7 CPUs of an existing plant securely via a VPN tunnel. No gateway is entered on the CPUs and the hardware setting should not be changed.
The destination port is not fixed and can be adjusted during setup.

Figure 2-24



Requirements

The basis of this constellation is an existing IPSec tunnel with SCALANCE S615 as tunnel end point. The VPN partner can, for example, be the SOFTNET Security Client or another SCALANCE S that is connected upstream of the PC.

For network separation, SCALANCE S615 has VLANs with different network IDs. Consequently, the device has a separate IP address for each VLAN (in this document: VLAN1: 192.168.2.1). Only VLAN1 is of interest for this setup, since the VPN tunnel terminates here.

To rewrite the messages from the VPN tunnel to another IP address, a NAT table is additionally defined in SCALANCE S615.

Procedure (active setup PC to CPU)

All messages coming from the VPN tunnel reach the SCALANCE S615 at the subnet VLAN1.

Based on the definition in its NAT table the SCALANCE S615 replaces the source IP address with its own IP address (192.168.2.1) and sends the packet to the corresponding node.

From the CPU point of view, all packets from the local subnet VLAN1, to which a direct response can be made.

In all response packets from the CPU to the PC the destination IP address is automatically replaced with the PC IP address.
The assignment is based on the already existing state in the firewall, a manual assignment as with the destination NAT is not necessary.

Advantages

The advantage is that access is possible without having to adjust the settings in the terminal devices (non-reactive).

Disadvantages

The disadvantage is that because the source IP addresses are identical, it is no longer possible to tell which remote node the packets come from.

NAT and firewall rules

In the NAT table of SCALANCE S615 all packets from the VPN tunnel are translated to their own VLAN1 IP address.

Figure 2-25

Source Interface	Destination Interface	Source IP Address(es)	Use Interface IP	Translated Source IP Address	Destination IP Address(es)
IPSec(all)	vlan1	0.0.0.0/0	☑	192.168.2.1	0.0.0.0/0

Communication between the VPN tunnel and the internal network VLAN1 must be allowed in the firewall. The services are unrestricted.

Figure 2-26

Action	From	To	Source (Range)	Destination (Range)	Service
Accept	IPSec(all)	Vlan1	0.0.0.0/0	192.168.2.0/24	Ports Beliebig = *

Notes

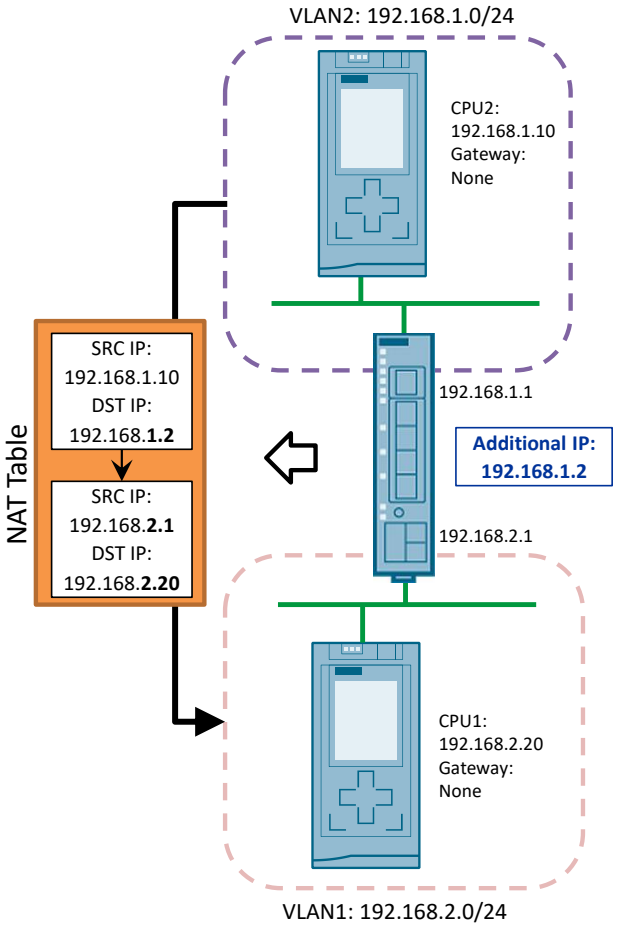
- Address translation with source NAT is done only after the firewall, so the remote VPN addresses must be used here as source area.
- By specifying 0.0.0.0/0, all IP addresses are allowed. This is necessary if, for example, when using the SSC, the remote subnet of the tunnel is not known in advance.
- The firewall rule shown is optional, because by default all packets coming from the VPN tunnel are always enabled for VLAN1.
  When using a different or additional VLAN, the rule is required.
- As source interface for firewall and NAT, either all tunnels ("IPSec all") or specific individual tunnels (via interface = "end point") can be enabled.
- This configuration corresponds to the functionality of SINEMA RC if the option "Device is network gateway" is not set. There is also a source NAT from the tunnel.

2.9 S7 Connection with Double NAT

Outset

The CPUs are to establish a S7 connection to each other. No gateway is configured in the modules and the hardware settings should not be changed. The S7 connection runs on an unchangeable port TCP 102.

Figure 2-27



Requirements

For network separation, SCALANCE S615 has two VLANs with different network IDs. Consequently, the device has a separate IP address for each VLAN (in this document: VLAN1: 192.168.2.1 and VLAN2: 192.168.1.1).

In addition, a source and destination NAT table is defined in SCALANCE S615 to rewrite the messages of the CPUs to another IP address. This requires another IP address from the subnet of VLAN2.

Procedure (active setup CPU2 to CPU1)

The additional NAT IP address 192.168.1.2 is occupied by SCALANCE S615.

The CPU2 addresses the local IP address 192.168.1.2 as destination.

Based on the definition in its NAT table the SCALANCE S615 replaces the source and destination IP address and sends the packet to the CPU1.

By changing the source IP address, from the point of view of CPU1, all packets from CPU2 come from the local subnet VLAN1. The CPU1 can therefore respond directly without gateway entry.

In all reply packets from CPU1 to CPU2 the source and destination IP address is automatically replaced.

Advantages

The advantage of the NAT table is that by using an additional address all ports can be forwarded or used.

No subsequent changes in the hardware configuration of the CPUs are required (non-reactive).

Disadvantages

The disadvantage is that only one active setup from CPU2 to CPU1 is possible. In addition, an additional IP address from the subnet of VLAN2 is required per plant section, each of which must be configured accordingly.

NAT and firewall rules

In the destination NAT table of SCALANCE S615, packets from VLAN2 with the destination IP address 192.168.1.2 are translated to the IP address of the CPU 192.168.2.20.

Figure 2-28

Type	Source Interface	Destination Interface	Source IP Subnet	Destination IP Subnet	Trans. Destination IP Subnet
Destination	vlan2	vlan1	192.168.**1.10**/32	192.168.**1.2**/32	192.168.**2.20**/32

With the NAT table of SCALANCE S615, packets with the source IP address 192.168.1.10 are translated to their own VLAN1 IP address 192.168.2.1.

Figure 2-29

Type	Source Interface	Destination Interface	Source IP Subnet	Trans. Source IP Subnet	Destination IP Subnet
Source	vlan2	vlan1	192.168.**1.10**/32	192.168.**2.1**/32	0.0.0.0/**0**

Communication between CPU2 (VLAN2) and CPU1 (VLAN1) must be allowed in the firewall. The services are limited to TCP port 102.

Figure 2-30

Action	From	To	Source (Range)	Destination (Range)	Service
Accept	vlan2	vlan1	192.168.**1.10**/32	192.168.**2.20**/32	Destination Port **102** TCP

Notes

- Address translation with source NAT is done only after the firewall, so the physical addresses must be used here.
- The destination NAT was done before the firewall, so the translated addresses must be used here.
- The "Trans.Destination IP Subnet" column in SCALANCE S615 may only be configured with a single IP address - i.e. /32. Only then does SCALANCE S615 also answer ARP requests for the additional IP addresses.

3 Information

3.1 General Principles

3.1.1 Classless Inter-Domain Routing (CIDR)

Description

As far as possible, the CIDR suffix notation is used for firewall and NAT configuration in the S615.

CIDR is a method that combines several IPv4 addresses into an address range by representing an IPv4 address combined with its subnet mask. For this purpose, a suffix "/x" is appended to the IPv4 address, which indicates the number ("x") of bits of the netmask set to "1".

The CIDR notation allows routing tables to be reduced and the available address ranges to be better utilized.

Example

IPv4 address 192.168.2.3 with subnet mask 255.255.255.0.

In the binary representation, the network part of the address comprises three times 8 bits, i.e. 24 bits. This results in the CIDR notation 192.168.2.0/24.

If all addresses are to be addressed, use the notation 0.0.0.0/0.

If only one address from the network is to be addressed (subnet mask 255.255.255.255), the notation is 192.168.2.3/32.

3.1.2 Connection Directions in the Network

Decisive for the configuration of the firewall and NAT is the direction of the connection setup and must therefore be defined in advance. A connection is always established actively by one node. The partner waits passively for an incoming connection. This defines the destination port (http on port 80, for example) for the connection setup.

The source port of the connection setup is usually dynamically managed by the operating system and not known in advance. Exceptions are, for example, native TCP/UDP connections between S7-CPUs or CPs where the source port is also fixed.

Note S7 connections always have the destination port TCP 102 and usually a dynamic source port.

3.1.3 The NAT Mechanisms

NAT

NAT (Network Address Translation) is a method for rewriting IP addresses in data packets. This permits two different networks (internal and external) to be connected with each other.

A difference is made between Source NAT, in which the source IP address is translated, and Destination NAT, in which the destination IP address is translated.

IP masquerading

IP masquerading is a simplified source NAT. For each outgoing data packet sent via this interface, the source IP address is replaced by the IP address of the interface. The modified data packet is sent to the destination IP address. For the destination host it looks like the requests always come from the same sender. The internal nodes cannot be accessed directly from the external network. With NAPT, the services of internal nodes can be made accessible via the external IP address of the device.

IP masquerading can be used if the internal IP addresses cannot or should not be forwarded externally, for example because the internal network structure must be hidden.

NAPT

NAPT (Network Address and Port Translation) is a form of destination NAT and is also known as port forwarding. This makes it possible to make services of internal nodes accessible from outside, which are hidden by IP masquerading or source NAT. Incoming data packets from the external network are translated and directed to an external IP address of the device (destination IP address). The destination IP address is replaced with the IP address of the internal node. Port translation is also possible in addition to address translation.

Source NAT

Like IP masquerading, source NAT rewrites the source IP address. Additionally the outgoing data packets can be limited. These include restrictions on certain IP addresses or IP address ranges and restrictions on certain interfaces. These rules can also be used on VPN connections. Source NAT can be used if the internal IP addresses cannot or should not be forwarded externally.

NETMAP

With NETMAP it is possible to translate complete subnets into another subnet. With this translation the subnet part of the IP address is changed and the host part remains the same. NETMAP requires only one rule for the translation. NETMAP can translate both the source IP address and the destination IP address. Many rules would be required to translate with destination NAT and source NAT. NETMAP can also be used on VPN connections.

3.1.4 Firewall and NAT

Firewall

The security functions of SCALANCE S615 include a stateful inspection firewall. This is a method of packet filtering or packet checking. The IP packets are checked against firewall rules that specify the following:

- The allowed protocols

- IP addresses and ports of allowed sources
- IP addresses and ports of allowed destinations

If an IP packet matches the specified parameters, it may pass the firewall. It is also defined how to handle IP packets that are not allowed to pass the firewall.

Simple packet filtering techniques require two firewall rules per connection.

- One rule for the request direction from source to destination.
- A second rule for the response direction from destination to source.

Stateful Inspection Firewall

With a stateful inspection firewall, on the other hand, you only need to assign one firewall rule for the request direction from the source to the destination. The second rule is added implicitly. The packet filter remembers when, for example, computer "A" communicates with computer "B" and only then allows responses to it. A request from computer "B" is therefore not possible without a previous request from computer "A".

Firewall and NAT

When NAT is configured, there is no automatic activation in the firewall. The settings for the NAT router and the firewall rules must be coordinated so that messages with a translated address can pass the firewall.

The order in which the messages pass through NAT and the firewall is important, as IP addresses/ports are changed depending on the NAT.

If a destination NAT is used, translation of the destination IP address and/or destination port takes place before passing the firewall.
Accordingly, the firewall rules must be created with the already changed IP addresses and ports.

When using a source NAT, the source IP address is translated after the firewall. The already changed IP address can no longer be filtered in the firewall.

Note An indication of the quantity framework of the rules can be found in the corresponding manuals.

3.2 S7 Connections and NAT

With S7 connections specified on both sides, the IP address of the partner is checked from both sides during setup.

Since NAT changes either the source or destination IP address, such a connection cannot work.

Instead a new connection with partner "Unspecified" must be created on both modules or alternatively a unilateral connection on resource 03 with PUT/GET.

With this setting, the IP address can be entered manually.
According to the NAT, the translated IP address with which the connection is received or sent must be used.

Rack and slot and connection resource are entered correspondingly in the address details. The "Local" values correspond inversely to the "Partner" entry for the other module.

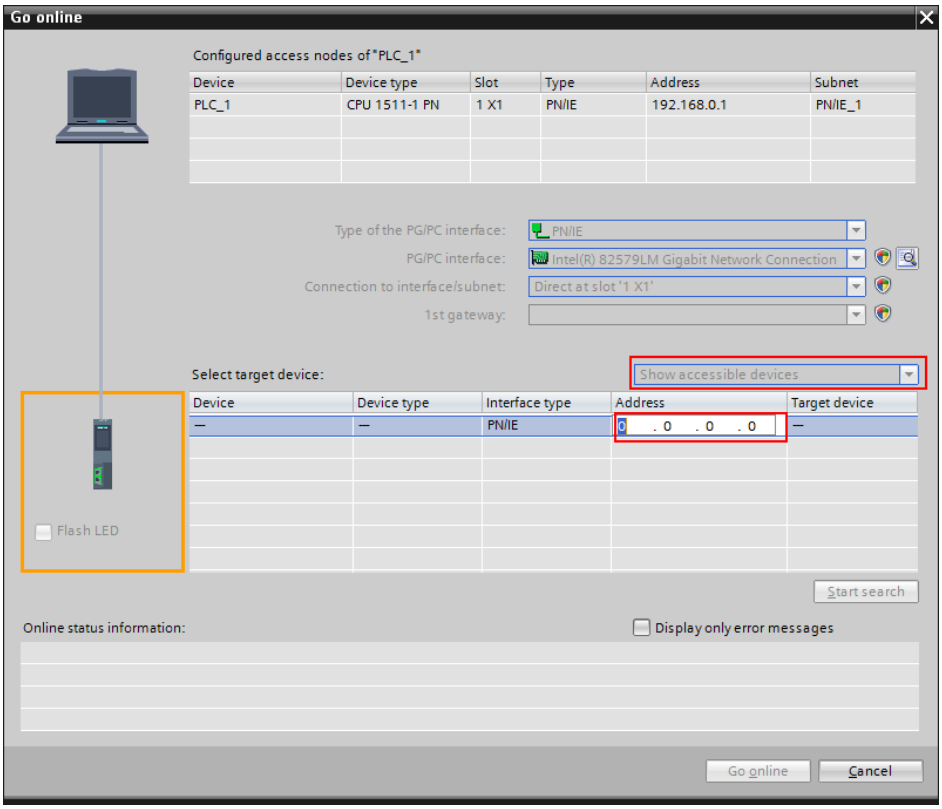
3.3 TIA Online Functions and NAT

Using Source NAT does not make a difference in the utilization of the TIA Online function because the PG connection is accepted by default by any IP addresses.

When using Destination NAT the IP address in the project no longer matches the IP address compiled by NAT via which the corresponding module can really be reached.

With the destination NAT, the translated NAT IP address to which the connection is to be established must therefore be specified in advance.

1. To do this, open the menu item "Online > Extended go online..." in TIA Portal.
2. Set the interface according to the PC or module interfaces used.
3. Set the selection to "Show accessible devices".
4. Click in the first empty row of the "Address" column. An input field appears in which you can enter the NAT IP address.



5. Then search for devices using the corresponding button.
6. If adding another IP address is suggested, reject it and click "Next".

4 Appendix

5 Appendix

5.1 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 – Training for Industry

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 Apple iOS, Android and Windows Phone:
support.industry.siemens.com/cs/ww/en/sc/2067

5.2 Links and literature

Table 5-1

No.	Topic
\1\	Siemens Industry Online Support https://support.industry.siemens.com
\2\	Link to the entry page of the application example https://support.industry.siemens.com/cs/ww/en/view/109744660
\3\	

5.3 Change Documentation

Table 5-2

Version	Date	Change
V1.0	02/2017	First edition
V1.1	08/2017	Section 2.4 and section 2.6 added
V1.2	04/2020	Section 2.4.1 and various elements added