Using the Custom > Forwarding and Routing (Scada) agents on SiteManager

This guide describes the principles of configuring an agent for accessing a device on the device network from the uplink network and vice versa. This application note does not fully cover all functionality of the agents. Please refer to the online help menu in the web interface of the SiteManager for more information.

Version: 2.2, November 2022

secomea

Table of Contents

Introduction

The Forwarding and Routing agents can be used when you want to communicate between devices “across” the interfaces of the SiteManager, whether it is from the Uplink to the Device network or vice versa.

Forwarding and Routing agents are active also when no GateManager connection is present. Essentially the Forwarding agent can be seen as a set of Firewall/NAT rules applied to the SiteManager’s Uplink/DEV interfaces, and the Routing agent can be seen as a set of Firewall/Routing rules applied to the Uplink/DEV interfaces.

Typical use:

The Forwarding agent is used when a local server on the Uplink network needs to collect data from devices attached to the Device network (DEV), or when a device on the Device network needs to submit data to a server on the Uplink network. In both cases the SiteManagers IP address represents the actual device address of the opposite side.

In some cases you want the sending party to reach the network on the other side directly by its local subnet, and the SiteManager will act as a router between the networks. This would be the case if you wanted a device on the DEV side to reach the entire Uplink network (or the Internet) through the SiteManager. In this case a Routing agent is used.

1. Brief description on the Forwarding and Routing (SCADA) Agent

Routing (SCADA) agent

The Scada agent is created as Device Type:

CUSTOM (Advanced) / Routing (SCADA).

The Routing (SCADA) agent is basically a set of firewall rules, which allows traffic both ways (UPLINK ←→ DEV), from the IP address/subnet defined in the agent parameter details menu. The Routing (SCADA) Agent is used when you have i.e. an industrial PC on your Uplink network, and you want to access devices on the Device side. You can also use it for allowing Internet access to devices on the Device network. Again, you need to specify in the parameter details, which IP addresses/subnets are allowed to access the Internet (UPLINK).

A Routing agent specifies which source addresses are allowed to be forwarded to the opposite side of the SiteManager, and is limited to 3 source addresses. All ports and IP addresses on the other side will be accessible by the configured IP devices.

If the device accessing a network via the Routing agent, does not have the SiteManager as default gateway, it will require a static route on the device in order to tell the device where to look for the IP addresses. Refer to the documentation for your device, in order to add/edit static routes.

Forwarding Agent

The Forwarding agent is created as Device Type:

CUSTOM (Advanced) / Forwarding

You can use the Forwarding Agent in two ways; either to grant access from a certain device to connect to another interface, or to be able to connect to a device via the UPLINK IP address.

The Forwarding Agent is more specific compared to the Routing (SCADA) agent. It also requires a bit more setup, in order to get things working. Its intended use is to give a quick option to access a device on the Device side via the UPLINK IP address, and vice versa – so basically, the SiteManager will act as a router, where you create port forwarding rules in it.

Only the ports stated in the Forwarding Agent will be accessible.

More than one Forwarding Agent can be active at one time; each agent can contain up to 10 forwarding rules.

Notes:

When configured correctly the Forwarding and Routing agents are always ON regardless of the GateManager or Internet connection and do not need to be activated by a LinkManager connection.

The Forwarding or Routing Agents will not show up in the GateManager or LinkManager Console.

2. Agent formats

NOTE: The description of the parameters and syntax can also be found in the SiteManager online help by entering the agent's Parameter Details and select HELP in the top bar

2.1. Forwarding Rule format

Each forwarding rule must be combined from a number of elements as follows:

[#|?] [[IN_IFACE*] [$LOCAL_IP]:] [PROTOCOL:] [SOURCE_IP[/MASK]:] [NAT_PORT] >[>] [OUT_IFACE[*]:] TARGET[/MASK] [:TARGET_PORT]

Elements in [...] are optional.

NOTE: Spaces are not allowed in the rule (they are inserted above for readability purposes).

- #:

  A leading number sign in a rule specifies that the rule is disabled (i.e. to be ignored).

- **?**:

  A leading question mark specifies an optional rule, meaning that any errors related to this rule should not be treated as fatal (i.e. rule is ignored in case of errors).

- **IN_IFACE / LOCAL_IP** ([*interface name*[*]][$*local IP*]):

  This specifies the incoming interface (and/or local IP address/alias) for the connection; if omitted, it defaults to opposite of OUT_IFACE (if set), else UPLINK*. The * is a wildcard meaning any interface of the specified type, e.g. UPLINK* or DEV*.

  The $ character is both a separator (if IN_IFACE is also specified) and is used to differentiate LOCAL_IP from the SOURCE_IP element.

- **PROTOCOL** (*protocol*):

  This specifies the network protocol, either TCP, UDP, or ANY; if omitted, it defaults to TCP.

  When **ANY** is used in a rule with either NAT_PORT or TARGET_PORT, it means "both TCP and UDP"; otherwise it means "any IP protocol".

- **SOURCE_IP** (*IP address*[/*mask*]):

  This specifies a source IP address or subnet filter for this rule.

- **NAT_PORT** (*port number[-number]*):

  This specifies the original destination port number (range) for port forwarding targeted at the IN_IFACE. Port forwarding means that traffic addressed to that specific port (range) on a SiteManager interface is translated and forwarded to a specific external target and port with translation.

  Notice: If you add a port forwarding rule for TCP port 443, this will disable access to the SiteManager WEB GUI from the rule's incoming interface. You can still access the WEB GUI using another interface or via the Appliance Launcher, or (if connected remotely) via LinkManager or GateManager.

- **> or >>** :

  A double >> separator indicates that source NAT translation should be applied for traffic forwarded by this rule, making the SiteManager the source of the forwarded traffic.

A single > indicates no source translation.

- **OUT_IFACE** (*interface name*[*]):

  This specifies the outgoing interface for the connection; if omitted, it defaults to opposite of IN_IFACE (if set), else DEV*. The * is a wildcard meaning any interface of the specified type, e.g. UPLINK* or DEV*.

- **TARGET** (*IP address*[/*mask*] or *hostname*):

  The TARGET part specifies the allowed IP address or subnet for the connection on the "other side" of the SiteManager.

- **TARGET_PORT** (*port number[-number]*):

  For a port forwarding rule (if NAT_PORT is specified), it specifies the target port (range) for the forwarded traffic; if omitted it defaults to the NAT_PORT.

  Note: If a port range is specified in NAT_PORT do *not* specify a port range here. Otherwise, the TARGET_PORT part specifies the allowed target port number(s) on the target system.

Optional parameters (field value):

- **Enable UPLINK Source Translation** (+TUP):

  When this option is set, the Forwarding agent will apply Source NAT to all connections forwarded out through an UPLINK interface (from a device on a DEV interface), regardless of the > or >> settings in the forwarding rules. This means that the target system will see the SiteManager UPLINK IP address as the source address rather than the original Device IP address.

  You will usually enable this option when creating outbound forwarding rules (from DEV to UPLINK). If not enabled, you probably need to configure static routes on the target system pointing at the UPLINK IP address, in order for the target system to determine the gateway back to the device.

- **Enable DEV Source Translation** (+TDEV):

  When this option is set, the Forwarding agent will apply Source NAT to all connections forwarded out through a DEV interface (from a system on an UPLINK interface), regardless of the > or >> settings in the forwarding rules. This means that the target device will see the SiteManager DEV IP address as the source address rather than the original system's IP address. You will usually enable this option when creating inbound forwarding rules (from UPLINK to DEV).

2.2. The Routing (Scada) agent Rule format

Parameters (*field value*):

- **Scada Address 1** (`ip_address`):
  The IP address of the first Scada PC.

- **Scada Address 2** (`ip_address`):
  The IP address of the second Scada PC.

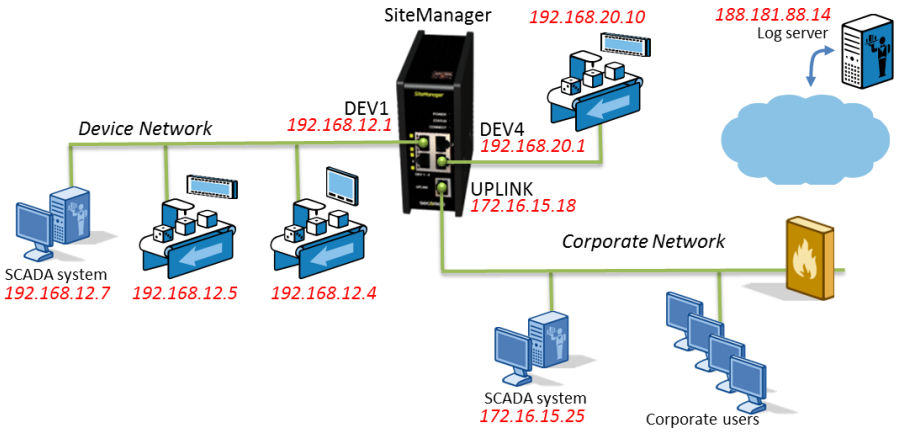
- **Scada Address 3** (`ip_address`):
  The IP address of the third Scada PC.

- **Enable UPLINK Source Translation** (`+TUP`):
  When this option is set, the Scada agent will apply Source NAT to all connections forwarded out through an UPLINK interface (from a device on a DEV interface). This means that the target system will see the SiteManager UPLINK IP address as the source address rather than the original Device IP address.

- **Enable DEV Source Translation** (`+TDEV`):
  When this option is set, the Scada agent will apply Source NAT to all connections forwarded out through a DEV interface (from a system on an UPLINK interface). This means that the target device will see the SiteManager DEV IP address as the source address rather than the original system's IP address.

3. Usage scenarios

In the following scenarios, we will use a typical setup that looks like this:



The IP addresses of the different interfaces of the SiteManager are: DEV1: 192.168.12.1, DEV4: 192.168.20.1 and UPLINK: 172.16.15.18. All address ranges are in the /24 (255.255.255.0) range.

On the UPLINK (or corporate) side, we have a Server/SCADA system located at 172.16.15.25 and a number of users placed on the corporate network.

On the DEV (or device) side, we have an HMI at 192.168.12.4, a PLC on 192.168.12.5 and an IPC/SCADA system on 192.168.12.7. All located on port 1. On port 4, we have a PLC on 192.168.20.10.

In addition, we have a logging server placed somewhere on the Internet at IP address 188.181.88.14.

When reading the scenarios, please note that the SiteManager has two sides, either UPLINK (the "Internet connection" or "corporate" side) or DEV (the device side where the equipment is placed). Both sides can have multiple interfaces as the 3429 model used in the demonstration, the DEV side can have up to 4, and the UPLINK side can have up to 2.

Referencing these interfaces can be done either on a single interface, or on a group of interfaces:

- "DEV1" or "UPLINK1" refers to a specific interface port
- "DEV*" or "UPLINK*" refers to all the interface ports as a group

Please always enter the interface reference on both sides of the forwarding rule, although it can be omitted. Referencing one side will automatically assume the other; however, this could cause confusion in some special cases.

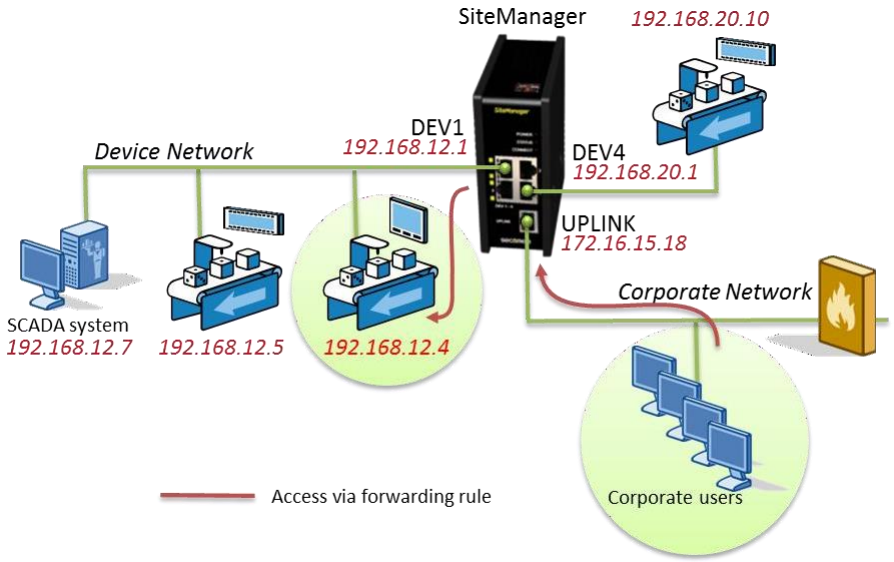
One or more ports are mandatory, but the port option on the right side of the “>/>>” will denote a destination port translation (PAT). The source port is never referenced and is assumed to be random.

Protocols can be referenced as "TCP", "UDP" or "ANY". If omitted, it will default to “TCP”.

The following pages contain usage scenarios for both the Forwarding Agent and the Routing (SCADA) Agent.

The scenarios are by no means exhaustive, but they are meant to provide a general understanding of how the agents are configured to solve in the most common infrastructure configurations, where the SiteManager is involved.

3.1. Accessing a device on DEV from the corporate network (UPLINK > DEV)

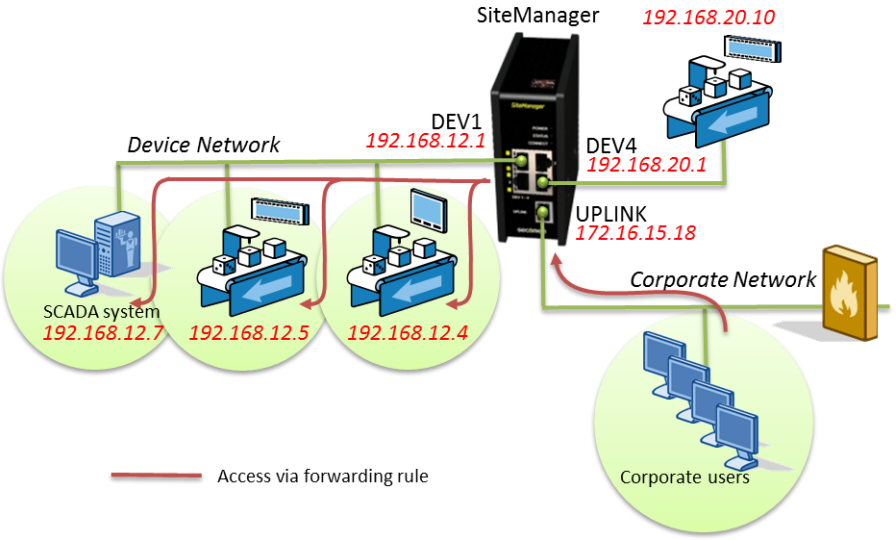


If a webserver in an HMI needs to be accessible from the corporate network, it can be achieved with the following forwarding rule:

```
UPLINK*:TCP:80>>DEV*:192.168.12.4
```

Whenever you browse the UPLINK interface (http://172.16.15.18) of the SiteManager, you will be redirected to the webserver.

3.2. Accessing multiple devices on DEV with the same port number from the corporate network (UPLINK > DEV)



If multiple webservers needs to be accessible from the corporate network, it can be achieved by using different ports on the UPLINK interface.

You can translate port numbers with the following forwarding rules:

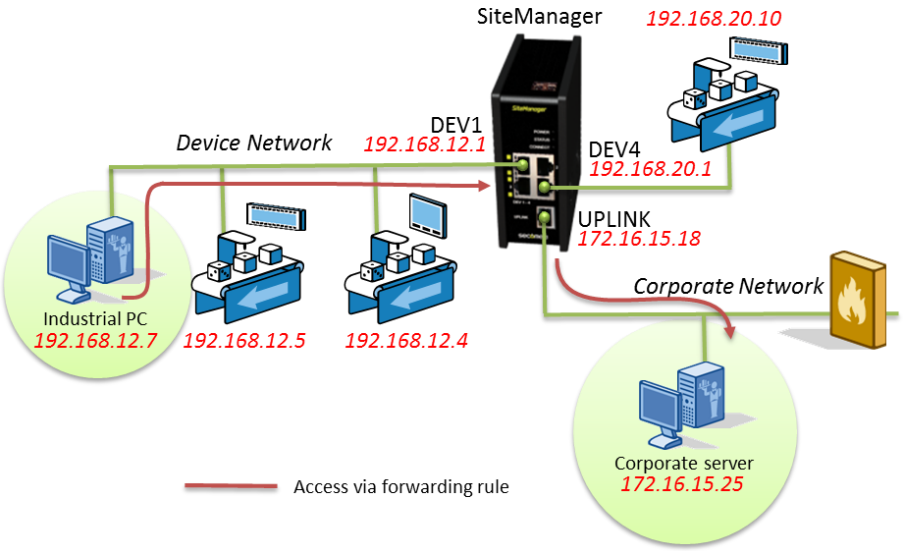
```
UPLINK*:TCP:80>>DEV1:192.168.12.4
UPLINK*:TCP:81>>DEV1:192.168.12.5:80
UPLINK*:TCP:82>>DEV1:192.168.12.7:80
```

Whenever you browse the UPLINK interface with http://172.16.15.18 of the SiteManager, you will be redirected to the webserver in the HMI on 192.168.12.4.

If you browse http://172.16.15.18:**81** you will hit the webserver in the PLC on 192.168.12.5 and if you browse http://172.16.15.18:**82** you will hit the webserver on the SCADA system on 192.168.12.7.

You can also access the devices on their own IP addresses. This would require you to add a static route on the PC you are connecting from. You would then need to tell the computer which gateway to use, when accessing the IP addresses. The gateway would be the IP address of the UPLINK interface (172.16.15.18).

3.3. Accessing a device on UPLINK from a device on DEV (DEV > UPLINK)



In this scenario, we have an Industrial PC on the device network that needs access to a server on port 4476 (TCP) the corporate network.

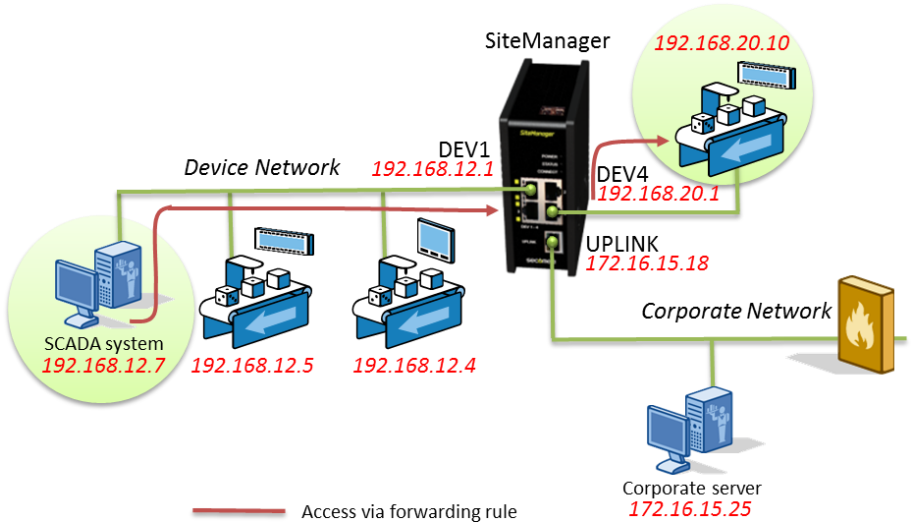
This can be achieved by the following forwarding rule:

```
DEV1:TCP:192.168.12.7:4476>UPLINK*:172.16.15.25 +TUP
```

The ”+TUP” option is needed because we are going from the DEV interface to the UPLINK interface. When the IP packet arrives at the corporate server, the source IP needs to be a known IP address.

For the server to know where the IP address is located there is a need for either a static route or a translation of the UPLINK interface IP address. In this case we have selected ”Enable UPLINK Source Translation:” in the forwarding rule form. Remember that selecting ”Enable UPLINK Source Translation:” overrules all ”>>” settings in any of the 10 forwarding rules in the form.

3.4. Accessing a device on DEV1 from a device on DEV4 (DEV > DEV)



In this scenario we assume that an SCADA system on the DEV1 interface needs to access a PLC on port 8004 (TCP) on the DEV4 interface.

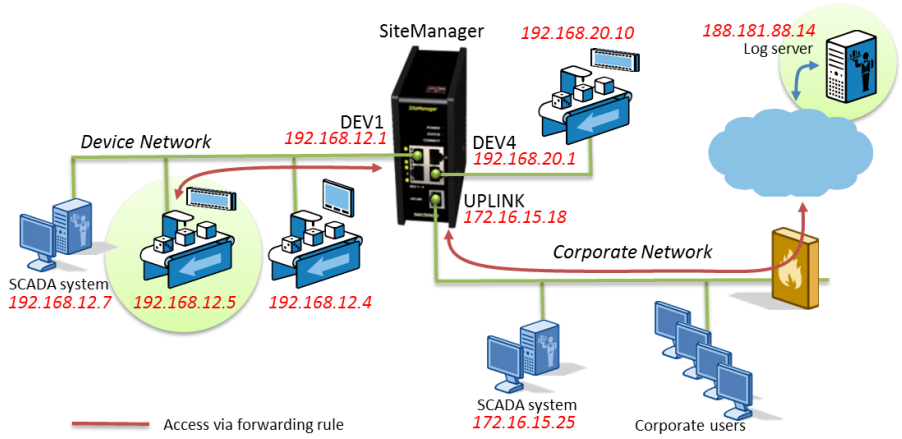
The forwarding rule would look like this:

```
DEV1:UDP:192.168.12.7:8004>DEV4:192.168.20.10
```

In this case we use only ”>” instead of ”>>”, as no NAT translation is necessary, as long as the PLC is using the DEV1 port as default gateway.

Remember that the SCADA system would need its default gateway set for the DEV1 interface (192.168.12.1) in order to access the PLC on the DEV4 interface.

3.5. Communicating with a LOG server on the Internet (UPLINK/DEV <> UPLINK/DEV)



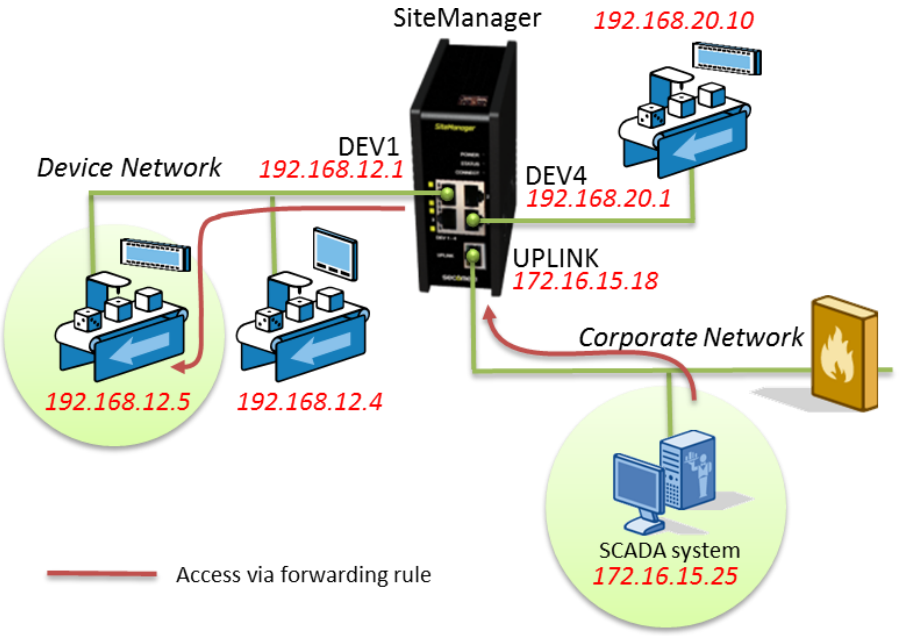
In this scenario, we have a logging server placed on the Internet, that needs to both pull and receive data from the PLC on port 1433 (TCP) placed on the DEV1 interface

The forwarding rules would look like this:

```
DEV1:TCP:192.168.12.5:1433>>UPLINK*:188.181.88.14
UPLINK*:TCP:188.181.88.14:1433>DEV1:192.168.12.5
```

For this to work, the PLC will need to have its default gateway set to the DEV1 interface address (192.168.12.1).

3.6. Accessing a device on DEV from a device on the corporate network (UPLINK > DEV)

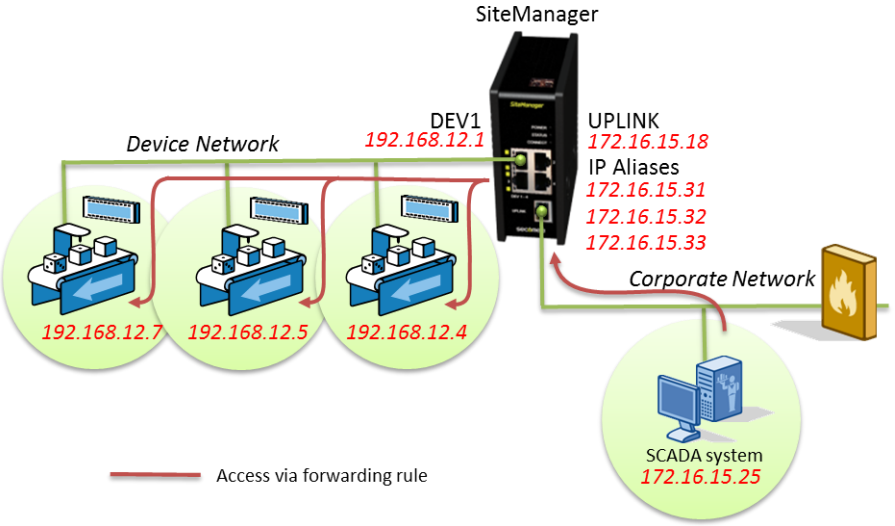


A PLC needs to be accessible from a SCADA system through port 1433 on the corporate network.

This can be achieved with the following forwarding rule:

```
UPLINK*:TCP:172.16.15.25:1433>>DEV1:192.168.12.5
```

3.7. Accessing devices on DEV from the corporate network through IP Aliases (DEV > UPLINK)

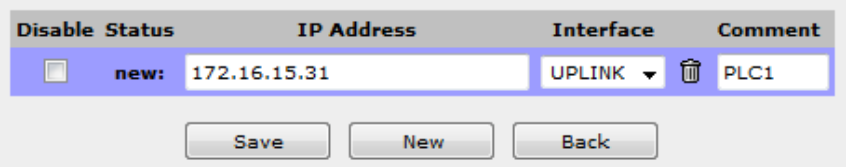


A server on the corporate network needs to access identical ports (1433) on 3 PLCs on the DEV1 interface. The ports cannot be changed on the server or on

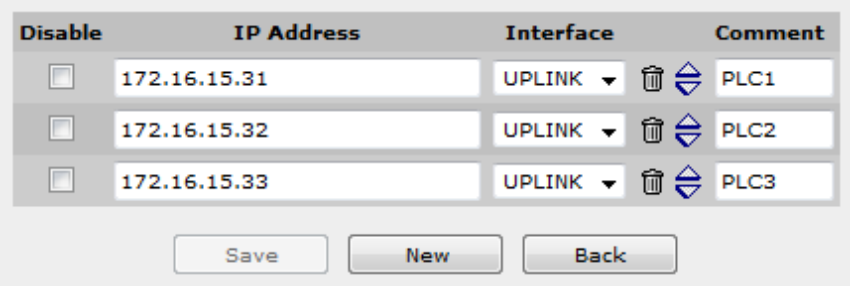
the PLCs. Also the default gateway of the server is not the SiteManager, and no extra routes are allowed on the server.

For this to work, we can use routable IP addresses on the corporate network, and add them to the SiteManager to match the IP addresses of the PLCs.

First of all, we need to add the IP addresses to the SiteManager. This is done in the SiteManager GUI under “Routing -> IP Aliases -> New”:



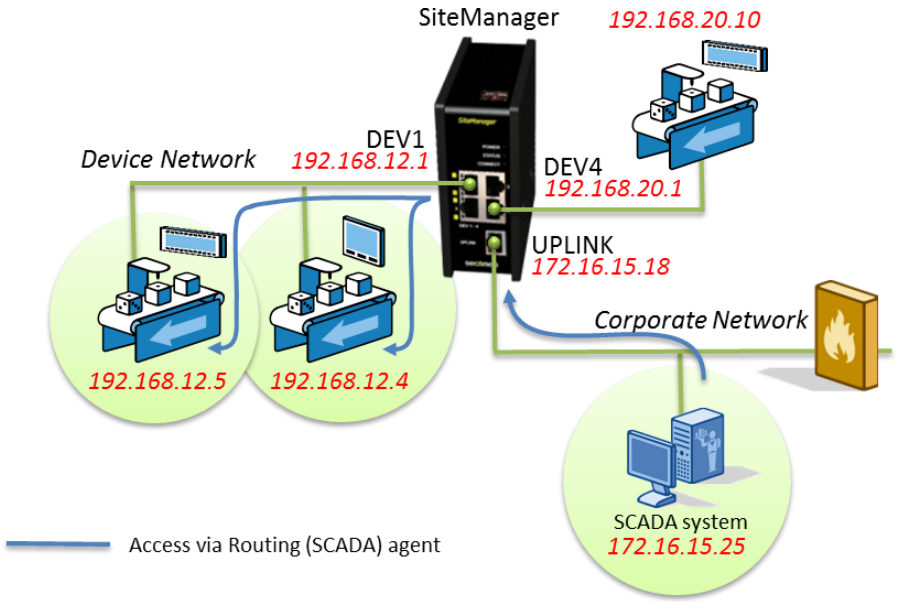
Enter the IP address, change the Interface to ”UPLINK” and add an optional comment. Click save and repeat for all 3 addresses:



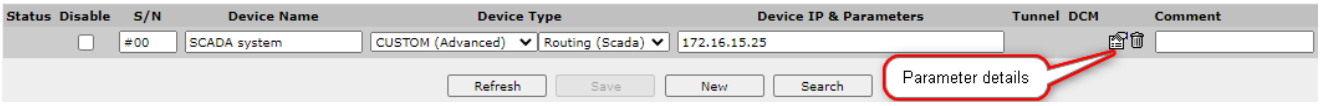
Then create the forwarding rules like this:

```
UPLINK*$172.16.15.31:TCP:172.16.15.25:1433>>DEV1:192.168.12.4
UPLINK*$172.16.15.32:TCP:172.16.15.25:1433>>DEV1:192.168.12.5
UPLINK*$172.16.15.33:TCP:172.16.15.25:1433>>DEV1:192.168.12.7
```

3.8. Accessing all devices on DEV from the corporate network (UPLINK > DEV)

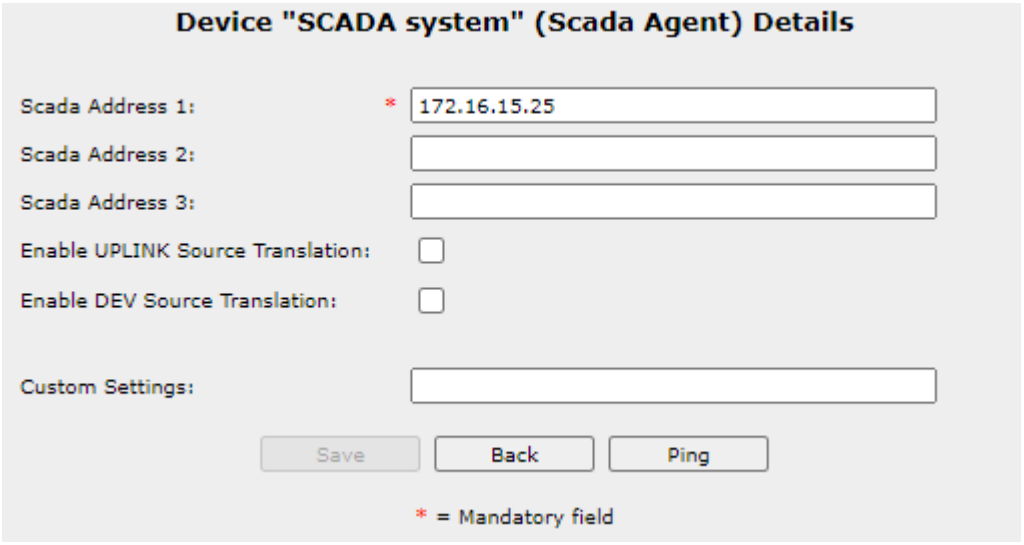


To be able to access the device net any port from i.e. a SCADA system, you can use the Routing (SCADA) Agent (and not the Forwarding Agent), like this:



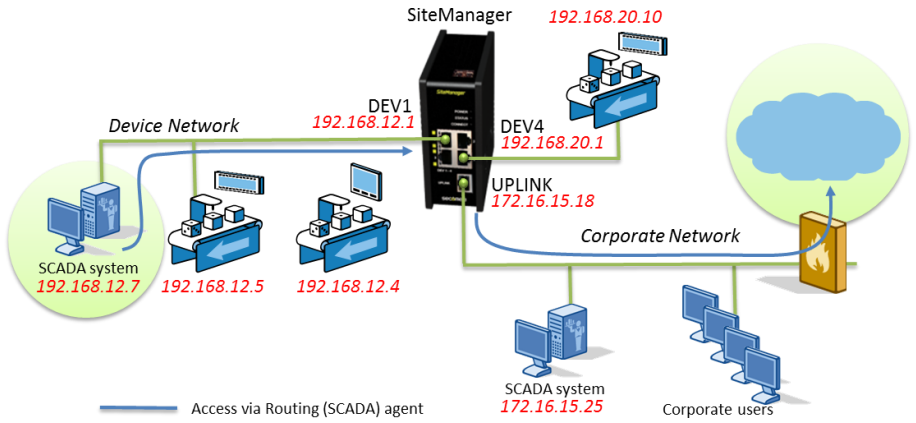
Here you assign the IP address of the SCADA system to the “Routing (Scada)” Agent. You would also need to enable “Enable DEV Source Translation:”, as the SCADA system IP address is unknown to the device network.

This is done by clicking the “Parameter details” button:

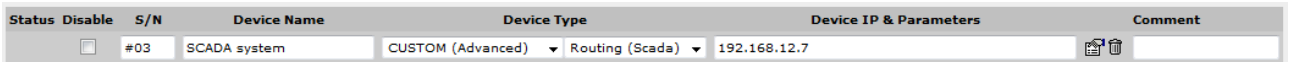


For this to work, the PLC will need to have its default gateway set to the DEV1 interface address (192.168.12.1), otherwise it will not know where the public IP addresses are located. Refer to **Appendix A** for more info on setting up a gateway on the device.

3.9. Accessing the Internet from a device on DEV (DEV > UPLINK)

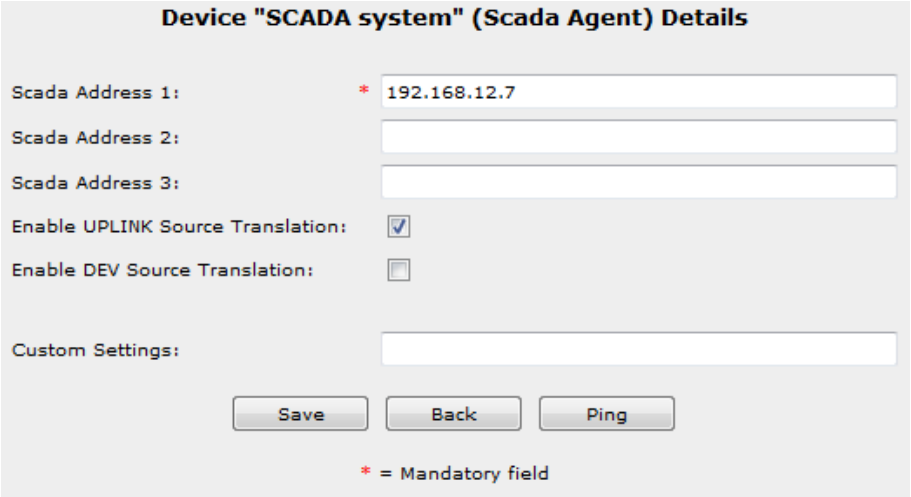


To be able to access the Internet from a device, you can use the Routing (SCADA) Agent (and not the Forwarding Agent), like this:



You would have to assign the IP address of the SCADA system to the “Routing (Scada)” Agent. You would also need to enable “Enable UPLINK Source Translation:”, as the SCADA system IP address is unknown to the corporate network.

Under Parameter Details the setup would look like this:



For this to work, the PLC will need to have its default gateway set to the DEV1 interface address (192.168.12.1), otherwise it will not know where the public IP addresses are located. Refer to **Appendix A** for more info on setting up a gateway on the device.

3.10. Advanced: Accessing all ports on devices on DEV with same IP (Uplink > DEV)

All PCs on the Uplink side needs to access two PLCs on the device network, and should have access to all ports on the PLCs.

This would typically be done by a Routing agent, but this is limited to 3 specific PCs. In addition you may have a route from the PCs to another network that is identical to that of the SiteManagers device side. For instance you could have two SiteManagers connected to the same Uplink network, but where the device networks of the SiteManagers are identical, and even the IP addresses of the PLCs are identical.

Let's assume that Uplink1 has the IP address 192.168.1.1. As there are two PLCs behind each SiteManager, you must create an "IP Alias" on Uplink1 (under routing >IP Aliases), in order to have an extra IP address to forward on e.g. 192.168.1.2 (Note: Make sure it does not conflict with an existing IP address in the Uplink network)

On the device side of the two SiteManagers we have two PLCs with the addresses 10.0.0.1 and 10.0.0.2

In order to allow any UDP or TCP port, we need to define a range in the forwarding rule:

```
$192.168.1.1:ANY:1-61000>>10.0.0.1
```

```
$192.168.1.2:ANY:1-61000>>10.0.0.2
```

This includes port 443, which means you cannot access the SiteManager Web GUI from the Uplink side (you can still access it from GateManager and LinkManager)

So in order to exclude port 443 from the range, it will require splitting the rule in two parts:

```
$192.168.1.1:ANY:1-442>>10.0.0.1
```

```
$192.168.1.1:ANY:444-61000>>10.0.0.1
```

```
$192.168.1.2:ANY:1-442>>10.0.0.2
```

```
$192.168.1.2:ANY:444-61000>>10.0.0.2
```

Notice that the SiteManager's NAT engine used by the Forwarding agent cannot handle protocols that make reverse connections, such as FTP Active mode connections (FTP Passive mode works fine)

You can also refine the rule to limit who can access the devices from Uplink. For instance if it was only the server with IP address 192.168.3.1 that was allowed to access the PLCs, the rule would look like this:

```
$192.168.1.1:ANY:192.168.1.3:1-61000>>10.0.0.1
$192.168.1.2:ANY:192.168.1.3:1-61000>>10.0.0.2
```

Appendix A. Configuring devices to use SiteManager as route

For a device to use the SiteManager as route based on the Routing agent, the device needs to know that the SiteManager is the gateway to the other network.

Method 1: Assign SiteManager as default Gateway

If the SiteManager is configured as default gateway for the device, the device will automatically use the SiteManager as route. If the device does not already use another device as gateway, you may safely change it to the local IP address of the SiteManager. This would typically only be the case for devices on an isolated DEV network.

If the device supports DHCP, you can enable DHCP on the DEV port of the SIteManager and the device will automatically get the SiteManager's DEV port as default gateway. If you are concerned that the IP address may change, you can enter the SiteManager menu DEV > DHCP > Leases and fix the MAC address of the device to always have a specific IP address assigned.

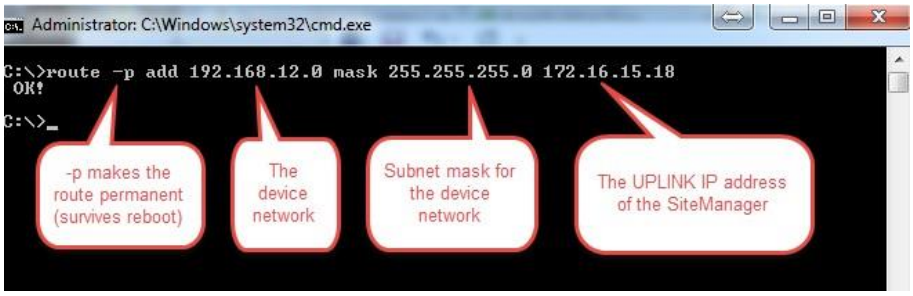
Method 2: Configure a local static route

If the device is on the Uplink side of the SiteManager, or does not allow to change its current default gateway, you must configure a static route on the device. Refer to the documentation of your device for instructions.

If the device is a Windows computer, such as a SCADA PC, you can open a command prompt and enter a static route through the "route" command.

Press "Windows key + R" or go to the start menu and type "cmd" and press ENTER.

Use the "route" commend to add a static route. See example below:



Then configure your software to access the IP address of the devices directly. I.e. 192.168.12.4 and 192.168.12.5.

Method 3: Inserting a route into the corporate firewall

When the SCADA PC needs access to an IP address not being in the same subnet as the SCADA PC, it will request the route from its default router. This router is typically the corporate firewall.

You should therefore insert a static route rule in the firewall that routes request to IP addresses of equipment in the device network to the uplink address of the SiteManager.

With the example above in mind, the firewall should be configured to forward requests for IP addresses in subnet 192.168.12.0 to the "router" 172.16.15.18.

Appendix B. Frequently Asked Questions (FAQ)

Q: How do I temporarily disable a forwarding rule?

A: Insert "#" (without the quotes) as the first character in the field

Q: Can I use the Source Translation checkmarks at the bottom?

A: Yes, but using these will overrule all ">" and ">>" translations in all rule fields. If you know what you are doing when creating rules, do not use these. Also refer to Scenario 3 above.

Q: How do I check if the forwarding rules have been applied?

A: In your SiteManager, go to "Status -> Extended -> Active Firewall Rules -> NAT TABLE -> Chain FWA", you should see something like this if you use scenario 5 as reference:

```
pkts bytes target prot opt in out source destination
 0 0 DNAT tcp -- eth1 * 188.181.88.14 0.0.0.0/0 tcp dpt:1433 to:192.168.12.5:1433
 0 0 DNAT tcp -- eth0 * 192.168.12.5 0.0.0.0/0 tcp dpt:1433 to:188.181.88.14:1433

Chain FWA_masq3524 (1 references) pkts bytes target prot opt in out source destina-
tion
 0 0 MASQUERADE tcp -- * eth0 188.181.88.14 192.168.12.5 tcp dpt:1433
 0 0 MASQUERADE tcp -- * eth1 192.168.12.5 188.181.88.14 tcp dpt:1433
```

Notices

Publication and copyright

Trademarks

Disclaimer

Secomea A/S reserves the right to make changes to this publication and to the products described herein without notice. The publication of this document does not represent a commitment on the part of Secomea A/S. Considerable effort has been made to ensure that this publication is free of inaccuracies and omissions but we cannot guarantee that there are none.

The following paragraph does not apply to any country or state where such provisions are inconsistent with local law:

SECOMEA A/S PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE

SECOMEA A/S SHALL NOT BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, CONSEQUENTIAL, OR OTHER DAMAGE ALLEGED IN CONNECTION WITH THE FURNISHING OR USE OF THIS INFORMATION.

Secomea A/S
Denmark

CVR No. DK 31 36 60 38

E-mail: sales@secomea.com
www.secomea.com