SCALANCE 安全模块 NAT 原理介绍及配置指南

SCALANCE SC600 / 1.0 / NAT

https://support.industry.siemens.com/cs/ww/en/view/109804265

Siemens Industry Online Support

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

Security information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.
In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions only form one element of such a concept.
Customer is responsible to prevent unauthorized access to its plants, systems, machines and networks. Systems, machines and components should only be connected to the enterprise network or the internet if and to the extent necessary and with appropriate security measures (e.g. use of firewalls and network segmentation) in place.
Additionally, Siemens' guidance on appropriate security measures should be taken into account. For more information about industrial security, please visit http://www.siemens.com/industrialsecurity.

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

目录

1 概述

1.1 概述

SCALANCE 模块可以保护工业网络和自动化系统免于未授权的访问。

SCALANCE 安全模块由于其多层属性，可以被用于保护不同类型的网络拓扑，灵活地实现安全概念。

- VLAN 结构的可以提供防止 DoS 访问和对于未授权访问的保护。
- 通过防火墙和 VPN 可以提供对于设备和网络访问的保护。
- 通过配置 NAT 功能，工业网络或者自动化系统的 IP 地址可以实现对于外部网络的隐藏，此外，IP 地址范围可以用于多个连接的私有网络，而不产生地址冲突。

文档动机

使用 SCLANCE 安全模块作为路由器时，由于其同时支持通用的 NAT 机制，因此在访问被保护的内部网络或自动化系统时，存在多种访问的方式：

- 静态路由
- NAPT
- NAT
- NETMAP
- IP 伪装

原则上，静态路由比各种 NAT 类型的方式更好，NAT 需要考虑额外的组态以及调试操作。

然而，有些场景下无法通过路由的访问方式解决，例如，如果无法配置设备网关地址，那么此时，就需要通过 NAT 的访问方式实现。

文档内容

本文档描述了基于所选的常用场景的不同选项，介绍了基本情况和前提条件，优点和缺点同时也进行了重点描述。

本文目的是提供现有选项的概览，并为最常用的应用场景提供合适的解决方案。

下表列出了涉及到的细节：

表 1-1

	使用案例	选择的解决方案
1.	使用网关地址的双向通讯	标准路由
2.	不使用网关地址的 WEB 服务器访问 （PC 主动，CPU 被动）	NAPT
3.	不使用网关地址的多个 CPU 的 PG 功能访问	目的 NAT
4.	整个子网的 NAT	目的 NAT
5.	不使用网关地址的所有 CPU 的 PG 功能访问	目的 NAT
6.	相同系列机器设备上的 CPU 间的通讯	目的 NAT
7.	不使用网关地址的到控制系统的通讯连接（CPU 主动）	源 NAT
8.	通过 VPN 访问现存工厂网络但不修改现存设备配置	源 NAT
9.	通过 S7 通讯访问现存系统但不修改现存设备配置	源和目的 NAT

注意

文档中描述的这些功能对于模块的固件要求：SCALANCE S615/M-800 ≥ V06.02，SCALANCE SC-600 ≥02.00.01。请确保使用的模块中至少已经安装了足够高的固件。

以下描述同样适用于 SCALANCE M-800， SCALANCE SC-600 和 SCALANCE S615 几个系列产品。

2 通用原理

2.1 无类域内路由选择(CIDR)

介绍

在 SCALANCE S 的防火墙和 NAT 组态中，尽可能使用 CIDR 后缀表示法。

CIDR 是一个通过将 IP 地址及其子网掩码组合表示来将多个 Ipv4 地址组合成一个地址范围的方法。为了这个目的，将子网掩码位数作为后缀添加到 IPv4 地址后面。

CIDR 表示法可以用于表示可用的地址范围，因此可以用于减少路由表的表项数目。

例子

IPv4 地址 192.168.2.3， 其子网掩码为 255.255.255.0。

在其二进制表示中，其地址的网络部分包含 24 位，因此它的 CIDR 表示法为 192.168.2.0/24。

如果要寻址所有 IP 地址，可以使用表示法 0.0.0.0/0。

如果要寻址网络中的某一个地址（子网掩码 255.255.255.255），其 CIDR 表示法例如 192.168.2.3/32。

2.2 网络中连接方向

连接建立的方向决定了防火墙和 NAT 的配置内容，因此必须预定义连接的建立方向。连接通常是由某一端主动建立，伙伴会被动等待建立连接的请求。这就需要在连接建立过程中的目的端口（例如 HTTP 端口号 80）。

连接建立的源端口号通常是由操作系统动态分配的，并不是预知的。当然也有例外情况，例如对于 S7-CPU 或 CP 之间的 TCP/UDP 连接，源端口号也可以是固定的。

注意 对于 S7 连接，连接建立过程中，目的端口号使用 TCP 端口 102，源端口号通常是动态的。

2.3 NAT 机制

NAT

NAT (网络地址转换) 是一种修改数据包中的 IP 地址的方法。

这就允许两个不同的网络（内网和外网）互相连接在一起。

NAT 具有不同的方式，对于源 NAT，IP 数据包的源 IP 地址会被转换，对于目的 NAT，数据包中的目的 IP 地址会被转换。

IP 伪装

IP 伪装是一种简单的源 NAT。对于每个通过某个接口发出的数据包，其中的源 IP 地址会被接口的 IP 地址替换。修改之后的数据包会被发送给目的 IP 地址，对于目的主机的角度来看，通讯数据包总是来自于同一个发送者。内部节点无法在外部网络中被直接访问。

如果内部 IP 地址不能或者不必要向外部转发，例如由于必须要隐藏内部网络结构，此时可以使用 IP 伪装功能。

NAPT

NAPT (网络地址和端口转换)是一种目的 NAT 的形式，一般也称作端口转发。

如果使用了 IP 伪装或者源 NAT 隐藏了内部网络，通过 NAPT，可以使从外部访问内部节点的服务成为可能，从外部网络进入的数据包会被转换和定向至设备的外部 IP 地址（目的 IP 地址），目的地址接着会被替换成内部节点的 IP 地址，除了地址转换外，端口转换一般也是需要的。

源 NAT

就像 IP 伪装，源 NAT 会修改源 IP 地址，此外，发出的数据包会受到限制，一般包含对于特定 IP 地址或 IP 地址范围的限制以及特定接口的限制。这些规则也可用于 VPN 连接。如果内部 IP 地址不能或者不必要向外部转发，此时可以使用源 NAT 功能。

NETMAP

通过 NETMAP，可以将整个子网转换为其它的网段。通过子网的转换，IP 地址网络部分被转换，主机部分保持不变。NETMAP 转换仅需要一条规则即可实现，通过 NETMAP，源 IP 地址和目的 IP 地址都可以被转换。如果要通过目的 NAT 和源 NAT 的方式，相应地需要很多条规则才能实现转换。

NETMAP 也可以用于 VPN 连接。

2.4 防火墙和 NAT

防火墙

SCALANCE SC646-2C 的安全功能包含状态检测防火墙，它是基于包过滤或包检测的方式，IP 数据包通过以下定义的防火墙规则进行检查：

- 允许的协议
- 允许的源 IP 地址和端口号
- 允许的目的 IP 地址和端口号

如果 IP 数据包匹配了相应的参数，那么它可以通过防火墙。除了允许通过外，也可以定义不允许 IP 数据包通过防火墙。

简单的包过滤技术需要为每条连接定义两个方向的防火墙规则：

- 一条规则用于定义从源端到目的端方向的请求。
- 另一条规则用于从目的端到源端方向的响应。

状态检测防火墙

通过状态检测防火墙，换句话说，只需要为从源端到目的端的请求添加一条防火墙规则即可。第二条反向的规则会暗中添加。包过滤会记住连接建立的方向，例如计算机 A 主动建立与计算机 B 通讯时，仅会允许响应数据，如果有从计算机 B 发出的连接请求， 因此不可能通过防火墙。

防火墙和 NAT

当配置了 NAT 条目时，防火墙中不会自动激活，NAT 的设置和防火墙规则配置必须保持匹配，以便地址转换后的数据包能够通过防火墙。

数据包进行 NAT 转换和通过防火墙的顺序是很重要的，因为 IP 地址及端口号会根据 NAT 的配置发生改变。

如果使用目的 NAT，目的 IP 地址和端口号的转换会首先进行，然后再通过防火墙。

相应地，防火墙规则创建时，必须使用转换后的 IP 地址和端口号。

如果使用源 NAT，数据包会首先通过防火墙的检查，然后源 IP 地址才会进行转换，已经进行 IP 转换后的数据包不会再进行防火墙的过滤。

注意 防火墙规则数量限制可以在相应产品的手册中查询。

3 PLC 相关 NAT 通讯注意事项

3.1 S7 连接中的 NAT

当定义双边 S7 连接时，连接建立过程中，双方都需要检查伙伴的 IP 地址。

由于 NAT 会改变源或者目的 IP 地址，导致连接无法建立。

此时，可以在每一侧模块上通过选择伙伴“未指定”，分别创建新的连接，或者在某一侧创建单边 S7 连接，通过连接资源 03 实现 PUT/GET 通讯，通过这种设置，IP 地址可以手动填写。

根据 NAT 的要求，接收或发送连接建立请求中，需要使用转换的 IP 地址。

地址详细信息中需要相应地填写机架、插槽以及连接资源等信息，对于通讯双方来说，本地和伙伴侧的地址需要交叉对应填写。

3.2 TIA 在线中的 NAT

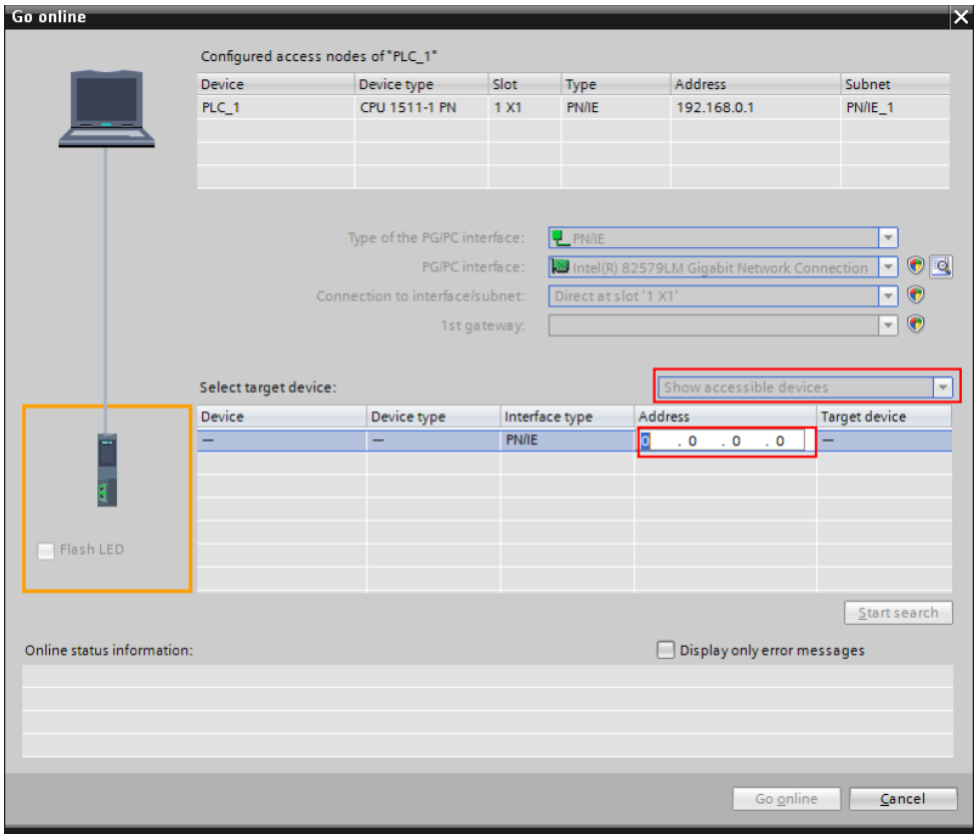
当使用 TIA 进行在线连接 PLC 时，源 NAT 不会产生任何影响，因为 PLC 默认会接受来自任何 IP 地址的连接。

当使用目的 NAT 时，项目中组态的设备的 IP 地址与 NAT 中配置的能够到达相应模块的 IP 地址是不一致的。

因此， 当使用目的 NAT 时，连接建立中用到的 NAT 转换 IP 地址需要预先定义：

1. 为此，在 TIA Portal 中打开菜单"在线" > "扩展的在线" 。
2. 根据 PC 连接到模块的方式选择相应的接口。
3. 设置并选择 "显示可访问的设备"。
4. 点击第一个空白行的“地址”列，一个输入框会出现，此时可以手动输入 NAT 的 IP 地址。

图 3-1



5. 然后使用下面的开始搜索按钮搜索设备。

6. 如果出现添加额外的 IP 地址的提示，拒绝并点击下一步。

4 常用应用场景介绍

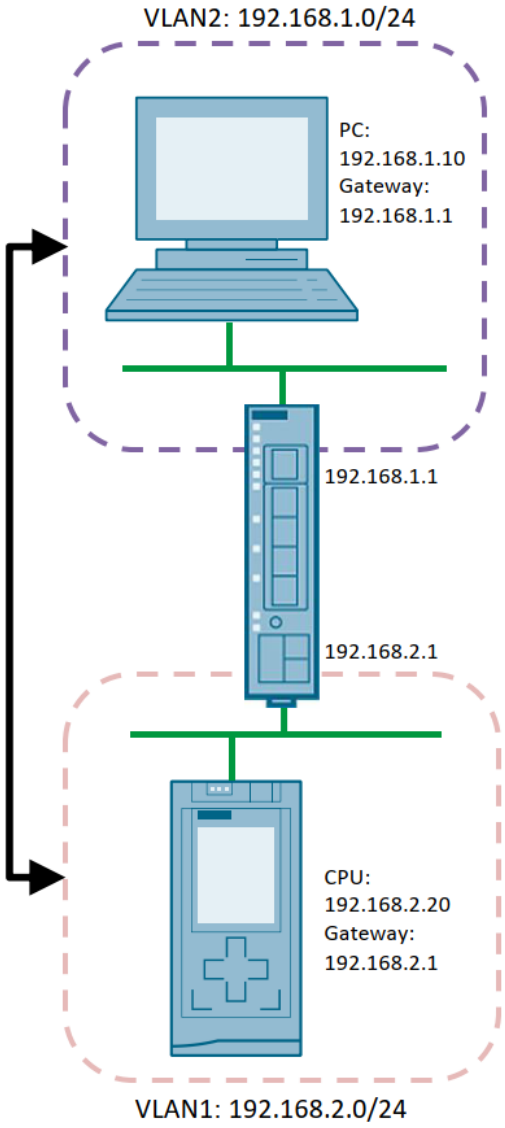
注意 本文档涉及到的基本原理和关于 NAT 功能的进一步信息可以参考章节 **Error! Reference source not found.**中的内容。

4.1 静态路由

应用场景示意

下图示例展示了 PC 机和 S7 CPU 间的双向通讯，通讯连接建立过程中的方向是双向的，即任意一侧设备均可发起建立主动连接。

图 4-1



要求

为了网络隔离，SCALANCE SC646-2C 配置了两个不同的 VLAN，因此，设备的每个 VLAN 具有不同子网的 IP 地址。

（本文示例中：VLAN1: 192.168.2.1，VLAN2: 192.168.1.1）

根据设备 VLAN 的划分，SCALANCE SC646-2C 两个 VLAN 的 IP 地址，必须在两侧配置为设备的网关地址（本文示例中的 PC 机或 S7 CPU）。

如果在 VLAN2 侧用到了额外的路由器，且需要通过这个路由器和 VLAN1 中的 CPU 通讯，那么 VLAN1 的子网必须保证在此路由器路由表中可达。

通讯过程（举例：CPU 到 PC 的主动连接）

对于 S7 CPU 来说，PC 的 IP 地址 192.168.1.10 通过本地子网是不可到达的，建立连接的数据包需要发送给网关。

SCALANCE SC646-2C 在子网 192.168.2.0 中有一个接口，它作为网关设备，将来自于 S7 CPU 的数据包直接转发给 PC。

从 PC 的角度来看，S7 CPU 的 IP 地址 192.168.2.20 不是本地子网，因此响应数据包也被发送给网关设备。

优势

这种应用场景的优势在于：

- 所有设备节点间的通讯连接建立可以是任意方向的。
- 每个节点可以通过唯一的 IP 地址被访问到。

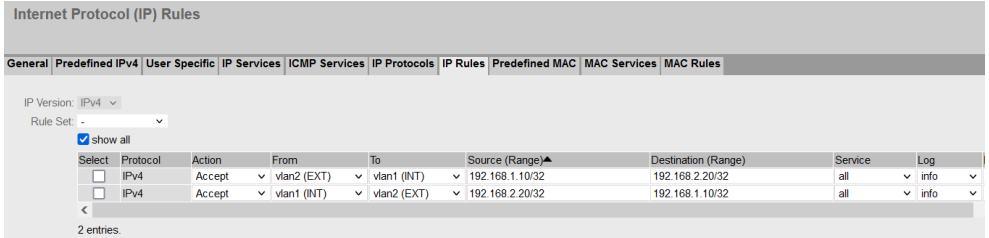
防火墙规则

在 SCALANCE SC646-2C 的防火墙功能选项下，允许两个 VLAN 间的双向通讯，规则如下所示：

图 4-2

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

图 4-3

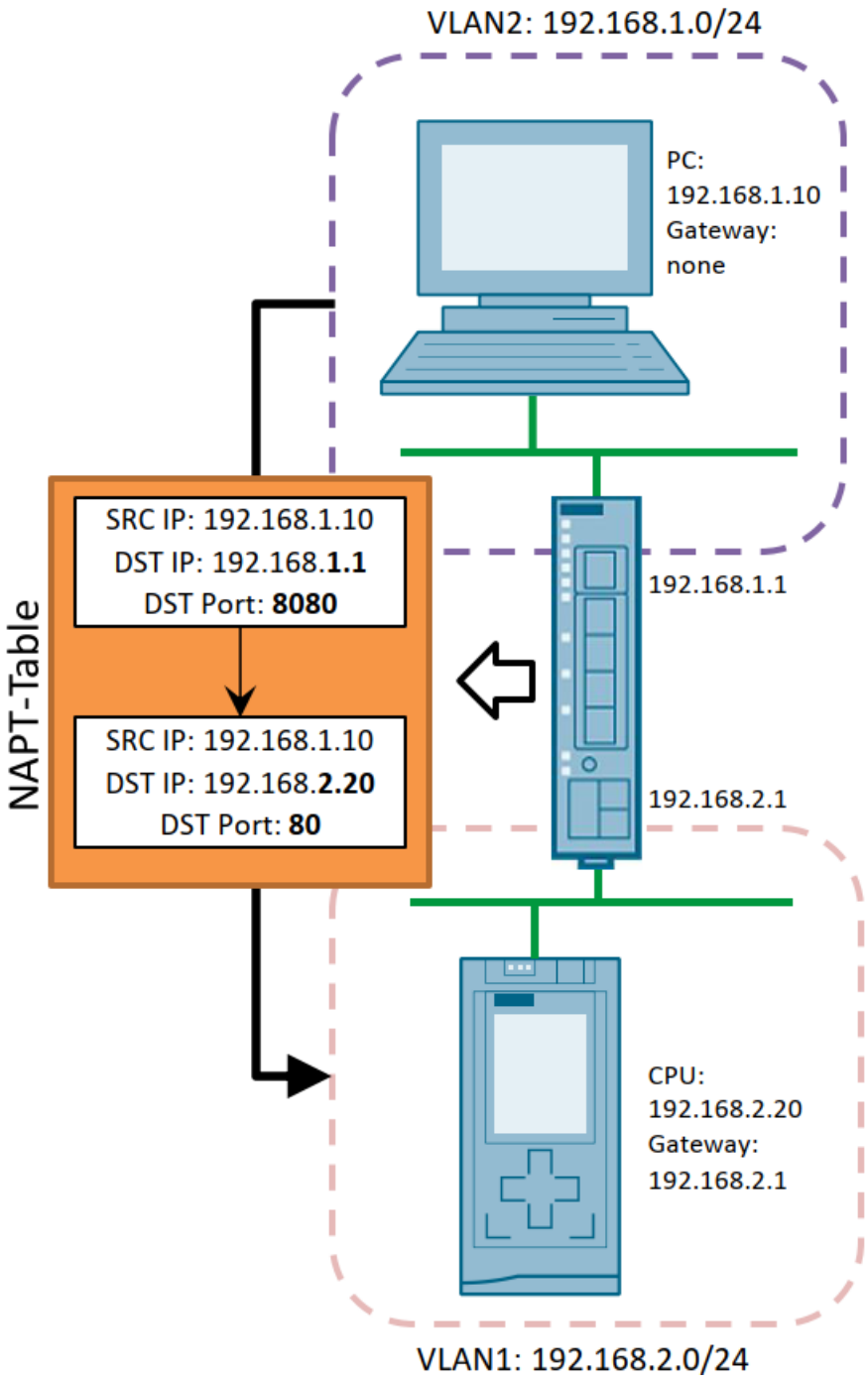


4.2 通过 NAPT 的 WEB 服务器访问

应用场景示意

在此应用场景下，PC 机需要能够无需配置网关地址即可访问 S7 CPU 的 WEB 服务器，访问的目的端口号不是必须固定的，可以在实际配置过程中进行调整。

图 4-4



要求

为了网络隔离，SCALANCE SC646-2C 配置了两个不同的 VLAN，因此，设备的每个 VLAN 具有不同子网的 IP 地址。

（本文示例中：VLAN1: 192.168.2.1，VLAN2: 192.168.1.1）

此外，在 SCALANCE SC646-2C 需要定义 NAPT 表，以便将 PC 发送的信息的目的 IP 地址替换成实际的设备的 IP 地址。

为了使 CPU 响应的数据包能够到达 VLAN2 中的 PC，必须在 CPU 的以太网参数配置中将 SCALANCE SC646-2C (VLAN1)的 IP 地址配置为 CPU 的网关地址。

通讯过程（PC 到 CPU 的主动连接）

PC 将 SCLANCE SC646-2C 的 IP 地址 192.168.1.1 和特定的端口号作为目的地址进行通讯，而不是实际的 CPU 的 IP 地址 192.168.2.20。

根据 NAPT 表的定义， SCALANCE SC646-2C 会将数据包中的目的 IP 地址和端口号替换成实际的 CPU 的 IP 地址和 WEB 服务器端口号，然后发送给 CPU。

源 IP 地址保持不变（本文示例中：192.168.1.10），从 CPU 的角度来看，数据包是来自于不同的子网，因此 CPU 需要额外设置网关地址（SCALANCE SC646-2C 中 VLAN1 接口的 IP 地址）。

在所有从 CPU 发向 PC 的响应数据包中，源 IP 地址 192.168.2.20 会根据 NAT 会话表自动地被替换为 192.168.1.1。

优势

这种应用场景的优势在于，在 PC 中无需额外的网关地址配置， SCALANCE SC646-2C 中与 PC 同一子网的接口的 IP 地址作为 PC 的目的地址，在 VLAN 2 中无需额外的 IP 配置。

劣势

这种应用场景的劣势在于，从 PC 到 CPU 建立主动连接的通讯时，每个端口的转发仅能配置一次。对于某些目的端口号固定的协议来说（例如 S7 协议），仅能访问 VLAN1 侧的一个节点。某些配置的转发端口（例如：HTTP，IPSec，SNMP 等）对于 SCALANCE SC646-2C 不再可用。

NAPT 和防火墙规则

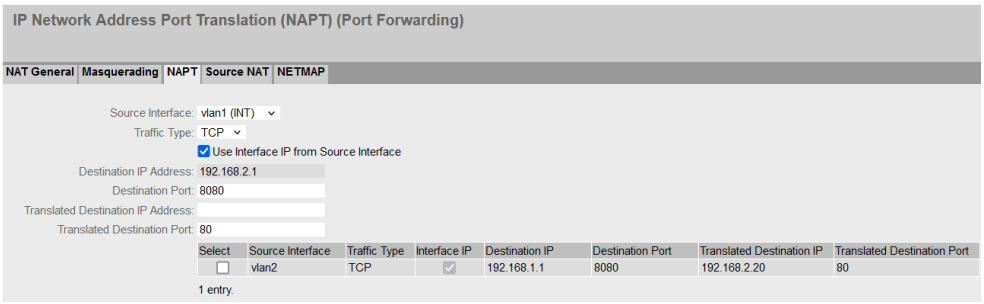
在 SCALANCE SC646-2C 的 NAPT 表中，来自于 VLAN2 的目的 IP 地址为 192.168.1.1:8080 的数据包，其目的 IP 和端口号会被转换为实际的 CPU 的地址及端口号 192.168.2.20:80， 端口号 80 是 CPU 的 WEB 服务器使用的端口。

NAPT 规则如下：

图 4-5

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

图 4-6

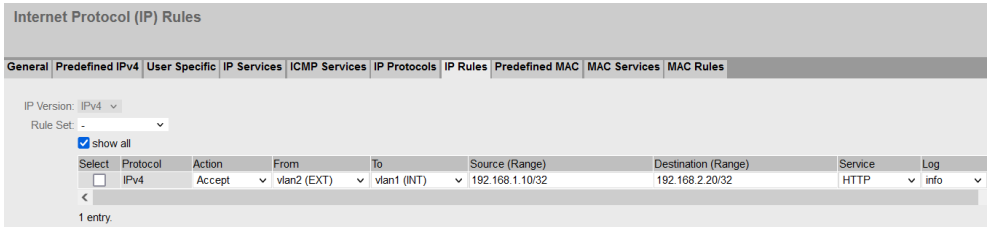


PC (VLAN2) 和 CPU (VLAN1)之间的通讯必须在防火墙配置中允许放行，配置防火墙规则如下：

图 4-7

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

图 4-8



注意

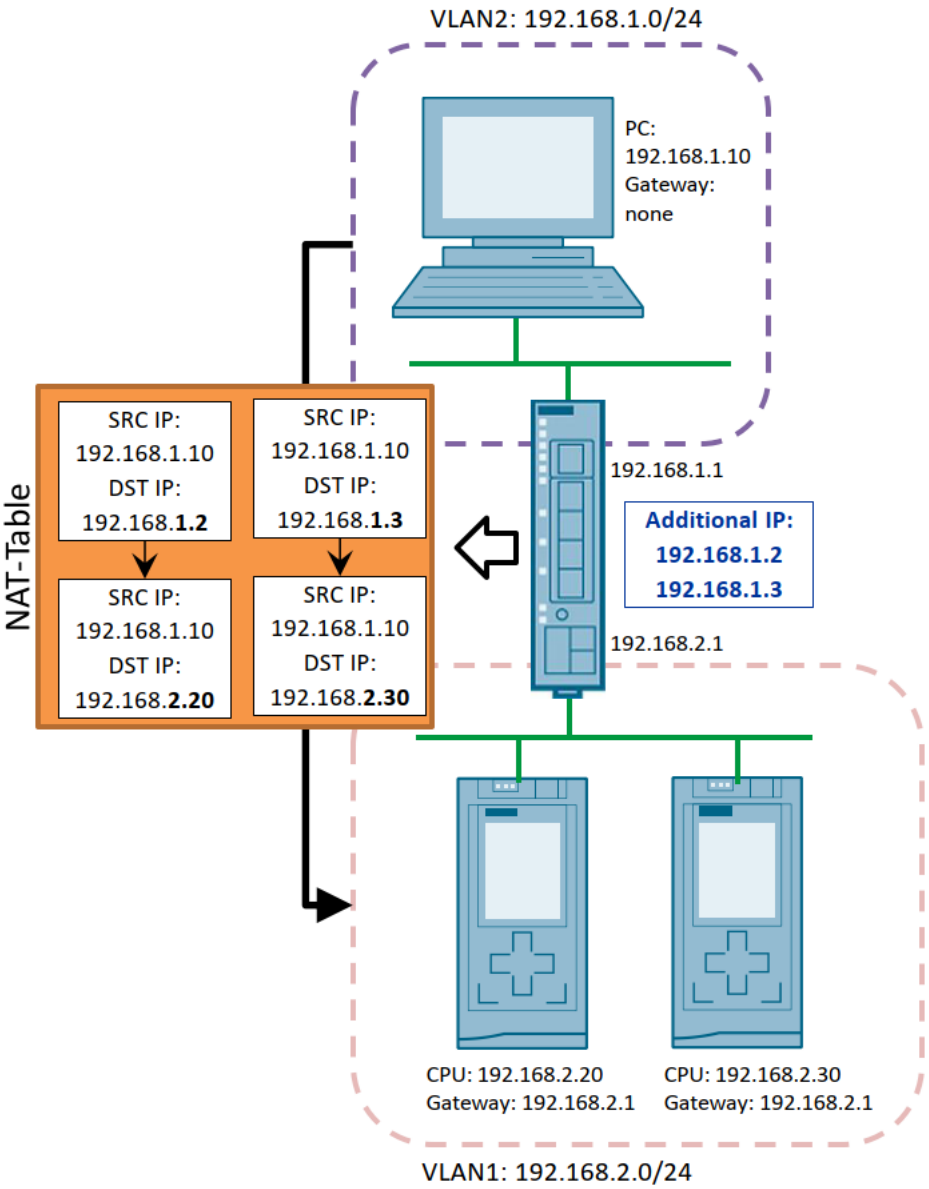
- NAPT 的地址转换会在防火墙规则检查前完成，所以在配置防火墙规则时，必须使用转换后的 IP 地址和端口号。
- 从 PC 机的角度来看，CPU 的 WEB 服务器可以通过 http://192.168.1.1:8080 来访问。
- 如果存在更多的 CPU， 可以通过使用不同的目的端口号来实现访问，例如 192.168.1.1:8081 -> 192.168.2.30:80。
- 如果要允许整个 VLAN2 的网段访问 CPU，那么防火墙的规则中的源地址需要修改为 192.168.1.0/24。
- 对于 NAPT 更常见的叫法是端口转发。

4.3 通过 NETMAP 和目的 NAT 实现的 PG 功能

应用场景示意

在此应用场景下，PC 机上能够无需配置网关地址，即可实现通过 STEP7 的 PG 功能访问多个 S7 CPU，STEP7 的 PG 功能是基于 S7 协议实现的，具有无法更改的目的 TCP 端口 102。

图 2-9



要求

为了网络隔离，SCALANCE SC646-2C 配置了两个不同的 VLAN，因此，设备的每个 VLAN 具有不同子网的 IP 地址。

（本文示例中：VLAN1: 192.168.2.1，VLAN2: 192.168.1.1）

在 SCALANCE SC646-2C 中需要额外定义 NAT 表，以便将 PC 发送的信息的目的 IP 地址替换成实际的设备的 IP 地址。这需要 VLAN2 子网中两个额外的未使用的 IP 地址。

为了使所有的 CPU 响应的数据包能够到达 VLAN2 中的 PC，必须在 CPU 的以太网参数配置中将 SCALANCE SC646-2C (VLAN1)的 IP 地址配置为 CPU 的网关地址。

通讯过程（PC 到 CPU 的主动连接）

SCALANCE SC646-2C 需要占用两个额外的 IP 地址 192.168.1.2 和 192.168.1.3 用于 NAT 功能。

PC 将使用本地网段的 IP 地址 192.168.1.2 或 192.168.1.3 作为目的地址进行通讯。

根据 NAT 表的定义， SCALANCE SC646-2C 会将数据包中的目的 IP 地址替换成实际的 CPU 的 IP 地址，然后将数据包发送给 CPU1 或者 CPU2。

源 IP 地址保持不变（本文示例中：192.168.1.10），从 CPU 的角度来看，数据包是来自于不同的子网，因此 CPU 需要额外设置网关地址（SCALANCE SC646-2C 中 VLAN1 接口的 IP 地址）。

在所有从 CPU 发向 PC 的响应数据包中，源 IP 地址 192.168.2.20（或者 192.168.2.30）会根据 NAT 会话表自动地被替换为 192.168.1.2（或者 192.168.1.3）。

优势

这种应用场景的优势在于，为每个 CPU 配置独立的 NAT 条目和 IP 地址，到每个 CPU 的所有端口的访问的数据包均可转发。

劣势

这种应用场景的劣势在于，仅能建立从 PC 到某个 CPU 的主动连接。

访问每个 CPU 都需要额外占用 VLAN2 子网中的 IP 地址，每个 IP 地址都必须相应地进行配置。

NAT 和防火墙规则

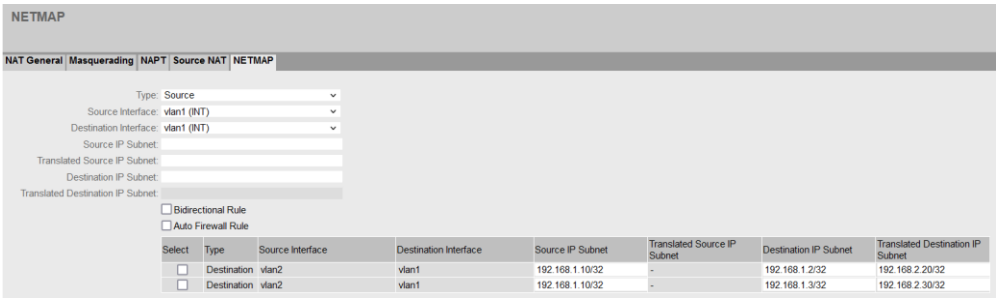
在 SCALANCE SC646-2C 的 NAT 表中，来自于 VLAN2 的目的 IP 地址为 192.168.1.2（或 192.168.1.3）的数据包，其目的 IP 会被转换为实际的 CPU 的地址 192.168.2.20（或 192.168.2.30），

NAT 规则如下：

图 4-10

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

图 4-11



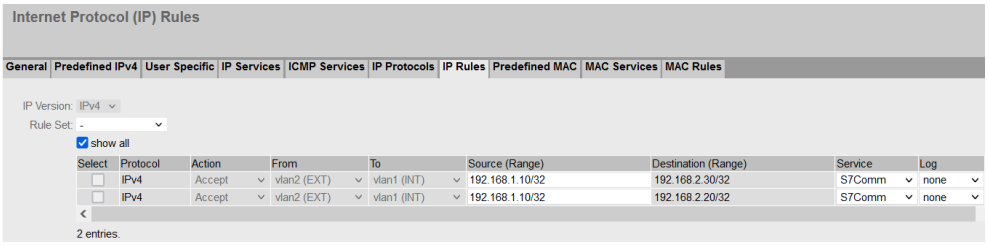
PC (VLAN2) 和所有 CPU (VLAN1)之间的通讯必须在防火墙配置中允许放行，服务选项限制仅使用 TCP 端口号 102，因为 STEP7 PG 功能是基于 S7 连接的。

配置防火墙规则如下：

图 4-12

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

图 4-13



NETMAP 双向/自动防火墙规则

为了简化配置，NETMAP 提供两个额外的选项：

- 通过双向规则选项，相应的反方向的 NAT 条目可以被自动创建，其使用相应的反方向的 IP 地址。

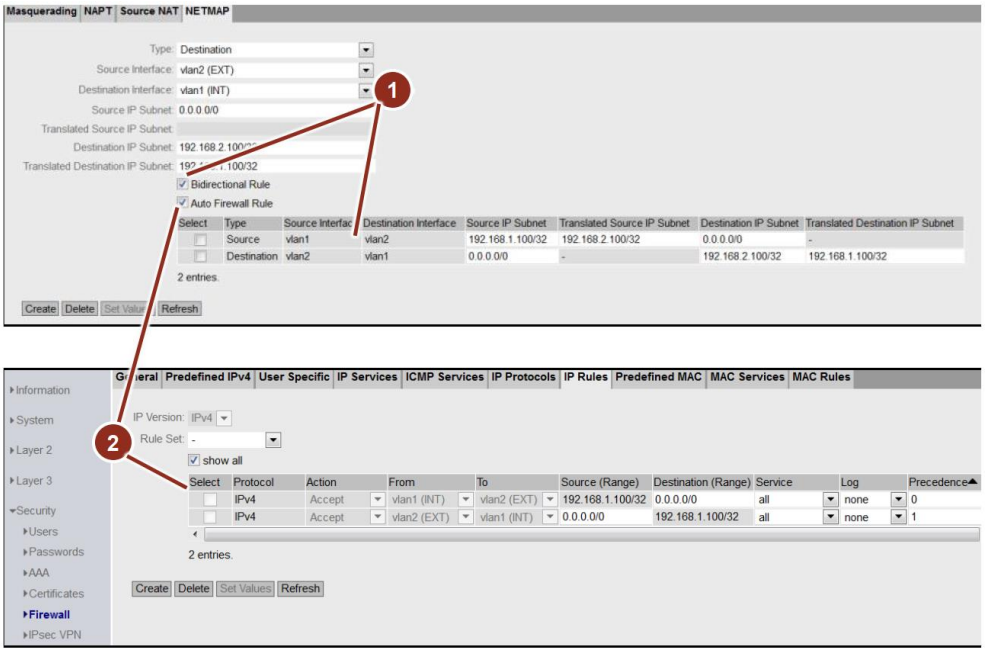
- 通过自动防火墙规则选项，相应的 NAT 条目的防火墙规则也可以自动被创建，防火墙条目会自动采用 NAT 中的 IP 地址。根据 NAT 的类型，源或者目的 IP 地址可以手动限制，如果用户改变了 NAT 条目中的 IP 地址，防火墙规则会自动随之修改。自动防火墙规则不能被手动删除，除非相应的 NAT 条目被删除。

注意

"Bidirectional Rule" 和 "Auto Firewall Rule" 功能使得配置变得更加容易。

建议配置时使用这两个选项。

图 4-14



注意

- 目的 NAT 的地址转换会在防火墙规则检查前完成，所以在配置防火墙规则时，必须使用转换后的 IP 地址。
- 从 PC（或者 STEP7）的角度来看，通过 IP 地址 192.168.1.2 和 192.168.1.3 来分别访问两个 CPU。
- 如果要允许整个 VLAN2 的网段访问 CPU，那么 NAT 规则和防火墙规则中的源地址需要修改为 192.168.1.0/24。
- NAPT 配置也可以用于访问 CPU，但仅能用于单个 CPU（参见 4.2 章节）。
- 通过 NETMAP，多个地址可以被转换成相同数量的其它网段的地址-也被称作 1:1 NAT。

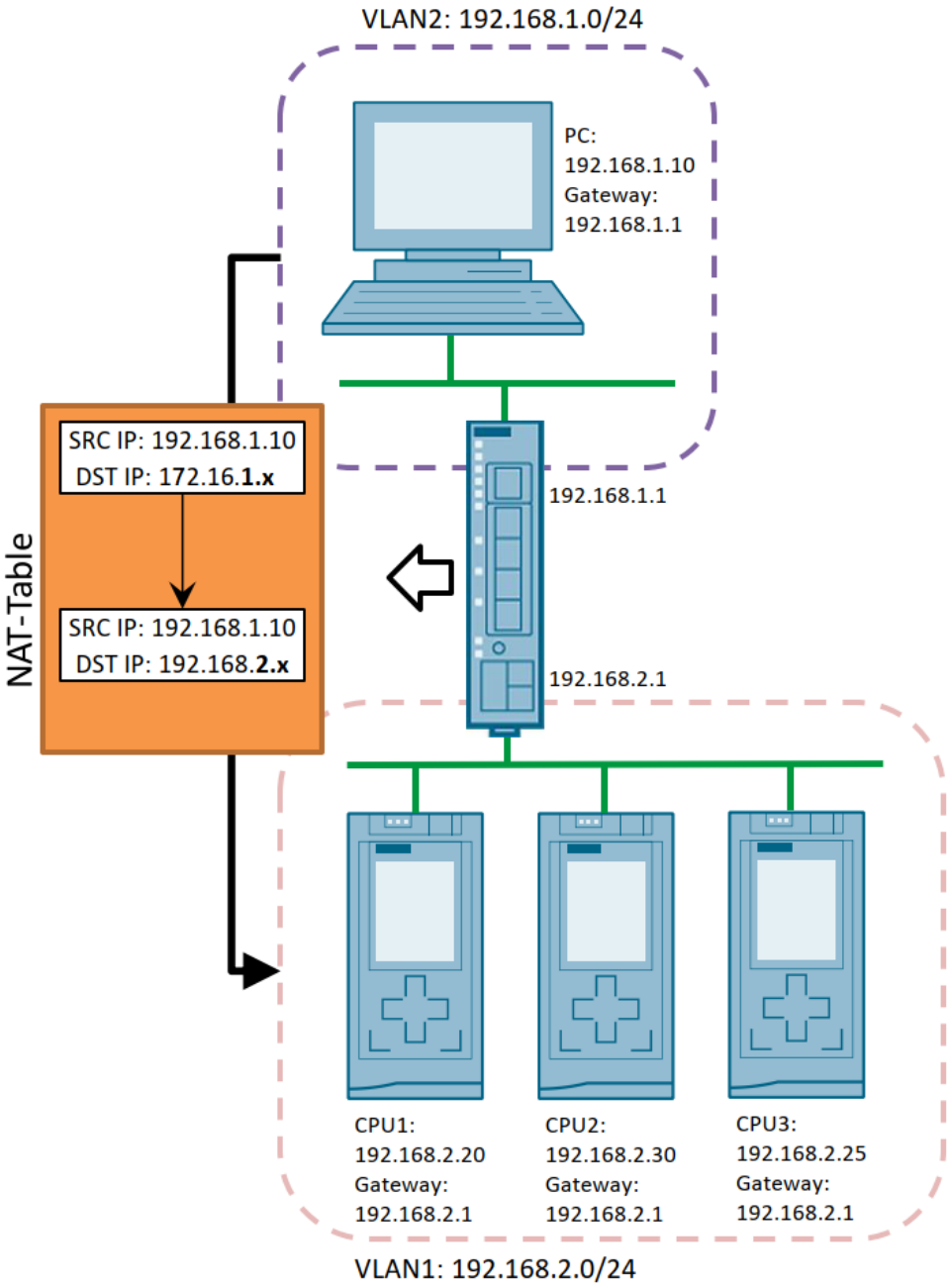
- 在 SCALANCE SC646-2C 中，"Destination IP Subnet"列中可以只配置单个 IP 地址，此时掩码位设置为/32，只有如此设置，SCALANCE SC646-2C 才会响应对于添加的 IP 地址的 ARP 请求。

4.4 通过 NETMAP 和目的 NAT 实现整个子网的地址转换

应用场景示意

在此应用场景下，PC 机需要能够与自动化网络中的多个或所有设备进行通讯，访问的目的端口号不是必须固定的，可以在实际配置过程中进行调整。

图 4-15



要求

为了网络隔离，SCALANCE SC646-2C 配置了两个不同的 VLAN，因此，设备的每个 VLAN 具有不同子网的 IP 地址。

（本文示例中：VLAN1: 192.168.2.1，VLAN2: 192.168.1.1）

在 SCALANCE SC646-2C 中需要额外定义 NAT 表，以便将 PC 发送的信息的目的 IP 地址替换成实际的设备的 IP 地址。这需要配置额外的未使用的虚拟子网（本文示例中：172.16.1.0/24）。此外，这个虚拟子网仅存在于 SCALANCE S 中，它是可以自由配置的且与 VLAN1 的子网完全无关的。

根据 VLAN 划分及子网 IP 设置，必须在终端设备（本文示例中：PC 或 S7 CPU）的以太网配置中将 SCALANCE SC646-2C 的 IP 地址配置为其网关地址。

通讯过程（PC 到 CPU 的主动连接）

SCALANCE SC646-2C 需要占用额外的子网 172.16.1.0/24，它使用 NETMAP 功能实现地址转换，通过 NETMAP，它可以将完整的子网转换为另一个子网。两个子网中的地址 1:1 进行转换。

下表中列出了应用例子中的转换结果：

表 4-1

目标 IP 地址	虚拟 NAT IP 地址
192.168.2.20	172.16.1.20
192.168.2.30	172.16.1.30
192.168.2.25	172.16.1.25

对于 PC 来说，由于目的 IP 地址（本文示例中：172.16.1.20）与其自身 IP 地址处于不同网段，所以 PC 会通过路由方式将通讯数据发送给其配置的网关，即 SCALACNE。

基于 NAT 表中的配置，SCALANCE SC646-2C 会将目的 IP 地址替换为 192.168.2.20，然后将报文发送给 CPU1。

源 IP 地址保持不变（本文示例中：192.168.1.10），从 CPU 的角度来看，数据包是来自于不同的子网，因此 CPU 需要额外设置网关地址（SCALANCE SC646-2C 中 VLAN1 接口的 IP 地址）。

在所有从 CPU 发向 PC 的响应数据包中，源 IP 地址 192.168.2.x 会根据 NAT 会话表自动地被替换为 172.16.1.x。

优势

这种应用场景的优势在于，访问每个 CPU 使用额外的 IP 地址，到每个 CPU 的所有端口的访问的数据包均可转发。1:1 地址转换的方式简化了 NAT 的配置，因为在 NAT 表中仅需配置一行即可。

劣势

这种应用场景的劣势在于，到虚拟子网的路由必须已知。虚拟 NAT 子网的 IP 地址无法被直接寻址。

NAT 和防火墙规则

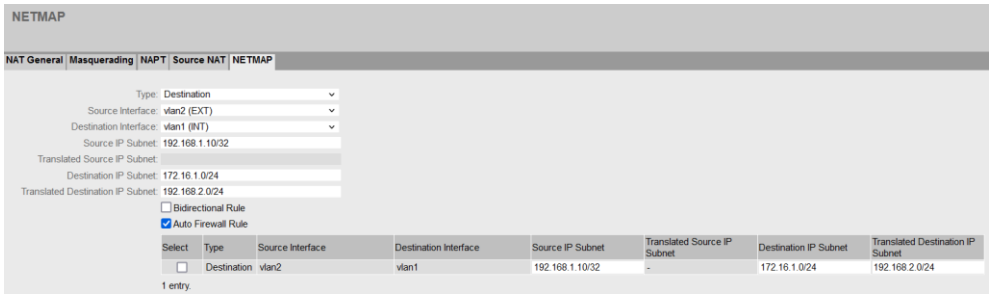
在 SCALANCE SC646-2C 的 NAT 表中，通讯报文中的 172.16.1.0/24 子网中的目标 IP 地址会被转换为 VLAN1 子网中的 IP 地址，转换是基于 1:1 的关系完成。

NAT 规则如下：

图 4-16

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**

图 4-17



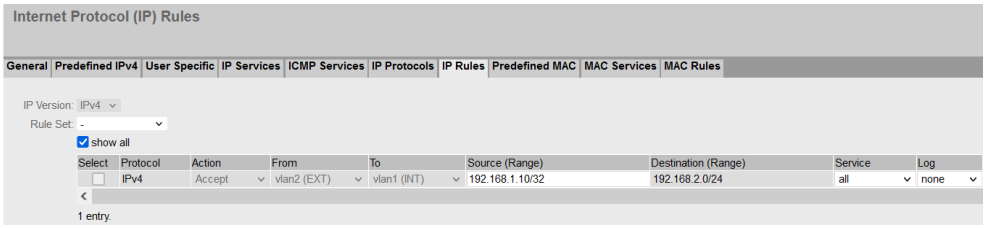
PC (VLAN2) 和所有 CPU (VLAN1)之间的通讯必须在防火墙配置中允许放行。

配置防火墙规则如下：

图 4-18

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

图 4-19



注意

- 目的 NAT 的地址转换会在防火墙规则检查前完成，所以在配置防火墙规则时，必须使用转换后的 IP 地址。
- 如果要允许整个 VLAN2 的网段访问所有 CPU 或自动化设备，那么 NAT 规则和防火墙规则中的源地址需要修改为 192.168.1.0/24。
- 虚拟子网段 172.16.1.x 上的 IP 地址不会响应 ARP 请求，因此，这些 IP 仅能通过路由访问到。
- NAPT 配置也可以用于访问 CPU，但仅能用于单个 CPU（参见 4.2 章节）。
- 通过 NETMAP，多个地址可以被转换成相同数量的其它网段的地址-也被称作 1:1 NAT。
- NETMAP 配置中的子网必须涵盖相同的范围，例如子网掩码位数都设置为 24 位：/24

4.4.1 NETMAP 虚拟子网

要求

- SCALANCE SC646-2C VLAN 接口的 IP 地址必须相应地在设备（本文示例中的 PC 机或 S7 CPU）中配置为它们的网关地址。
- 虚拟子网必须是可以通过路由到达的（例如，对于本文例子中的 PC，可以通过其默认路由到达）。
- NAT 转换表中的虚拟子网和实际物理子网必须具有相同的范围，能够实现 1:1 的转换。

通讯过程（双向的的主动连接）

- PC 会通过路由方式寻址虚拟子网 172.16.1.X 中的 IP 地址，因此会将通讯数据发送给其配置的网关，即 SCALANCE。

- SCALANCE SC646-2C 会将虚拟子网中的 IP 地址与 VLAN1 中的实际 IP 地址进行 1 对 1 的转换：172.16.1.1 > 192.168.2.1，172.16.1.2 > 192.168.2.2，172.16.1.x > 192.168.2.x
- 如果通讯过程中，CPU 主动建立连接，会在上述的相反方向进行类似的转换。

优势

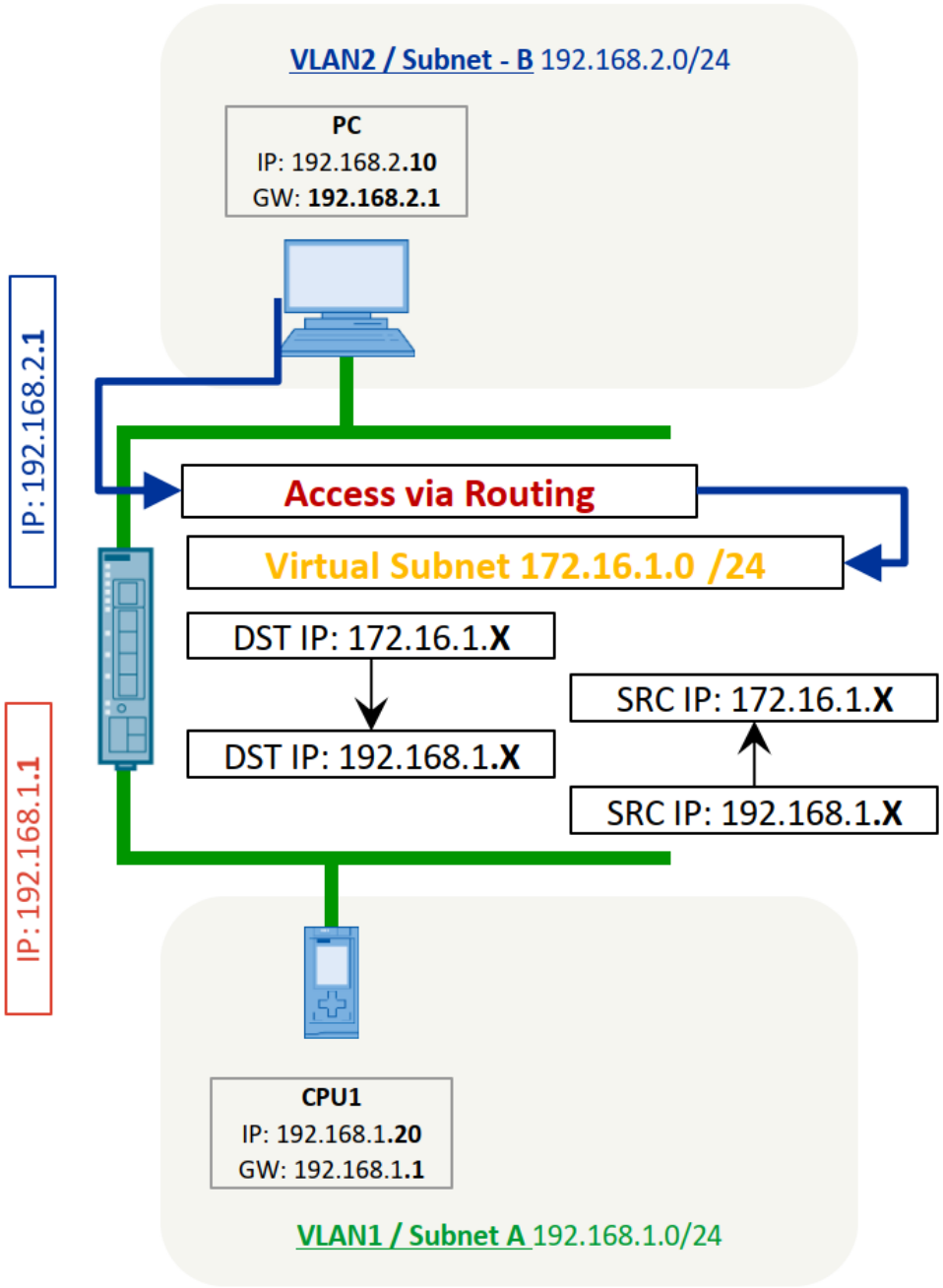
这种应用场景的优势在于：

- 不需要占用 VLAN2 中的其它 IP 地址。
- 虚拟子网是可以自由选择的，不通过路由，虚拟子网的 IP 地址在网络上是不可见的。
- NETMAP 配置中仅需要一行即可简单地实现整个子网的转换。
- 在 PC 中无需额外的网关地址配置， SCALANCE SC646-2C 中与 PC 同一子网的接口的 IP 地址作为 PC 的目的地址，在 VLAN 2 中无需额外的 IP 配置。
- 由于地址没有被实际占用，因此 NAT 可以与 VRRP 组合使用。

劣势

这种应用场景的优势在于，虚拟子网必须可以通过路由方式访问到。

图 4-20



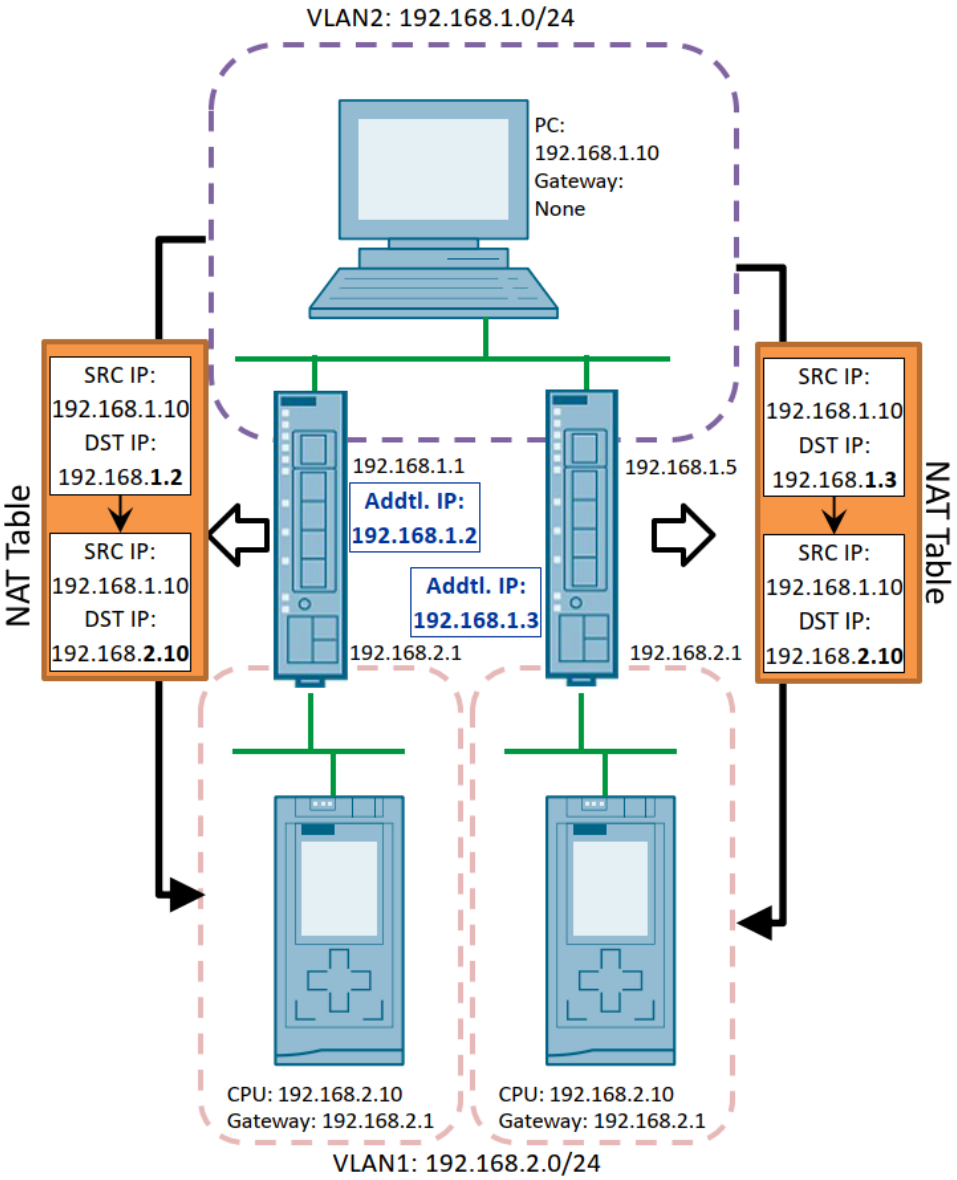
4.5 通过 NETMAP 和目的 NAT 实现 PC 到相同系列机器设备上的 CPU 间的通讯

应用场景示意

在此应用场景下，PC 机需要能够访问到多个完全相同的机器设备，对于这些机器设备，它们使用相同的子网（本文示例中：192.168.2.x）。

PC 机能够无需配置网关地址即可访问到这些设备上的每个 CPU，同时执行任何通讯功能。

图 4-21



要求

每个机器设备上都需要有一个 SCALANCE SC646-2C 进行互连。

为了网络隔离，SCALANCE SC646-2C 配置了两个不同的 VLAN，因此，设备的每个 VLAN 具有不同子网的 IP 地址。

（本文示例中：VLAN1: 192.168.2.1，VLAN2: 192.168.1.1 或者 192.168.1.5）

每个 SCALANCE SC646-2C 的 VLAN2 接口与 PC 互连。

这种场景无法靠纯路由的方式实现，而必须依靠 NAT 功能，因为 VLAN1 的子网不是唯一的，与连接建立的方向或者是否为 PC 设置网关无关。

每个相同的内部子网都需要一个 SCALANCE SC646-2C 模块，而不能同时将多个相同子网连接至一个 SCALANCE SC646-2C 上。

这就意味着在 SCALANCE SC646-2C 中需要额外定义 NAT 表，以便将 PC 发送的信息的目的 IP 地址替换成实际的设备的 IP 地址。这需要占用 VLAN2 子网中额外的未使用的 IP 地址。

为了使所有的 CPU 响应的数据包能够返回到 VLAN2 中的 PC，必须在 CPU 的以太网参数配置中将 SCALANCE SC646-2C (VLAN1)的 IP 地址配置为 CPU 的网关地址。

通讯过程（PC 到 CPU 的主动连接）

本应用例子中的两个 SCALANCE SC646-2C 需要占用两个额外的 IP 地址 192.168.1.2 和 192.168.1.3 用于 NAT 功能。

PC 将使用本地网段的 IP 地址 192.168.1.2 或 192.168.1.3 作为目的地址进行通讯。

根据 NAT 表的定义， 相应的 SCALANCE SC646-2C 会将数据包中的目的 IP 地址替换成实际的 CPU 的 IP 地址，然后将数据包发送给 CPU1 或者 CPU2。

源 IP 地址保持不变（本文示例中：192.168.1.10），从 CPU 的角度来看，数据包是来自于不同的子网，因此 CPU 需要额外设置网关地址（相应的 SCALANCE SC646-2C 中 VLAN1 接口的 IP 地址）。.

在所有从 CPU 发向 PC 的响应数据包中，源 IP 地址 192.168.2.10 会根据 NAT 会话表自动地被替换为 192.168.1.2（或者 192.168.1.3）。

优势

这种应用场景的优势在于，为每个 CPU 配置独立的 NAT 条目和 IP 地址，到每个 CPU 的所有端口的访问的数据包均可转发。

劣势

这种应用场景的劣势在于，仅能建立从 PC 到某个 CPU 的主动连接。

访问每个配置相同的机器设备上的 CPU 时，都需要额外占用 VLAN2 子网中的 IP 地址，每个 IP 地址都必须相应地进行配置。

NAT 和防火墙规则

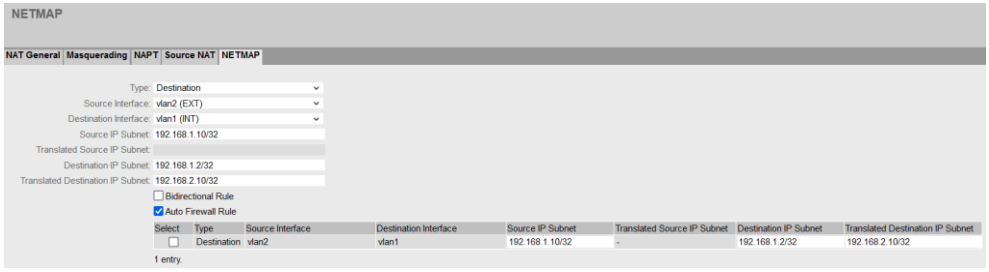
在第一个设备对应的 SCALANCE SC646-2C 的 NAT 表中，来自于 VLAN2 的目的 IP 地址为 192.168.1.2 的数据包，其目的 IP 会被转换为实际的 CPU 的地址 192.168.2.10.

NAT 规则如下：

图 4-22

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

图 4-23



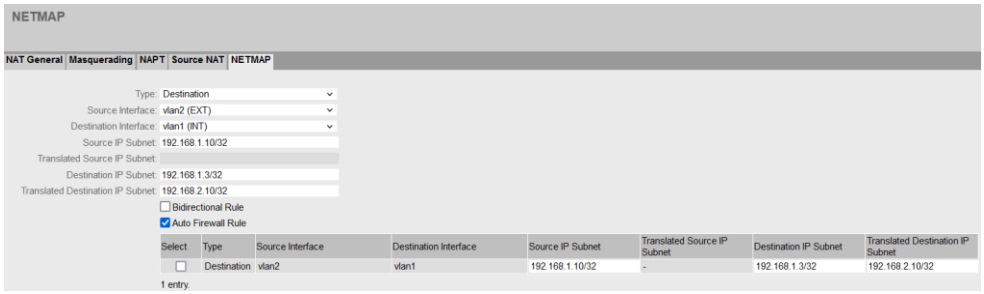
在第二个设备对应的 SCALANCE SC646-2C 的 NAT 表中，来自于 VLAN2 的目的 IP 地址为 192.168.1.3 的数据包，其目的 IP 会被转换为实际的 CPU 的地址 192.168.2.10.

NAT 规则如下：

图 4-24

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

图 4-25



所有 SCALANCE SC646-2C 的防火墙规则是相同的，因为对应的 VLAN1 内网中连接的 CPU 的 IP 地址是相同的。

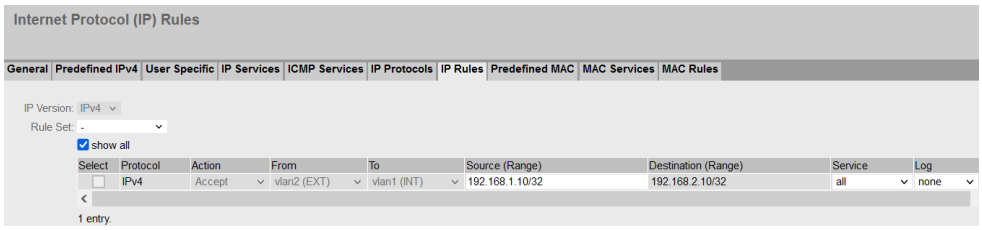
PC (VLAN2) 和所有 CPU (VLAN1)之间的通讯必须在防火墙配置中允许放行，由于可能建立任意类型的通讯连接，所以没有对通讯端口进行限制。

配置防火墙规则如下：

图 4-26

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

图 4-27



注意

- 目的 NAT 的地址转换会在防火墙规则检查前完成，所以在配置防火墙规则时，必须使用转换后的 IP 地址。
- 从 PC（或者 STEP7）的角度来看，可以通过 IP 地址 192.168.1.2 和 192.168.1.3 来分别访问两个 CPU。这就实现了与这两个 CPU 的通讯，即使它们在各自的 VLAN1 中具有相同的子网 IP 地址。

- 如果要允许整个 VLAN2 的网段访问 CPU，那么 NAT 规则和防火墙规则中的源地址需要修改为 192.168.1.0/24。
- 通过 NETMAP，多个地址可以被转换成相同数量的其它网段的地址-也被称作 1:1 NAT。
- 在 SCALANCE SC646-2C 中，"Destination IP Subnet"列中可以只配置单个 IP 地址，此时掩码位设置为/32，只有如此设置，SCALANCE SC646-2C 才会响应对于添加的 IP 地址的 ARP 请求。

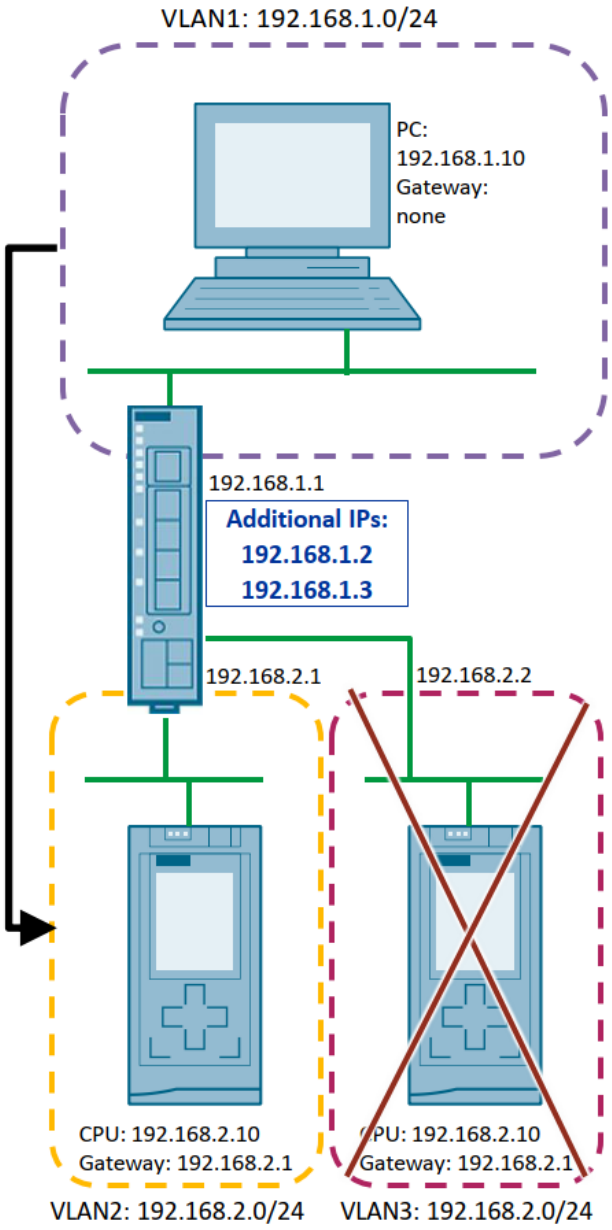
限制

本应用场景中不可能仅使用一个 SCALANCE S 模块实现，将相同子网 IP 的设备连接到这个 SCALANCE S 模块不同的 VLAN 上。

即使在 SCALANCE S 上创建 VLAN2 和 VLAN3 这两个 VLAN，用于分别连接两个相同子网 IP 的设备，也没有办法为这两个 VLAN 接口分配相同网段的子网 IP。

假设能够在一个 SCALANCE S 模块上为两个 VLAN 接口分配相同网段的子网 IP，在实际通讯过程中，在数据包路由处理阶段，SCALANCE S 模块需要根据路由表决定数据包从那个接口发出，由于模块上存在两个相同网段 192.168.2.0/24 的 VLAN 接口，会导致路由表中存在两条相同的路由条目，这种情况下，仅有一条生效，另一条不起作用。

图 2-28

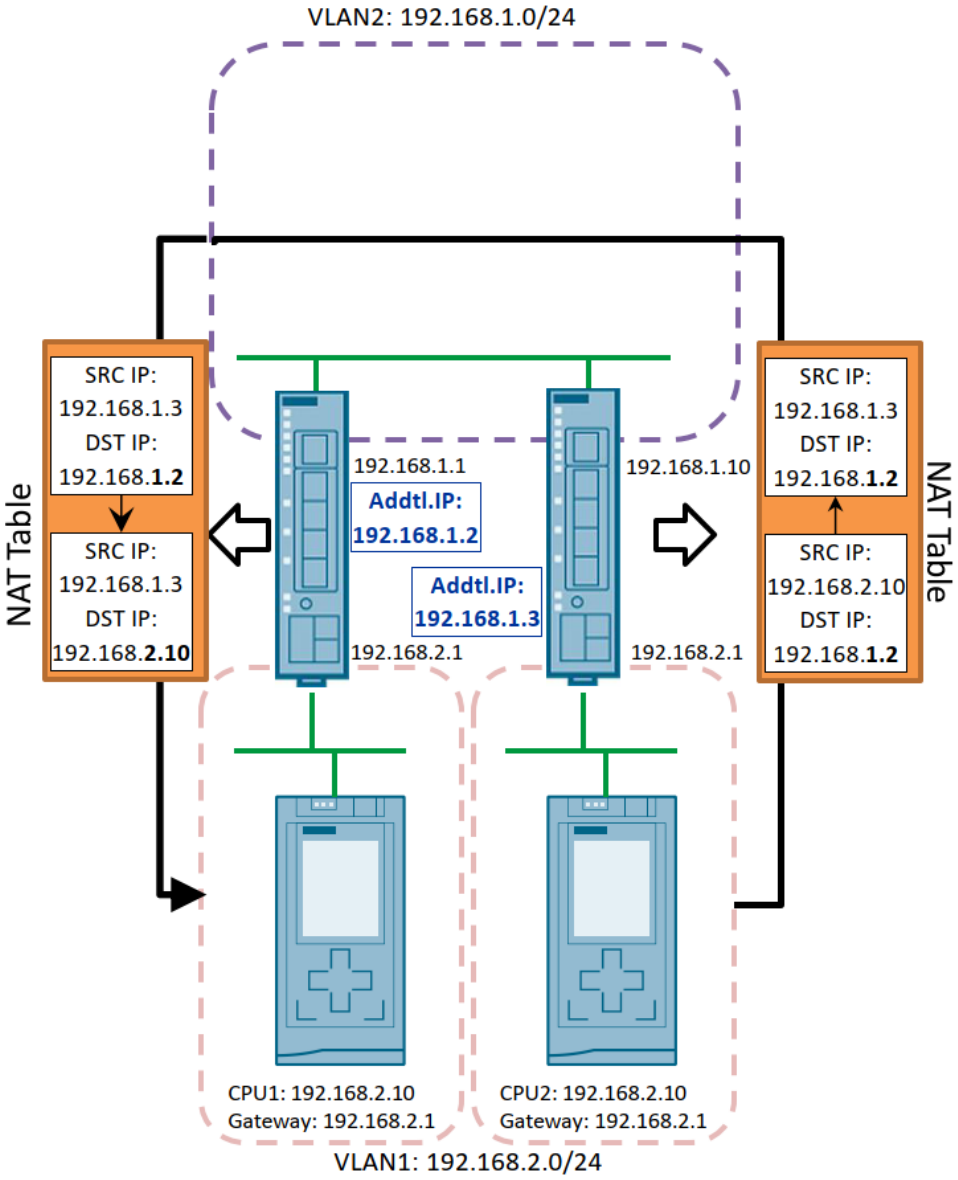


4.6 通过 NETMAP 和目的 NAT 实现相同系列机器设备上的 CPU 之间的通讯

应用场景示意

在此应用场景下，多个完全相同的机器设备之间（本文示例中：CPU1 和 CPU2）可以实现互相通讯，对于这些机器设备，它们使用相同的子网（本文示例中：192.168.2.x）。

图 4-29



要求

每个机器设备上都需要有一个 SCALANCE SC646-2C 进行互连。

为了网络隔离，SCALANCE SC646-2C 配置了两个不同的 VLAN，因此，设备的每个 VLAN 具有不同子网的 IP 地址。

（本文示例中：VLAN1: 192.168.2.1，VLAN2: 192.168.1.1 或者 192.168.1.10）

两个 SCALANCE SC646-2C 的 VLAN2 接口互连。

这种场景无法靠纯路由的方式实现，而必须依靠 NAT 功能，因为 VLAN1 的子网不是唯一的，与连接建立的方向或者是否为 PC 设置网关无关。

每个相同的内部子网都需要一个 SCALANCE SC646-2C 模块，而不能同时将多个相同子网连接至一个 SCALANCE SC646-2C 上。

这就意味着在 SCALANCE SC646-2C 中需要额外定义 NAT 表，以便将 PC 发送的信息的目的 IP 地址替换成实际的设备的 IP 地址。这需要占用 VLAN2 子网中额外的未使用的 IP 地址。

本应用例子中的左侧 SCALANCE SC646-2C（第一个机器设备）需要配置目的 NAT，右侧 SCALANCE SC646-2C（第二个机器设备）需要配置源 NAT。

为了使所有的 CPU 响应的数据包能够返回到 VLAN2，必须在 CPU 的以太网参数配置中将相应的 SCALANCE SC646-2C (VLAN1)的 IP 地址配置为 CPU 的网关地址。

通讯过程（CPU2 到 CPU1 的主动连接）

本应用例子中的两个 SCALANCE SC646-2C 需要占用两个额外的 IP 地址 192.168.1.2 和 192.168.1.3 用于 NAT 功能。其中 192.168.1.3 相当于 CPU2 在 VLAN2 中的虚拟 IP 地址，192.168.1.2 相当于 CPU1 在 VLAN2 的虚拟 IP 地址。

CPU2 将使用 IP 地址 192.168.1.2 作为目的地址进行通讯。

根据 NAT 表的定义， 右侧的 SCALANCE SC646-2C 会将来自 CPU2 的数据包中的源 IP 地址替换成 192.168.1.3，然后将数据包发送给左侧的 SCALANCE SC646-2C。

根据 NAT 表的定义， 左侧的 SCALANCE SC646-2C 会将来自 CPU2 的数据包中的目的 IP 地址替换成 192.168.2.10，然后将数据包发送给 CPU1。

由于源 IP 地址被转换，从 CPU1 的角度来看，数据包是来自于不同的子网。配置源 NAT 转换源 IP 地址是必需的：由于 CPU1 和 CPU2 使用相同的内网 IP 地址（本文示例中：192.168.2.10），如果不转换源 IP 地址，那么当 CPU1 接收到来自于 CPU2 的数据包时，看起来就像数据包就来自于它自己的 IP 地址。.

优势

这种应用场景的优势在于，尽管所有 CPU 具有相同的子网 IP 地址，直接的 CPU 之间也能实现通讯。

劣势

这种应用场景的劣势在于，仅能建立从 CPU2 到 CPU1 的主动连接。如果要实现双向均可以建立主动连接的 CPU 之间的通讯，那么相反的方向也需要相应地添加规则。

对于每个配置相同的机器设备上需要建立通讯的 CPU，都需要额外占用 VLAN2 子网中的 IP 地址，每个 IP 地址都必须相应地进行配置。

NAT 和防火墙规则

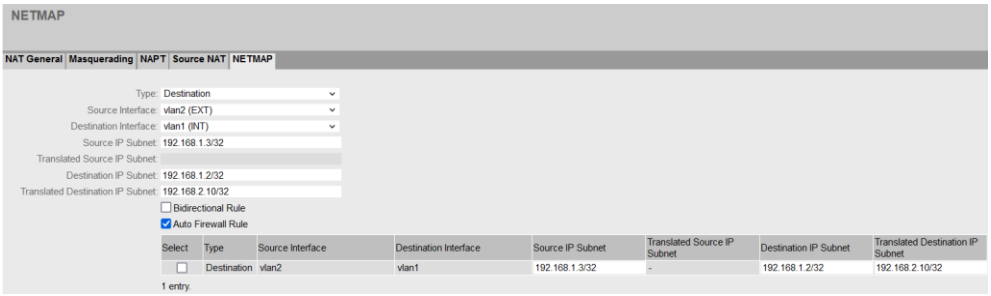
在第一个设备对应的 SCALANCE SC646-2C 的 NAT 表中，来自于 VLAN2 的目的 IP 地址为 192.168.1.2 的数据包，其目的 IP 会被转换为实际的 CPU1 的地址 192.168.2.10.

NAT 规则如下：

图 4-30

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**

图 4-31



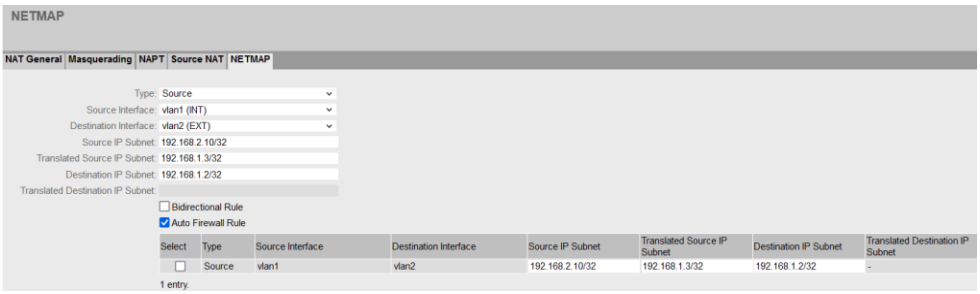
在第二个设备对应的 SCALANCE SC646-2C 的 NAT 表中，来自于 VLAN1 的源 IP 地址为 192.168.2.10 的数据包，其源 IP 会被转换为 192.168.1.3。

NAT 规则如下：

图 4-32

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**

图 4-33



CPU1(VLAN1) 和 CPU2 (VLAN1) 之间的通讯必须在所有的 SCALANCE SC646-2C 的防火墙中允许放行，规则需要参照相应的 NAT 表中的配置。

例如 CPU1-CPU2 之间仅进行 S7 协议通讯，那么可以在防火墙的服务选项中仅允许 TCP 端口 102。

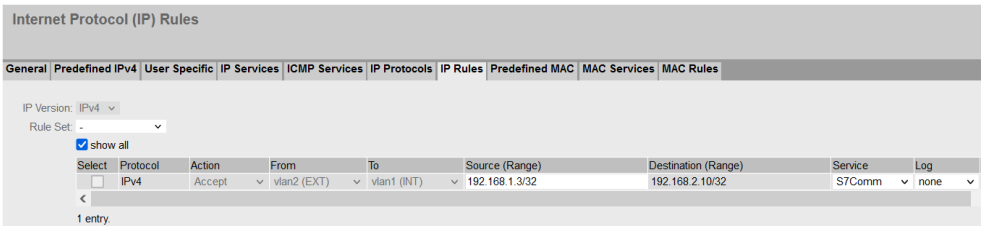
在第一个设备对应的 SCALANCE SC646-2C 的防火墙中，其 VLAN2（右侧 SCALANCE SC646-2C 的 NAT IP 地址）到 VLAN1（CPU1）之间的通讯必须允许放行。

配置防火墙规则如下：

图 4-34

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

图 4-35



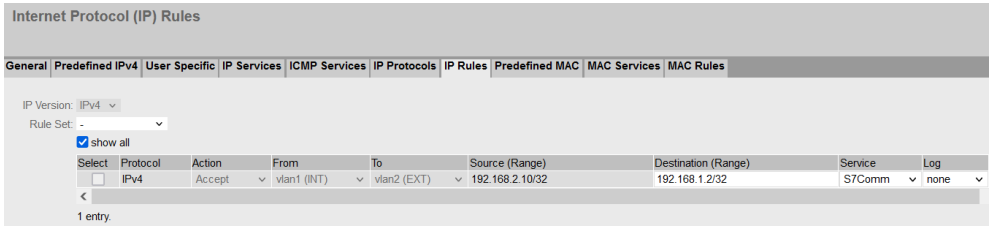
在第二个设备对应的 SCALANCE SC646-2C 的防火墙中，其 VLAN1（CPU2）到 VLAN2（左侧 SCALANCE SC646-2C 的 NAT IP 地址）之间的通讯必须允许放行。

配置防火墙规则如下：

图 2-36

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

图 2-37



注意

- 对于第一个设备的 SCALANCE SC646-2C（左侧），其目的 NAT 的地址转换会在防火墙规则检查前完成，所以在配置防火墙规则时，必须使用转换后的 IP 地址。.
- 对于第二个设备的 SCALANCE SC646-2C（右侧），其源 NAT 的地址转换会在防火墙规则检查完成后进行，所以在配置防火墙规则时，必须使用转换前的 IP 地址。
- 在 SCALANCE SC646-2C 中，"Destination IP Subnet"或"Translated Source IP Subnet" 列中可以只配置单个 IP 地址，此时掩码位设置为/32，只有如此设置，SCALANCE SC646-2C 才会响应对于额外添加的 IP 地址的 ARP 请求。
- 如果要将第二个设备的 SCALANCE SC646-2C（右侧）内网连接的所有节点转换为 VLAN2 中的 IP 地址，除了例子中的 NETMAP（Source NAT）方式外，也可以选择“Masquerading”或“Source NAT”实现。

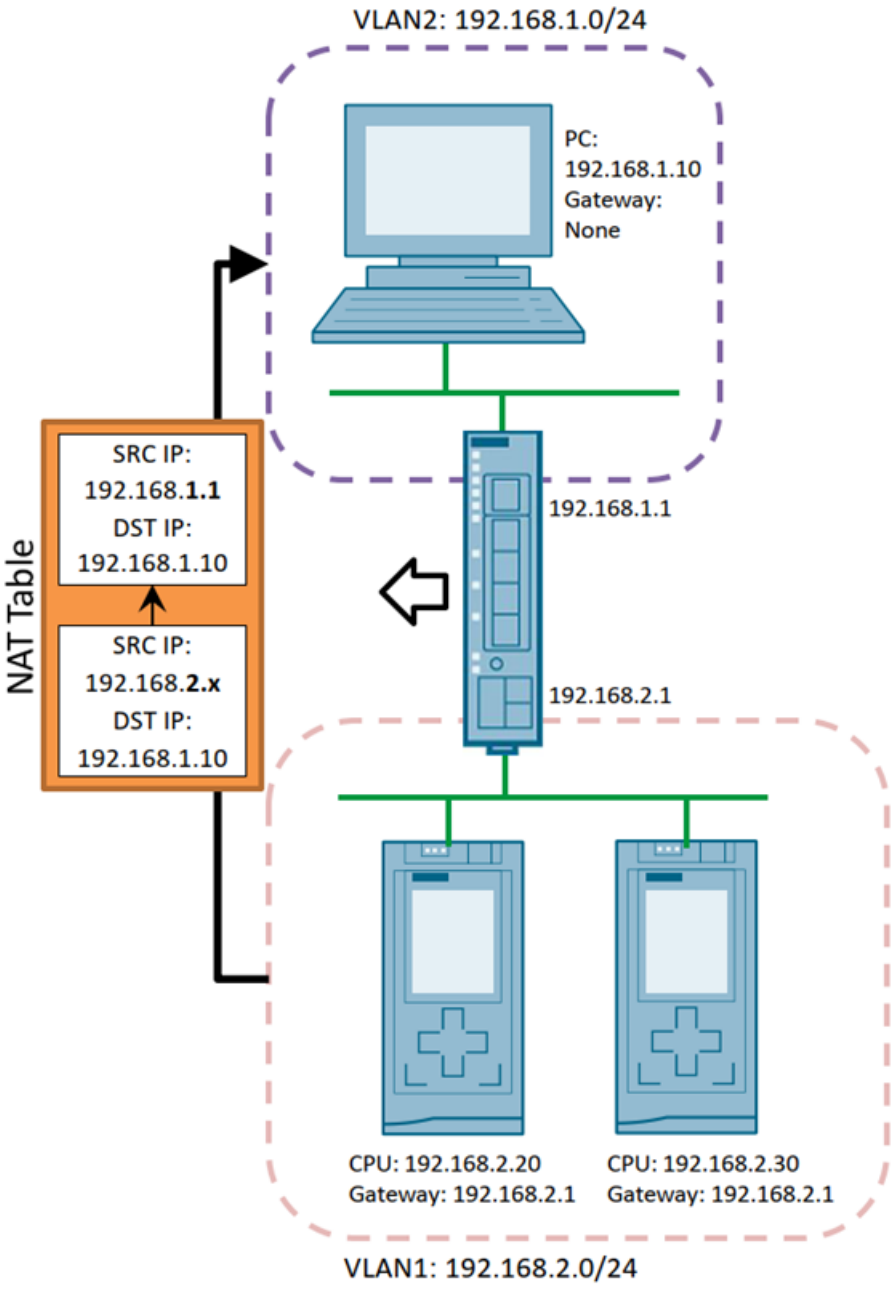
4.7 通过源 NAT 实现到控制系统的连接

应用场景示意

在此应用场景下，内网中的多个 CPU 通过主动方式建立到控制系统 PC 的连接，PC 机上能够无需配置网关地址。

目的端口号可以固定或者根据需要修改（例如 S7 连接或者 TCP/UDP）。

图 2-38



要求

为了网络隔离，SCALANCE SC646-2C 配置了两个不同的 VLAN，因此，设备的每个 VLAN 具有不同子网的 IP 地址。

（本文示例中：VLAN1: 192.168.2.1，VLAN2: 192.168.1.1）

此外，在 SCALANCE SC646-2C 中需要额外定义 NAT 表，以便将所有 CPU 发送的信息的源 IP 地址替换成其它的 IP 地址。

为了使所有的 CPU 发送的数据包能够到达 VLAN2 中的 PC，必须在 CPU 的以太网参数配置中将 SCALANCE SC646-2C (VLAN1)的 IP 地址配置为 CPU 的网关地址。

通讯过程（CPU 到 PC 的主动连接）

目的 IP 地址 192.168.1.10 的子网与 VLAN1 的本地 IP 子网不同，因此所有信息都发往网关（SCALANCE SC646-2C 的 VLAN1 接口 IP 地址）。

基于 NAT 表中的配置，SCALANCE SC646-2C 会将源 IP 地址替换为自身的（192.168.1.1），然后将报文发送给目的 IP 地址（PC）。

从 PC 的角度来看，所有 CPU 的数据包是来自于 VLAN2 的本地子网，因此 PC 可以直接响应，对于外部的 PC 来说，内部 VLAN1 的子网是不可见的。.

在所有从 PC 发向 CPU 的响应数据包中，目的 IP 地址会根据 NAT 会话表自动地被替换为相应的 CPU 的实际 IP 地址。

优势

这种应用场景的优势在于，NAT 配置无需额外的 IP 地址，源 IP 地址使用 SCALANCE SC646-2C VLAN2 接口的 IP 地址。

劣势

这种应用场景的劣势在于，仅能建立从 CPU 到某个 PC 的主动连接。

由于 NAT 配置使用相同的源 IP 地址，不可能辨别数据包来源于哪个 CPU。

NAT 和防火墙规则

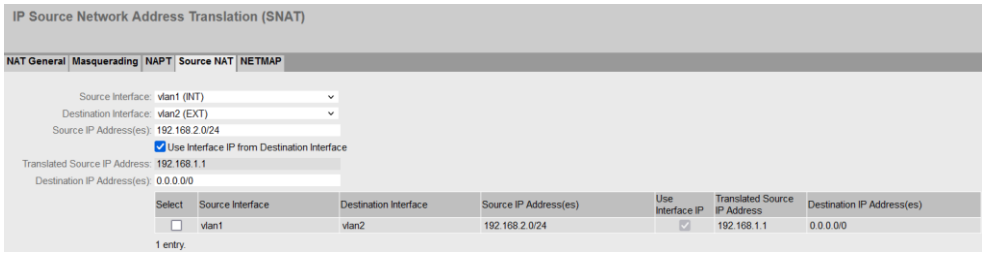
在 SCALANCE SC646-2C 的 NAT 表中，来自于 VLAN1 的源 IP 地址为 192.168.2.x 的数据包，源 IP 会被转换为其自身的 VLAN2 接口的地址 192.168.1.1。

NAT 规则如下：

图 4-39

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

图 4-40



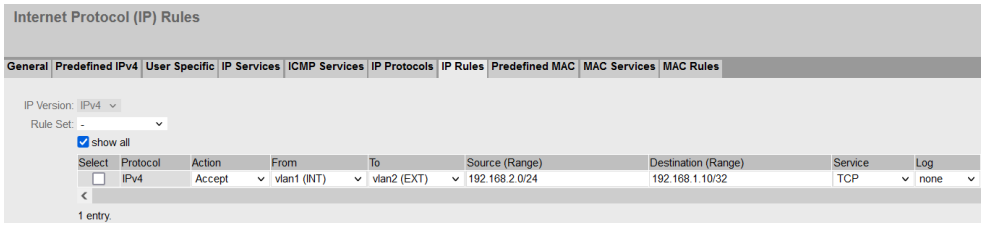
所有 CPU (VLAN1) 和 PC (VLAN2)之间的通讯必须在防火墙配置中允许放行，服务选项限制仅使用 TCP 连接。

配置防火墙规则如下：

图 4-41

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**

图 4-42



注意

- 源 NAT 的地址转换会在防火墙规则检查后完成，所以在配置防火墙规则时，必须使用转换前的实际 IP 地址。
- 如果要允许任意源或目的 IP 地址间的通讯，那么防火墙规则中的源或目的地址需要修改为 0.0.0.0/0 。
- 源 NAT 选项会将多个任意 IP 地址转换为一个独立的 IP 地址，因此可以称为 N:1 NAT。
- NETMAP 中的源 NAT 可以将多个 IP 转换为相应数目的其它子网 IP 地址，可以称为 1:1 NAT。
- 如果两个 CPU 没有设置网关地址，在相反的方向，类似的设置也可以正常工作。
- 通过源 NAT，由于通常不需要检查连接的源 IP 地址，这里展示的转换通常足够了。否则，需要通过选项 "NETMAP > Source NAT" (参见章节 4.5)来转换为独立的 IP 地址。

- 由于将多个 IP 地址转换为独立的一个 IP 地址，连接请求的源端口号可能也需要在源 NAT 的过程中进行转换，当两个节点使用相同的源端口号时，这种端口号的转换是必需的。

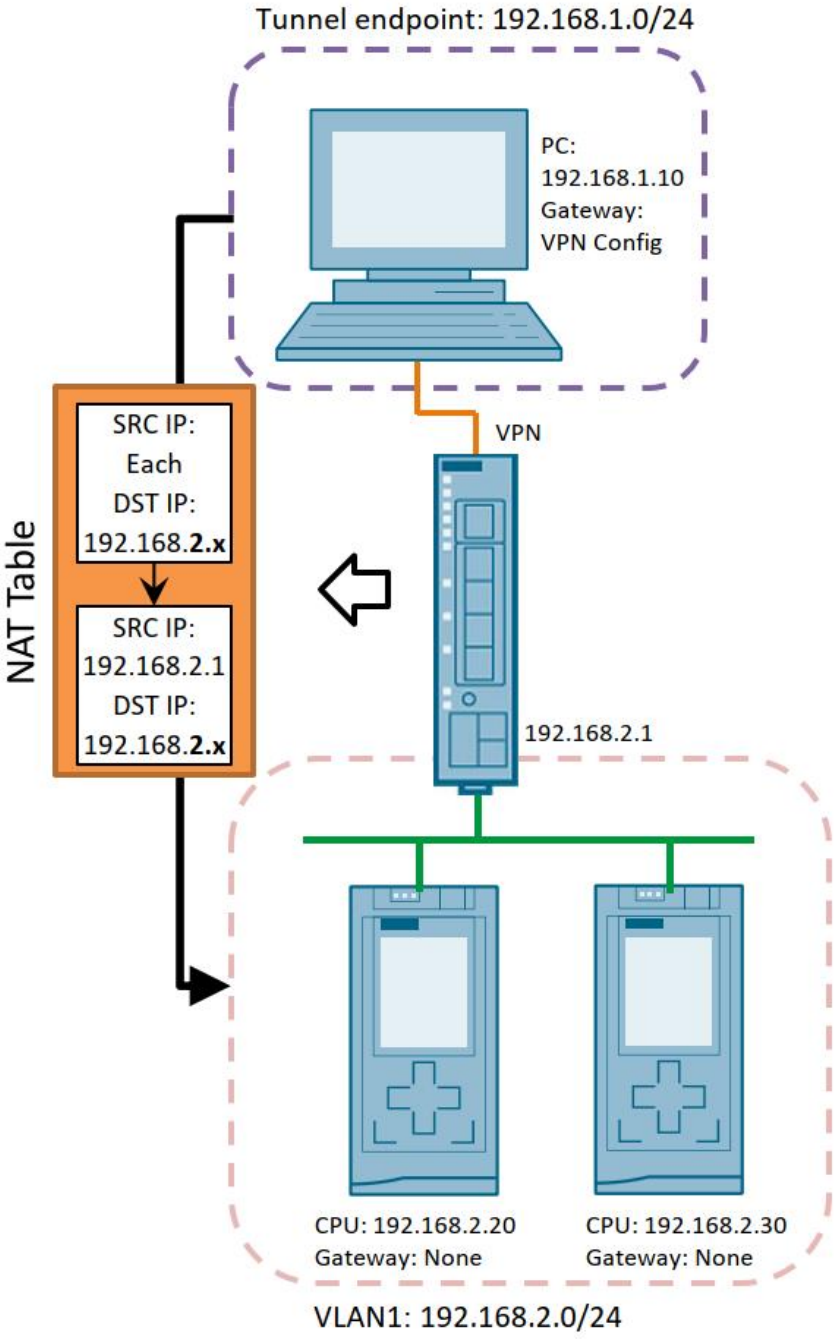
4.8 通过 VPN 隧道实现的源 NAT

应用场景示意

在此应用场景下，PC 机能够通过 VPN 隧道安全地访问现存工厂中的 S7 CPU，执行任何通讯功能。所有 CPU 上都不需要设置网关地址，也不需要修改硬件组态。

访问的目的端口号不是必须固定的，可以在实际配置过程中进行调整。

图 4-43



要求

这个应用场景的基础是在 SCALANCE SC646-2C 中配置 IPSec VPN 隧道，SCALANCE SC646-2C 作为隧道的端点，VPN 的伙伴可以是 SOFTNET Security Client 或者 PC 侧连接的另一个 SCALANCE S 模块。

为了网络隔离，SCALANCE SC646-2C 配置了两个不同的 VLAN，因此，设备的每个 VLAN 具有不同子网的 IP 地址。

（本文示例中：VLAN1: 192.168.2.1）。本例中仅关注 VLAN1，因为它是 VPN 隧道的终端。

此外，在 SCALANCE SC646-2C 中需要额外定义 NAT 表，以便将所有来自于 VPN 隧道的信息的源 IP 地址替换成其它的 IP 地址。

通讯过程（PC 到 CPU 的主动连接）

来源于 VPN 隧道的所有信息最终都会到达 SCALANCE SC646-2C 的 VLAN1 子网。

基于 NAT 表中的配置，SCALANCE SC646-2C 会将源 IP 地址替换为自身的 IP 地址（192.168.2.1），然后将报文发送给相应的节点（CPU）。

从 CPU 的角度来看，所有的数据包是来自于 VLAN1 的本地子网，因此 CPU 可以直接响应。

在所有从 CPU 发向 PC 的响应数据包中，目的 IP 地址会根据 NAT 会话表自动地被替换为 PC 的实际 IP 地址。

优势

这种应用场景的优势在于，无需修改现存的终端设备的设置即可实现访问。

劣势

这种应用场景的劣势在于，由于 NAT 配置使用相同的源 IP 地址，不可能辨别数据包来源于哪个远程节点。

NAT 和防火墙规则

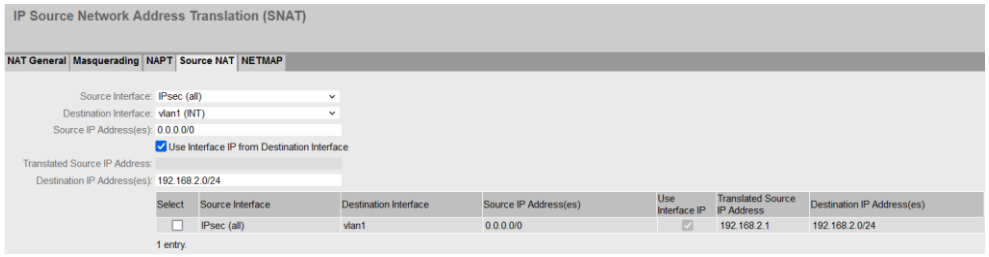
在 SCALANCE SC646-2C 的 NAT 表中，所有来自于 VPN 隧道的数据包，源 IP 会被转换为其自身的 VLAN1 接口的地址 192.168.2.1。

NAT 规则如下：

图 4-44

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	192.168.2.0/24

图 4-45



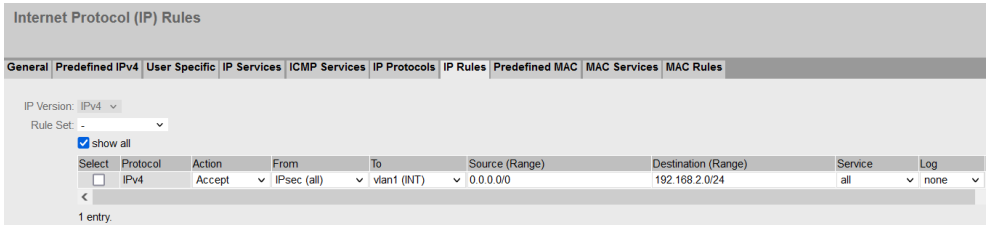
VPN 隧道 和 VLAN1 内网之间的通讯必须在防火墙配置中允许放行，服务选项不做限制。

配置防火墙规则如下：

图 4-46

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

图 4-47



注意

- 源 NAT 的地址转换会在防火墙规则检查后进行，所以在配置防火墙规则时，源区域必须使用转换前的远程 VPN 地址。
- 如果要允许任意源 IP 地址的通讯，那么防火墙规则中的源地址需要修改为 0.0.0.0/0 ，例如，当使用 SSC 作为 VPN 客户端时，隧道的远端子网预先不知道时，这是必需的。
- 这里展示的防火墙规则不是必须的，因为默认所有来源于 VPN 隧道的数据包是可以到达 VLAN1 的，但是当使用不同的 VLAN 或额外的 VLAN 时，防火墙规则是必需的。
- 对于防火墙和 NAT 配置中的源接口，可以通过所有隧道（"IPSec all"）或者特定的隧道（通过接口="end point"）进行选择。
- 这里的配置相当于在 SINEMA RC 中的选项 “Device is network gateway” 没有设置时的功能。来自于 VPN 隧道的方向也存在源 NAT 转换。

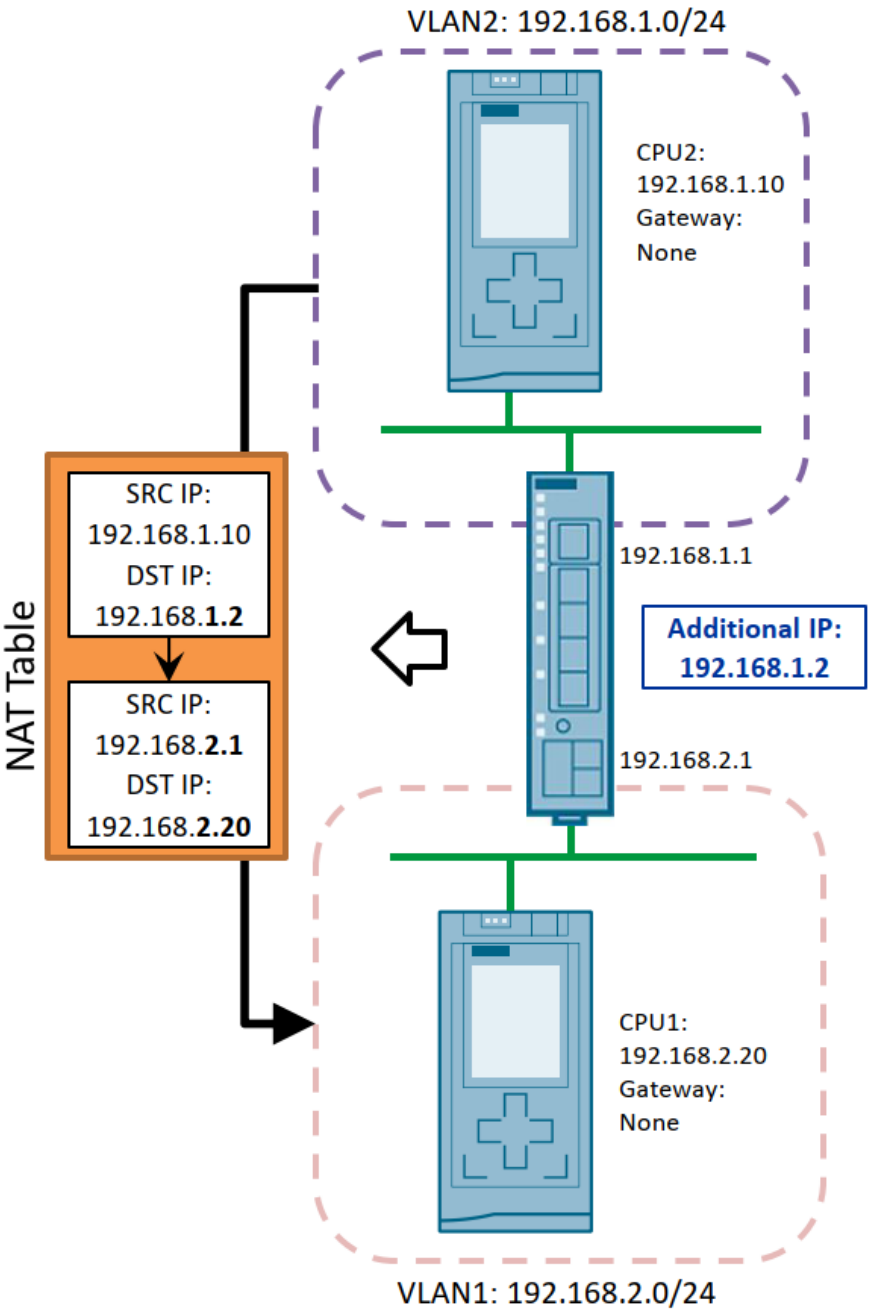
4.9 通过双向 NAT 实现的 S7 连接

应用场景示意

在此应用场景下，CPU 之间可以互相建立 S7 连接。CPU 模块中无需配置网关地址，硬件组态也无需修改。

S7 协议使用不可修改的 TCP 端口 102 建立通讯。

图 4-48



要求

为了网络隔离，SCALANCE SC646-2C 配置了两个不同的 VLAN，因此，设备的每个 VLAN 具有不同子网的 IP 地址。

（本文示例中：VLAN1: 192.168.2.1，VLAN2: 192.168.1.1）

此外，在 SCALANCE SC646-2C 中需要额外定义源和目的 NAT 表，以便将所有 CPU 的信息的 IP 地址替换成其它的 IP 地址。这需要在 VLAN2 子网中占用额外的未使用的 IP 地址。

通讯过程（CPU2 到 CPU1 的主动连接）

SCALANCE SC646-2C 需要在 NAT 配置中占用 VLAN2 子网的 IP 地址 192.168.1.2。

CPU2 会将本地子网中的 IP 地址 192.168.1.2 作为目的地址进行通讯。

根据 NAT 表的定义， SCALANCE SC646-2C 会替换数据包中的源 IP 地址和目的 IP 地址，然后将数据包发送给 CPU1。

通过改变源 IP 地址，从 CPU1 的角度来看，来自 CPU2 的数据包是来自于 VLAN1 的本地子网，因此 CPU1 无需使用网关即可直接进行响应。

在所有从 CPU1 发向 CPU2 的响应数据包中，源和目的 IP 地址会根据 NAT 会话表自动地被替换。

优势

这种应用场景的优势在于，通过使用额外的 IP 地址，到 CPU 的所有端口的访问的数据包均可转发。

CPU 的硬件组态无需修改。

劣势

这种应用场景的劣势在于，仅能建立从 CPU2 到 CPU1 的主动连接，此外，访问每个 CPU 都需要额外占用 VLAN2 子网中的 IP 地址，每个 IP 地址都必须相应地进行配置。

NAT 和防火墙规则

在 SCALANCE SC646-2C 的目的 NAT 表中，来自于 VLAN2 的目的 IP 地址为 192.168.1.2 的数据包，其目的 IP 会被转换为实际的 CPU 的地址 192.168.2.20。

在 SCALANCE SC646-2C 的 NAT 表中，来自于 VLAN2 的源 IP 地址为 192.168.1.10 的数据包，其源 IP 会被转换为其自身的 VLAN1 接口的 IP 地址 192.168.2.1。

NAT 规则如下：

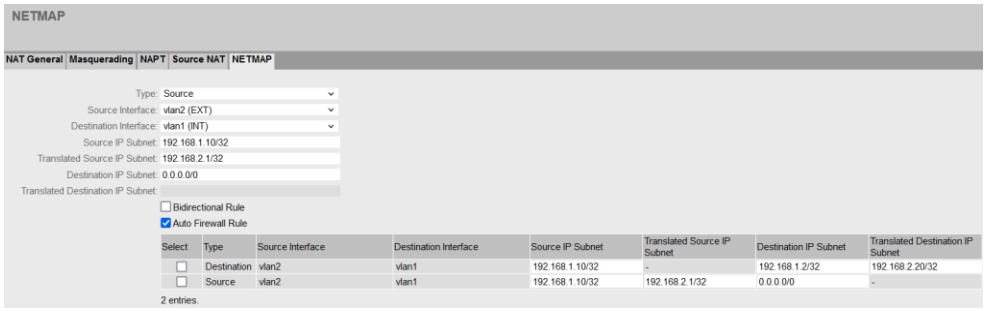
图 4-49

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

图 2-50

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

图 2-51

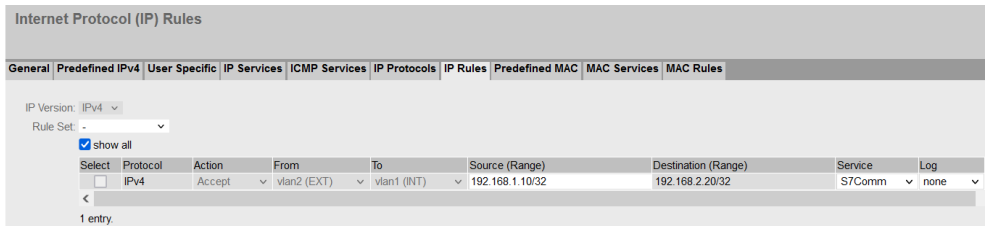


CPU2 (VLAN2) 和 CPU1 (VLAN1)之间的通讯必须在防火墙配置中允许放行，服务选项限制仅使用 TCP 端口号 102。

图 4-52

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

图 4-53



注意

- 源 NAT 的地址转换会在防火墙规则检查后进行，所以在配置防火墙规则时，必须使用转换前的 IP 地址。
- 目的 NAT 的地址转换会在防火墙规则检查前完成，所以在配置防火墙规则时，必须使用转换后的 IP 地址。
- 在 SCALANCE SC646-2C 中，"Destination IP Subnet"列中可以只配置单个 IP 地址，此时掩码位设置为/32，只有如此设置，SCALANCE SC646-2C 才会响应对于添加的 IP 地址的 ARP 请求。

5 附录

5.1 相关文档链接

表 5-1

1.	Which NAT scenarios can you realize with SCALANCE SC-600 / M-800 / S615? https://support.industry.siemens.com/cs/ww/en/view/109744660
2.	How can you use the STEP 7 Online functions even when NAT (Network Address Translation) is being used or a remote subnetwork is to be reached? https://support.industry.siemens.com/cs/cn/en/view/109754922
3.	What are the functions of the SCALANCE S-600, SC-600 and M-800 devices and differences between them? https://support.industry.siemens.com/cs/cn/en/view/109794014
4.	Industrial Security Quantity Framework Limits https://support.industry.siemens.com/cs/cn/en/view/58217657
5.	Understanding and Using Firewall of Industrial Security Appliance SCALANCE S https://support.industry.siemens.com/cs/cn/en/view/22376747
6.	SIMATIC NET: Industrial Ethernet Security SCALANCE SC-600 Web Based Management (WBM) https://support.industry.siemens.com/cs/cn/en/view/109754815
7.	SIMATIC NET: Industrial Ethernet Security SCALANCE S615 Web Based Management https://support.industry.siemens.com/cs/cn/en/view/109751632
8.	
9.	
10.	