Logging via SiteManager Relay Chains
Deployment Overview

This guide describes the deployment process when using the SiteManager Server/Device Relay functions for pushing or pulling log data from devices to a central server.

This document is an extension to the presentation “Secomea on-demand and Permanent access combined.ppt”. It is advised to study that presentation to get an overview of the data flow.

Version: 2.4, August 2014

secomea

Table of Contents

Introduction

Additional to the standard LinkManager “on-demand” access to industrial equipment, there may be a requirement for persistent connections to devices simultaneously from a central server.

Solution models

NOTE: This document focuses on the Relay chains solution.

A. Relay Chains

Relay links between a GateManager or a SiteManager located at the server site to SiteManagers on remotes sites.

Advantages:

- All remote sites can have the same subnet. Subnet conflicts do not occur. This allow for the same standardized configuration for all sites.
- The firewall friendly connection via GateManager is used for all communication. No separate connections are needed.
- If using SiteManager-to-SiteManager relay, no Public IP address are required in either end.
- Ideal for collection of log data.

Disadvantages:

- All communication travel via the GateManager. Use of bandwidth intensive and timing critical applications are not recommended.
- Less ideal if logging multiple devices at each site with different services (protocols). This is referred to in the following as the ADVANCED SCENARIO)
- You must have an own GateManager installed. Currently Relay Chains are disabled on the Secomea hosted GateManagers.

B. TrustGate to SiteManager EasyTunnel VPN

VPN access from a Secomea TrustGate EasyTunnel Server on the server site directly to EasyTunnel clients in SiteManagers on remotes sites.

Advantages:

- Ideal for advanced video streaming and similar protocols with demands to QoS or advanced routing capabilities.
- You get access to the entire device network and therefore do not have to be concerned about allowing specific IP addresses or ports

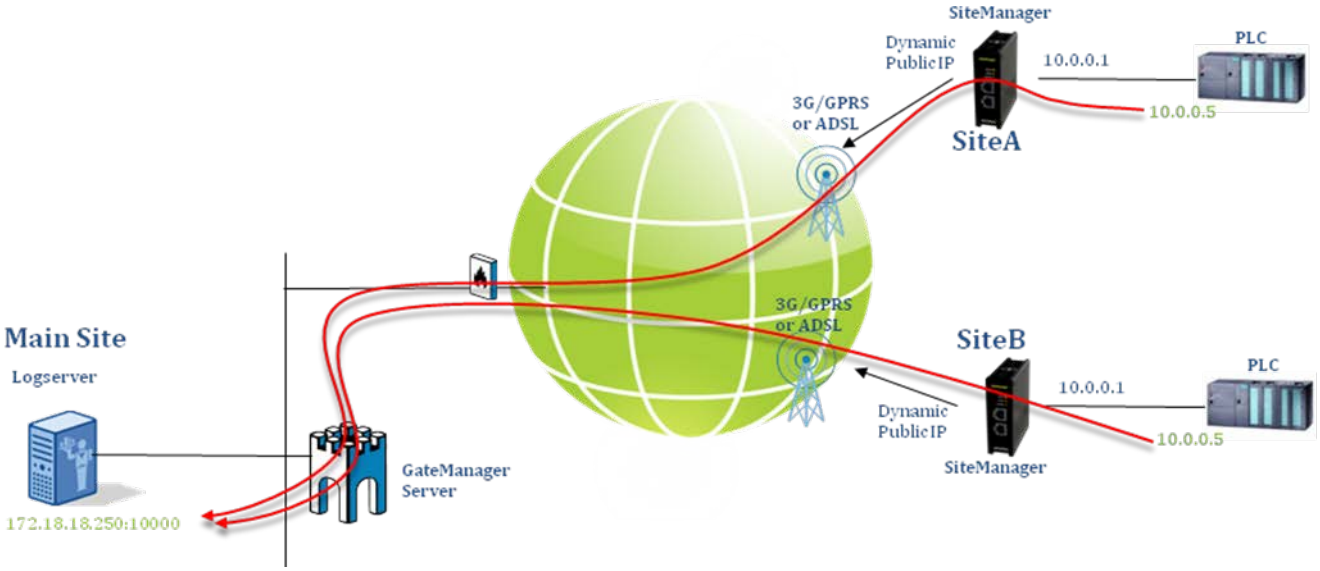
Disadvantages:

- The TrustGate must be available on a public address (can be placed behind another firewall that has a public address)
- The device network behind the SiteManagers must have different subnets.
- UDP port 4500 most be open outgoing on the firewall in front of the SiteManager (if using 3G this is not an issue)
- You get access to the entire device network, which the customer's IT department may dislike.

Refer to the document “**Logging via SiteManager EasyTunnel Client - Deployment overview**” for more info on this solution model.

1. PUSH-Data using SiteManager-to-GateManager Relay-chain

You can configure that all devices should push their log data to a central Log server.

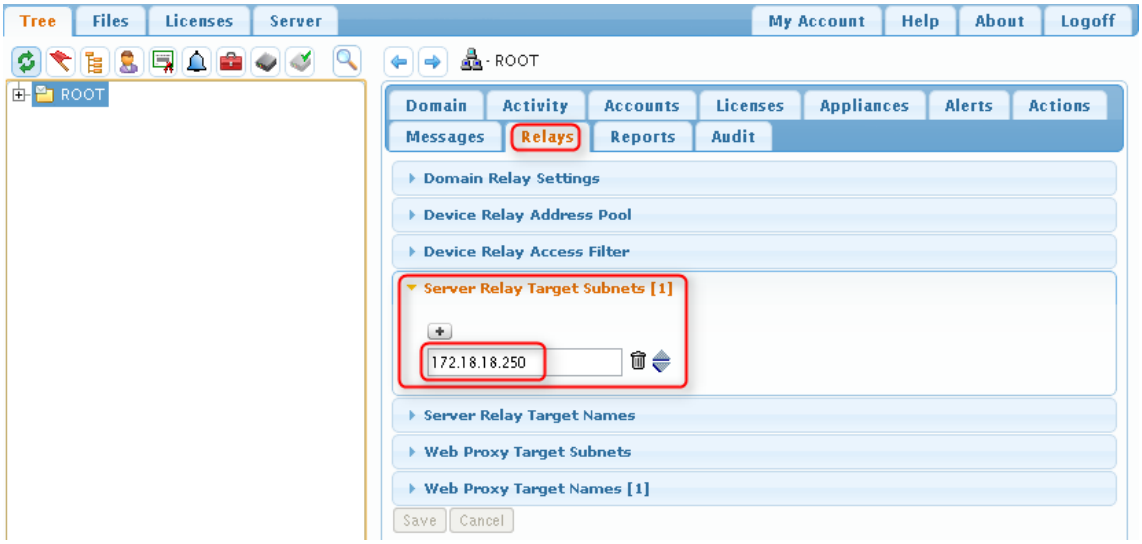


Note that the Log server cannot determine the identity of the devices based on their source addresses, since all log data will have the GateManager's local address as source (eth0). So the log data must contain the identity of the device.

If you require a push based solution where the Log server identifies the device by its source address, you must use the EasyTunnel VPN approach.

1.1.1. Define a “Server Relay Target Subnet”

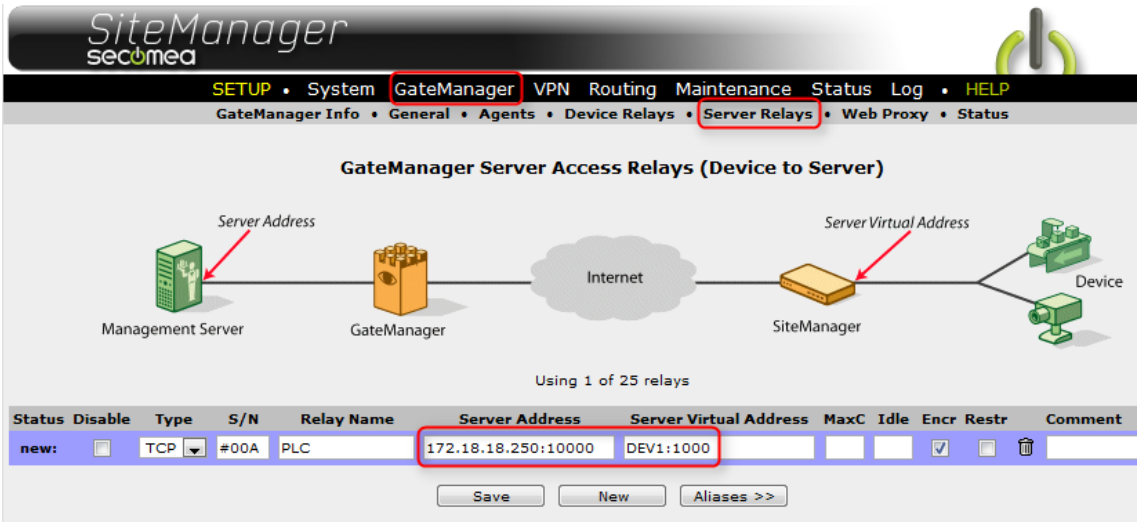
The GateManager must know the address of the Log server, to which it will forward the data received from the devices. In this example the Log server has IP address **172.18.18.250.** I.e. the subnet consists of a single address only, and that is filled into the **Server Relay Target Subnets** section of the domain where the SiteManagers are connected.



1.2. Configure SiteManagers

Configuration of SiteManagers is quite simple.

In the SiteManager Web GUI, enter the menu **GateManager** --> **Server Relays** menu and click **New**



The Server Address should be the Log servers' real IP address, and the port that the Log server receives log data on.

The Server Virtual Address should just be DEV1 and the same port number 10000. (Only if you had a 4 port switch version of the SiteManager you could specify which of the 4 managed ports the log data would refer to).

The configuration is identical on all SiteManagers!

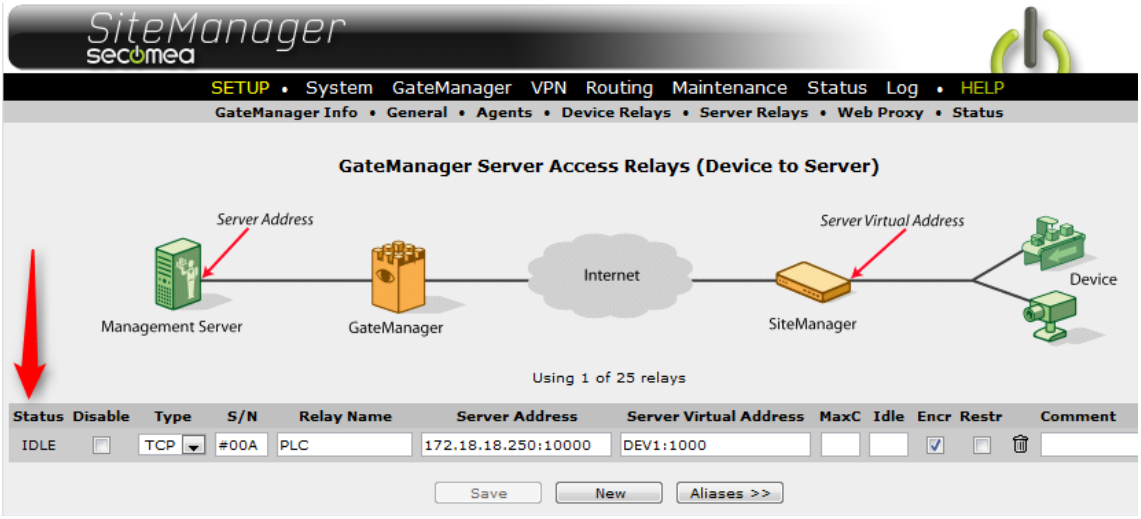
1.3. Configure the Log server IP address on the devices

The Log server IP address configured on the devices should be the DEV port of the SiteManager. So in principle they see the SiteManager's DEV port as the Log server.

Since the relay concept allows all sites to have the same subnet, you can configure the SiteManager DEV port and the device IP address identically on all installations.

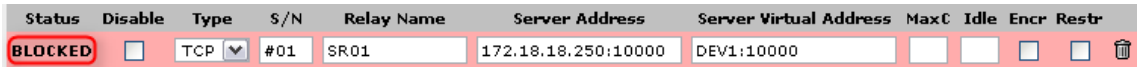
1.4. Troubleshooting

Even if you have typed the a wrong Device Virtual Address, or if the address pool is not enabled for the GateManager domain in which the SiteManager is connected, you will see the Server Access Relay go IDLE:

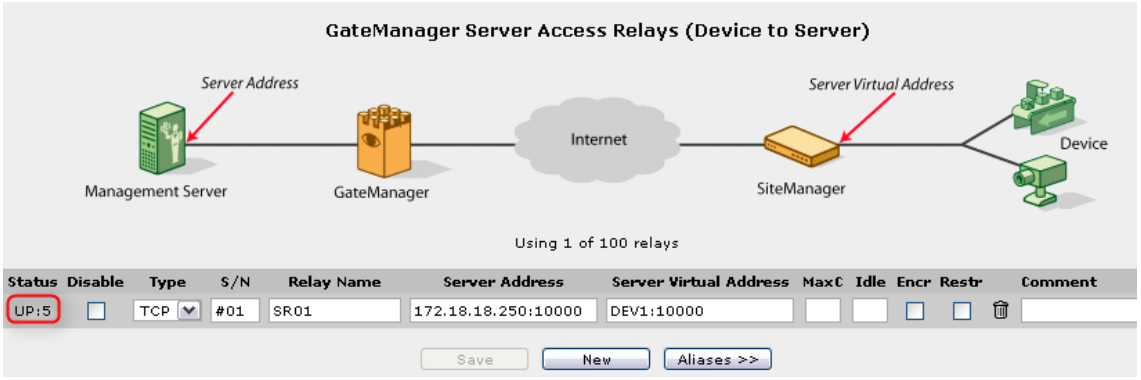


The first time data is transmitted on the Server Relay, it will be verified if there is in fact a connection.

If it shows blocked, it indicates a configuration error on the SiteManager, or that the Server Relay Target may not have been defined for the domain in which the SiteManager is connected.

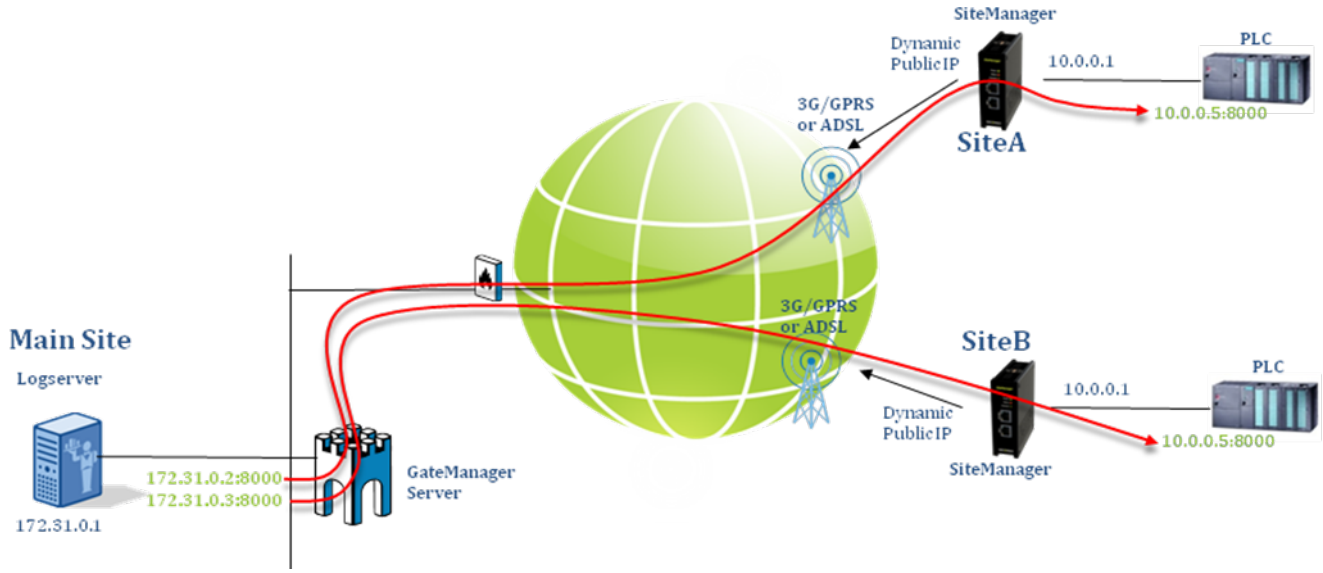


Check you configuration and Disable and Enable the Blocked relay and you should see the following:



2. PULL-Data using GateManager-to-SiteManager Relay-chain

The typical scenario is that the Log server pulls log data from a single device at each site using a single protocol; while other services, such as https, RDP or programming access, should be done interactively using LinkManager.

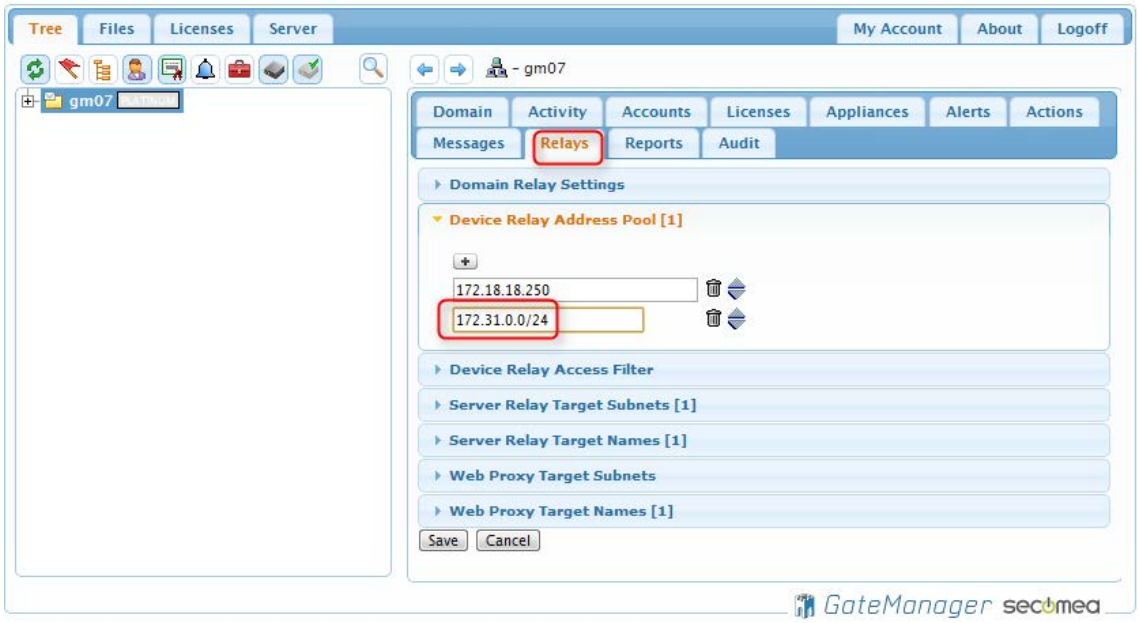


In this example the GateManager is placed in the same network as the Log server. More likely the GateManager will be placed in a hosting centre, or in a DMZ zone, and the Log server would reach it via a router (gateway).

2.1.1. Define a “Device Relay Address pool"

The GateManager administrator has to allow a pool of addresses that will represent each remote device.

In this example the pool is **172.31.0.0/24**. This means the range of “Device Addresses” is 172.31.0.1 – 172.31.0.254



The server addresses are also referred to as **Device Virtual Addresses** and in this case represents **different sites**.

So you could define a table like this:

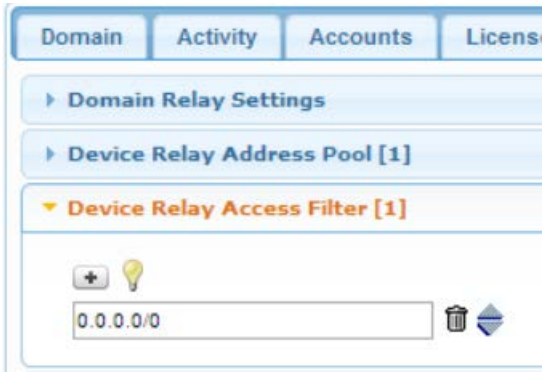
Site A: 172.31.0.2

Site B: 172.31.0.3

Etc.

2.1.2. Define Relay Access Filter

You also need to define a Relay Access Filter. This is the subnet, which is allowed to use the relay connection. If you do not want to have any restrictions, simply add 0.0.0.0/0

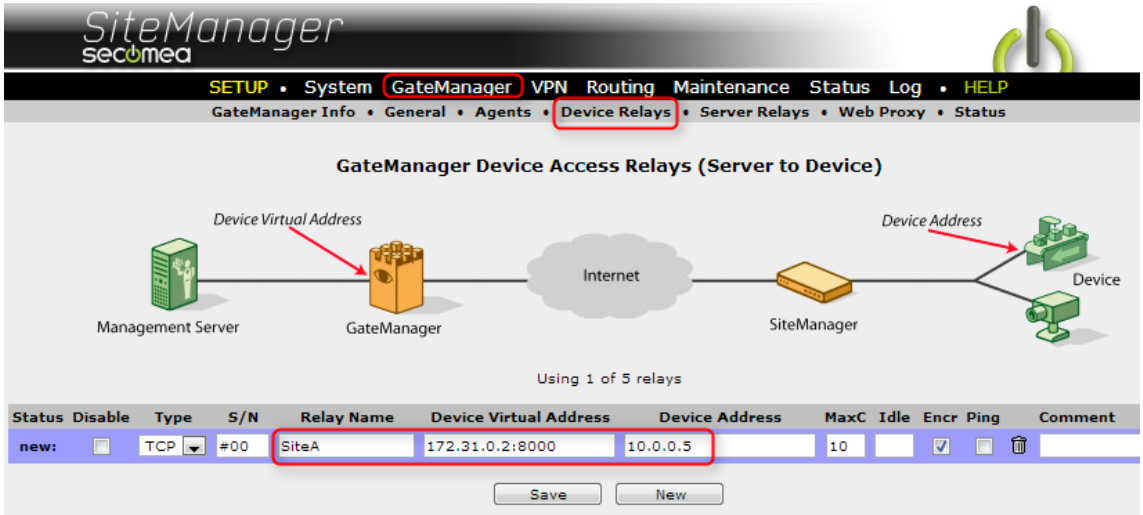


2.2. Configure the SiteManagers

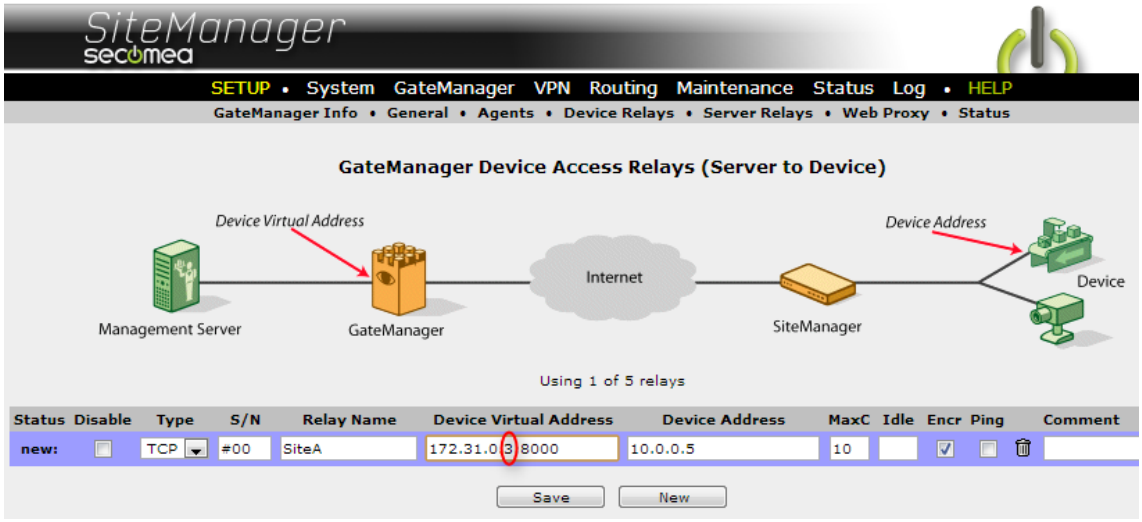
Configuration of SiteManagers is quite simple.

On the SiteManager Web GUI, enter the menu **GateManager** --> **Device Relays** and click **New**

On the SiteManager at SiteA, you define the **Device Virtual Address** that the Log server should access to get relayed to the real **Device Address**

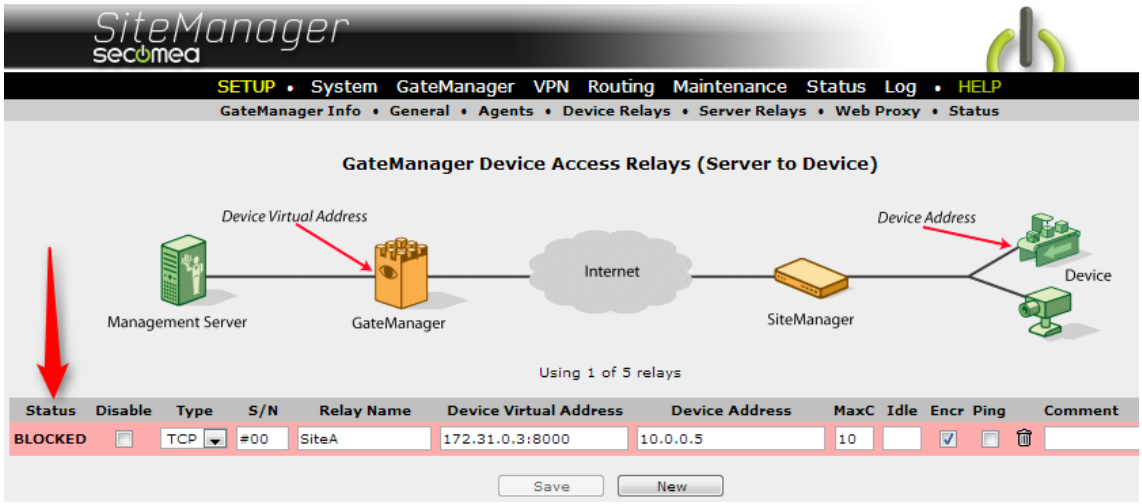


The configuration for the SiteManager at SiteB, is almost identical. You just change the Device Virtual Address.


SiteManager
secomea
SETUP • System GateManager VPN Routing Maintenance Status Log • HELP
GateManager Info • General • Agents • Device Relays • Server Relays • Web Proxy • Status
GateManager Device Access Relays (Server to Device)
Device Virtual Address
Device Address
Management Server
GateManager
Internet
SiteManager
Device
Using 1 of 5 relays
Status Disable Type S/N Relay Name Device Virtual Address Device Address MaxC Idle Encr Ping Comment
new: TCP #00 SiteA 172.31.0.3:8000 10.0.0.5 10
Save New

2.3. Troubleshooting

If you experience that you get a "blocked" message on the Device Relay definition, it means that either you have typed a wrong Device Virtual Address, or the address pool is not enabled for the GateManager domain in which the SiteManager is connected.



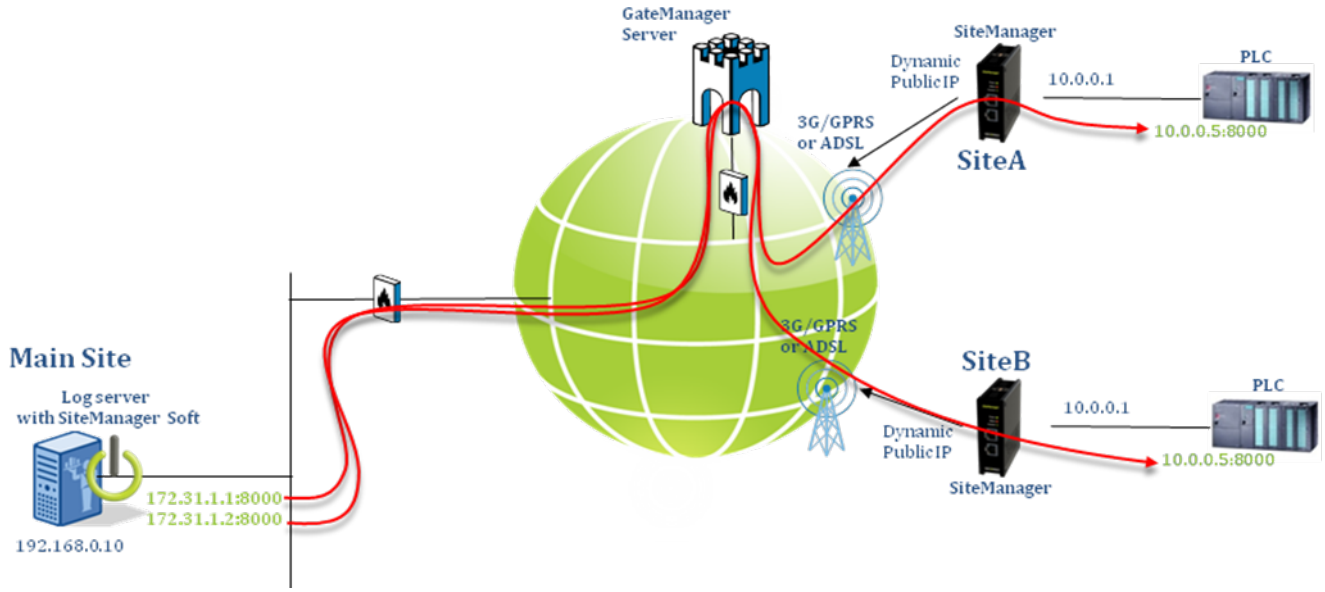
Once you make sure that everything is correct, you should Disable and Enable the Relay and the Status will turn **IDLE**

3. PULL-Data using SiteManager-to-SiteManager Relay-chain

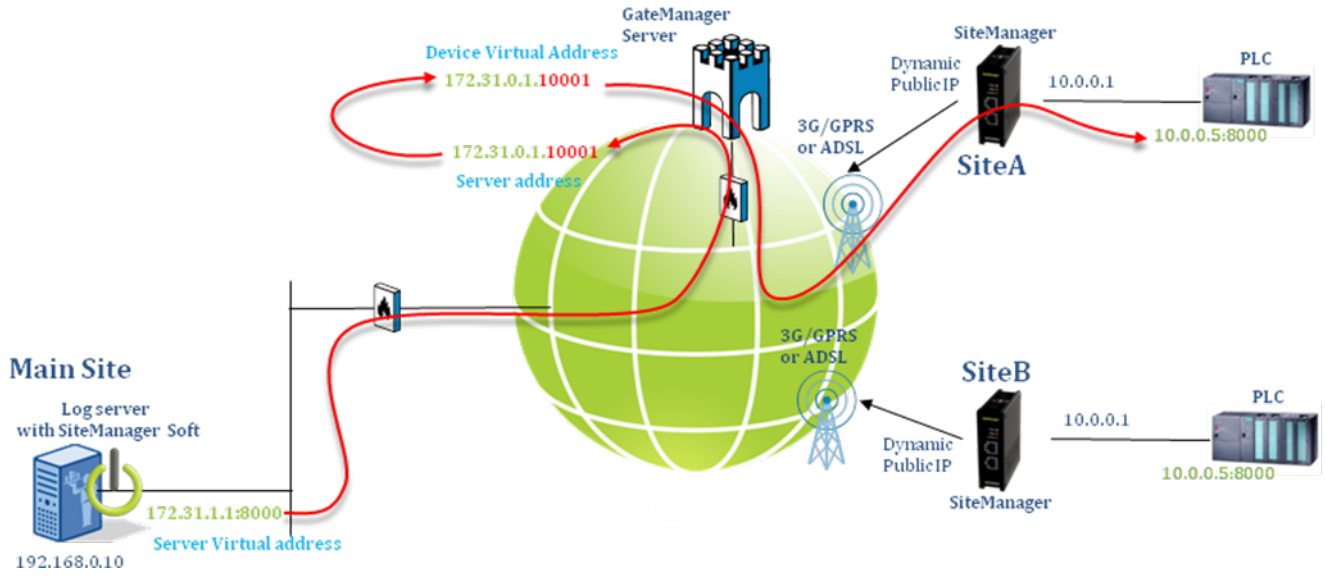
NOTE: that this scenario is not supported by the Secomea hosted servers. You must deploy an own GateManager server.

The typical scenario is that the log server only pulls log data from a single device at each site, using a single protocol, while other services, such as https, RDP and programming access, is done using LinkManager.

Also note that the following scenarios illustrate a SiteManager Soft at the Main Site. SiteManager Soft is a discontinued product so for the central site a SiteManager Embedded or SiteManager hardware unit should be used.



3.1. Principle of the SiteManager-to-SiteManager Relay chain



The principle is that IP addresses are relayed via that GateManager to a specified destination. ”Virtual addresses” are used for eliminating subnet conflicts.

This may be a bit complicated to explain and to understand in details, so instead we just define a recommended setup that does not require you to understand the mechanism in depth.

3.2. Planning and Server setup

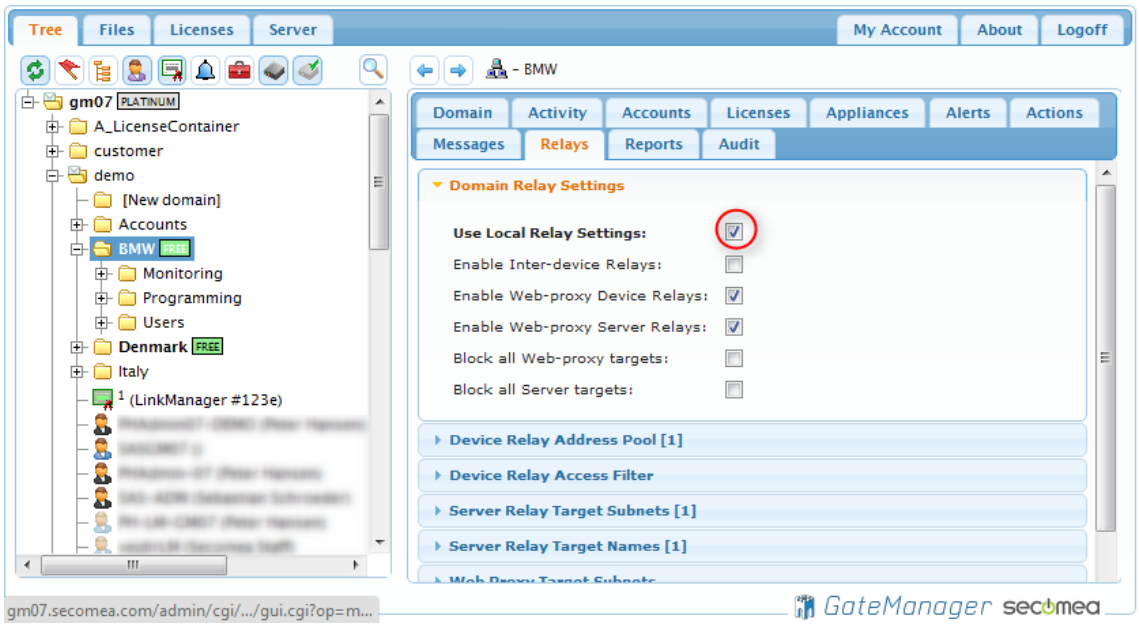
3.2.1. Get a “Server Address” granted

The GateManager owner has to define an address to be used as Server address.

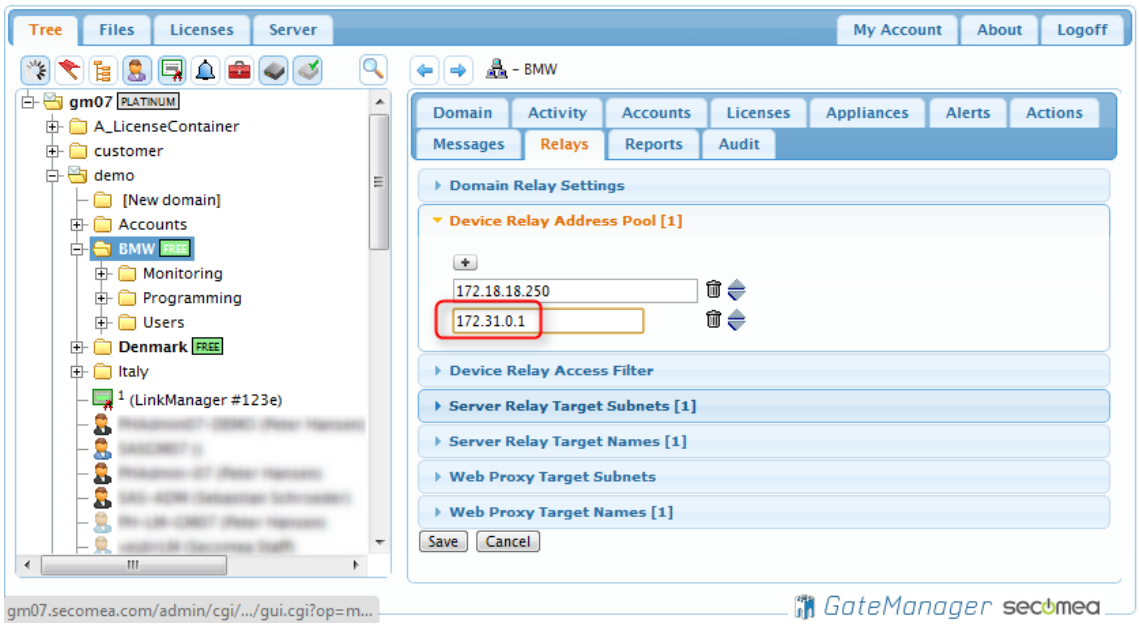
In this example we use **172.31.0.1**. Note that it only consist of a single address, and not a pool or subnet. We only need one, since we plan to differentiate sites on port numbers.

The following shows the settings needed on the GateManager. It is ONLY the GateManager Server Administrator that can configure these settings

First make sure **Use Local Relay Settings** is checked.



The check that the address is defined in your customer root domain. Note that it should be entered in the **Device Relay Address Pool** field.



This address is used for all sites. You don't really have to worry about what it does, since it is only used locally on the GateManager, and it is the same used for all devices.

3.2.2. Define "Device Virtual address"

This will always be identical to the "Server Address" above.

3.2.3. Define a virtual port

The real logging port has to be mapped to a virtual port in order to pass it via the server.

We choose port **10001** as the virtual representation for the log port 8000

3.2.4. Define a server Virtual Address pool

This is the "alias" addresses on which the log server accesses the individual devices at the remote sites.

In this case we have selected the subnet start 172.31.1.1, which is just above the Server Address subnet. If considering it a Class B subnet, it will give you the IP range 172.31.1.1 – 172.31.254.254

You could then make a table like this:

Device	Alias	Real device IP
PLC on Site A:	172.31.1.**1**	10.0.0.5
PLC on Site B:	172.31.1.**2**	10.0.0.5
PLC on Site C:	172.31.1.**3**	10.0.0.5

Etc.

As you may notice it is not really necessary to make the last column, since the PLC has the same IP addresses on all sites.

3.2.5. Install SiteManager at the log server site.

NOTE: The following illustrates a SiteManager Soft installed on the log server, which is a discontinued product. Instead a SiteManager Soft should be used (which is limited to 10 relays), or it can be a SiteManager hardware device installed in the same network as the log server (supports up to 100 relays.

The server does not need to have the IP address of the above illustration. It could be any IP address.

3.3. Configure the remote SiteManagers

The following is based on the IP addresses mentioned in the previous section.

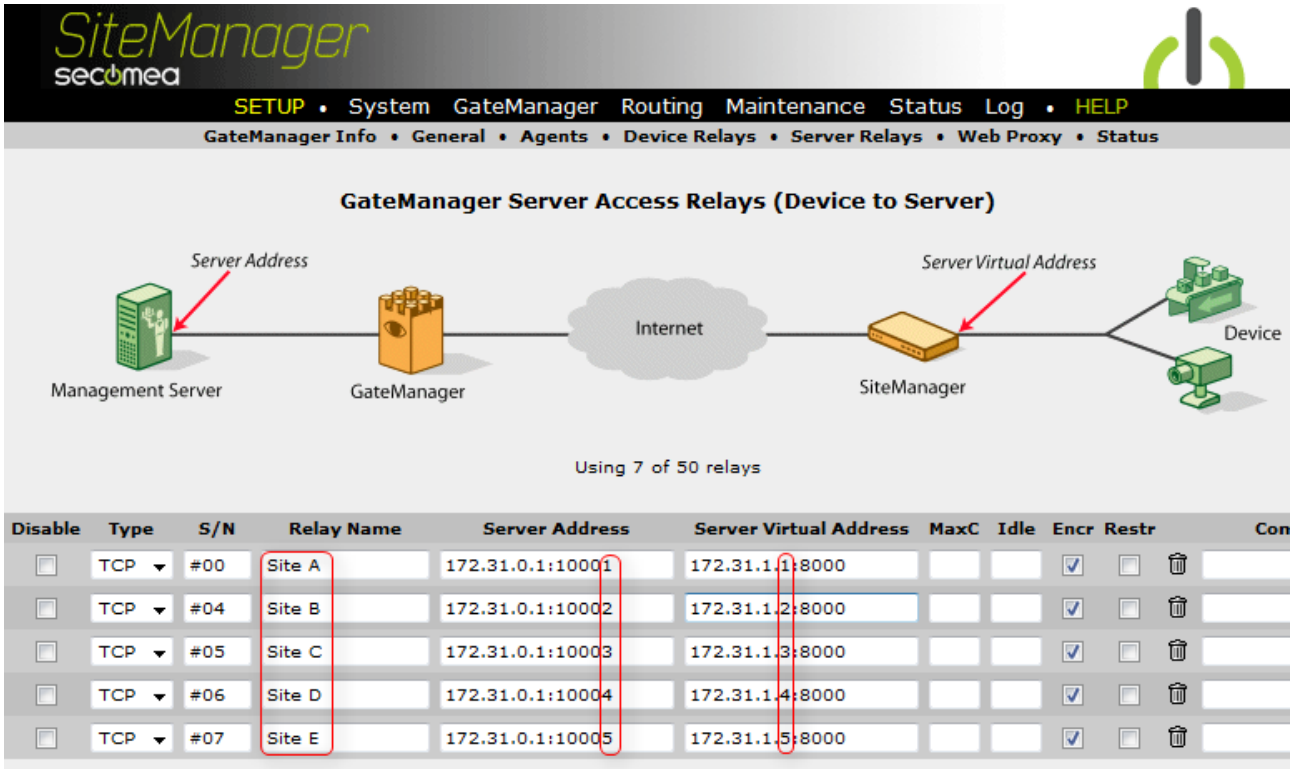
3.3.1. Install SiteManager at the remote site.

The SiteManager is installed on site as normal. Configure the DEV address to correspond to the device subnet. In this example 10.0.0.1

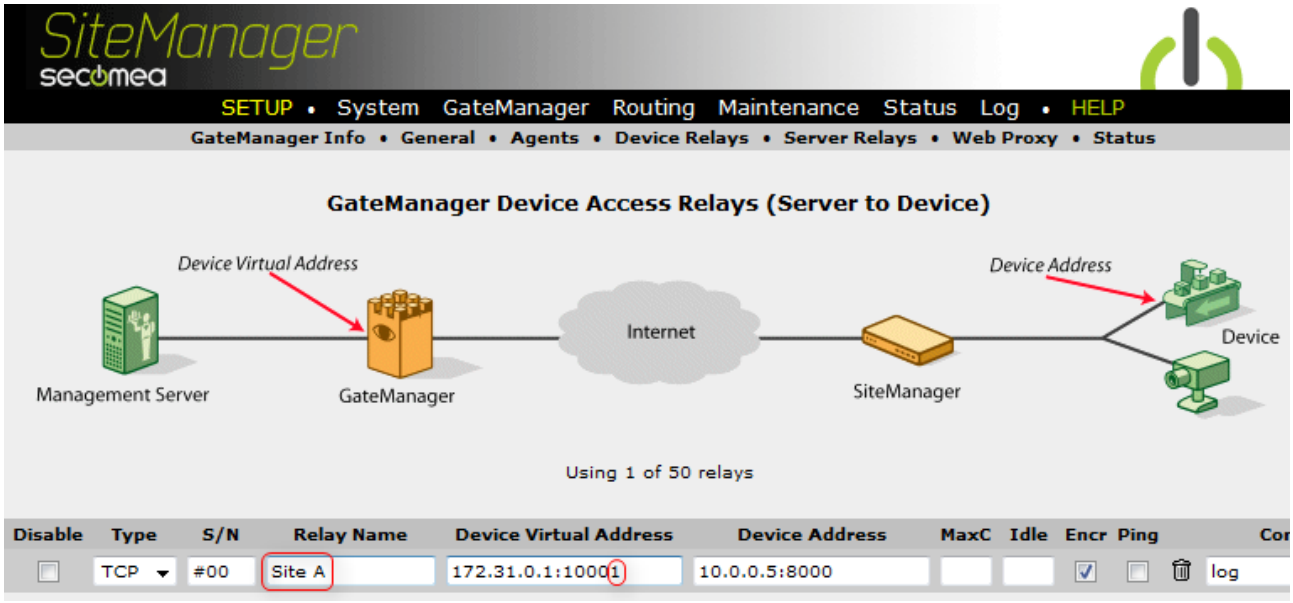
3.3.2. Configure Server Relays on the central SiteManager

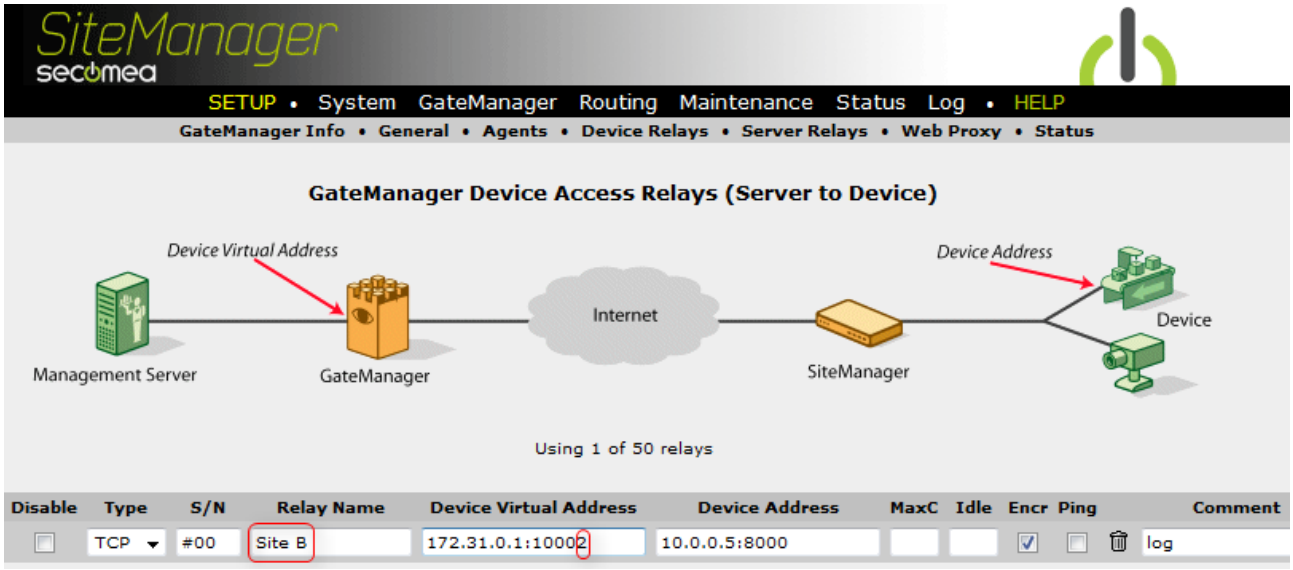
From the GateManager or the LinkManager enter the Web GUI of the SiteManager installed at the Log Server site and browse to the menu **GateManager → Server Relays**

Insert the definitions for each site:



On the SiteManagers at the remote sites insert the following corresponding Device Relays:





Etc.

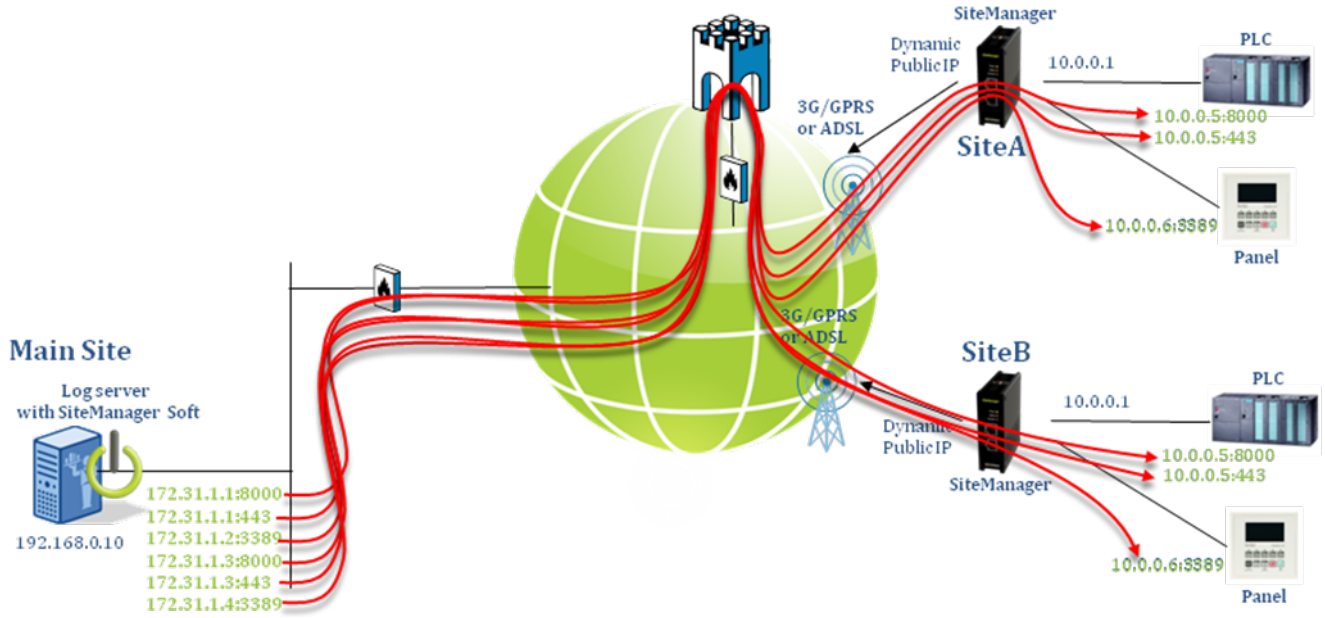
4. ADVANCED Pull-data Access using SiteManager-to-SiteManager Relay-chain

More complex scenarios are also possible, but require some more planning.

It should be considered to use EasyTunnel VPN if access to multiple devices with multiple protocols is required. Refer to the document “Logging via Site-Manager EasyTunnel Client – Deployment overview” for more information.

In this chapter we will work with the following setup. The central server needs access to 2 devices at each site, and by 3 different protocols.

Note: The following scenarios illustrate a SiteManager Soft at the Main Site. SiteManager Soft is a discontinued product so for the central site a SiteMan-ager Embedded or SiteManager hardware unit should be used.



4.1. Planning and Server setup

4.1.1. Get a “Server Address” pool granted

The GateManager owner has to allow a pool of addresses to be used as Server addresses. This pool must be granted by Secomea if using Secomea’s hosted GateManager.

In this example the pool is **172.31.0.0/24**. This means the range of “Server Addresses” is 172.31.0.1 – 172.31.0.254

The server addresses represents **different devices at the site**. So this means you can have up to 254 different devices at each site.

So you could define a table like this:

Siemens PLC:	172.31.0.1
Pro-face Panel:	172.31.0.2

Etc.

4.1.2. Define “Device Virtual address”

This will always be identical to the “Server Address” above.

4.1.3. Define a port mapping table

Instead of mapping on IP addresses we map by port numbers, which will also represent the sites.

We decide to construct the “virtual port” number like this:

Virtual “Site” port range (up to 999 different sites): xx001 - xx999

Virtual “Service” port range (max. 55 services/protocols): 10xxx – 65xxx

So you can define a “Site port” table like this:

Remote Site A: xx001

Remote Site B: xx002

Etc.

And a “Service port” table like this:

Siemens PLC log:	port 800	10xxx
Secure Web (https):	port 443	11xxx
MS RDP:	port 3389	12xxx

Etc.

For example port **11002** represents **https** access to devices on **Site B**

4.1.4. Define a server Virtual Address pool

This is the “alias” addresses the log server accesses the individual devices at the remote sites.

In this case we have selected the subnet start 172.31.1.1, which is just above the Server Address subnet. If considering it being a Class B subnet, it will give you the IP range 172.31.1.1 – 172.31.254.254

You could then make a table like this:

Device	**Alias**	**Real device IP**
Siemens PLC on Site A:	172.31.1.**1**	10.0.0.5
Pro-face panel on Site A:	172.31.1.**2**	10.0.0.6
Siemens PLC on Site B:	172.31.1.**3**	10.0.0.5
Pro-face Panel on Site B:	172.31.1.**4**	10.0.0.6

Etc.

As you may notice it may not really be necessary to make the last column, since the equipment has the same IP addresses on all sites. So instead make a separate table like this, which is common for all sites:

Siemens PLC: 10.0.0.5

Pro-face panel: 10.0.0.6

Etc.

4.1.5. Install SiteManager at the log server site.

This is only done once.

NOTE: The following illustrates a SiteManager Soft installed on the log server, which is a discontinued product. Instead a SiteManager Soft should be used (which is limited to 10 relays), or it can be a SiteManager hardware device installed in the same network as the log server (supports up to 100 relays.

The server does not need to have the IP address of the above illustration. It could be any IP address.

4.2. Configuring SiteManagers

The following is based on the IP addresses in the previous section.

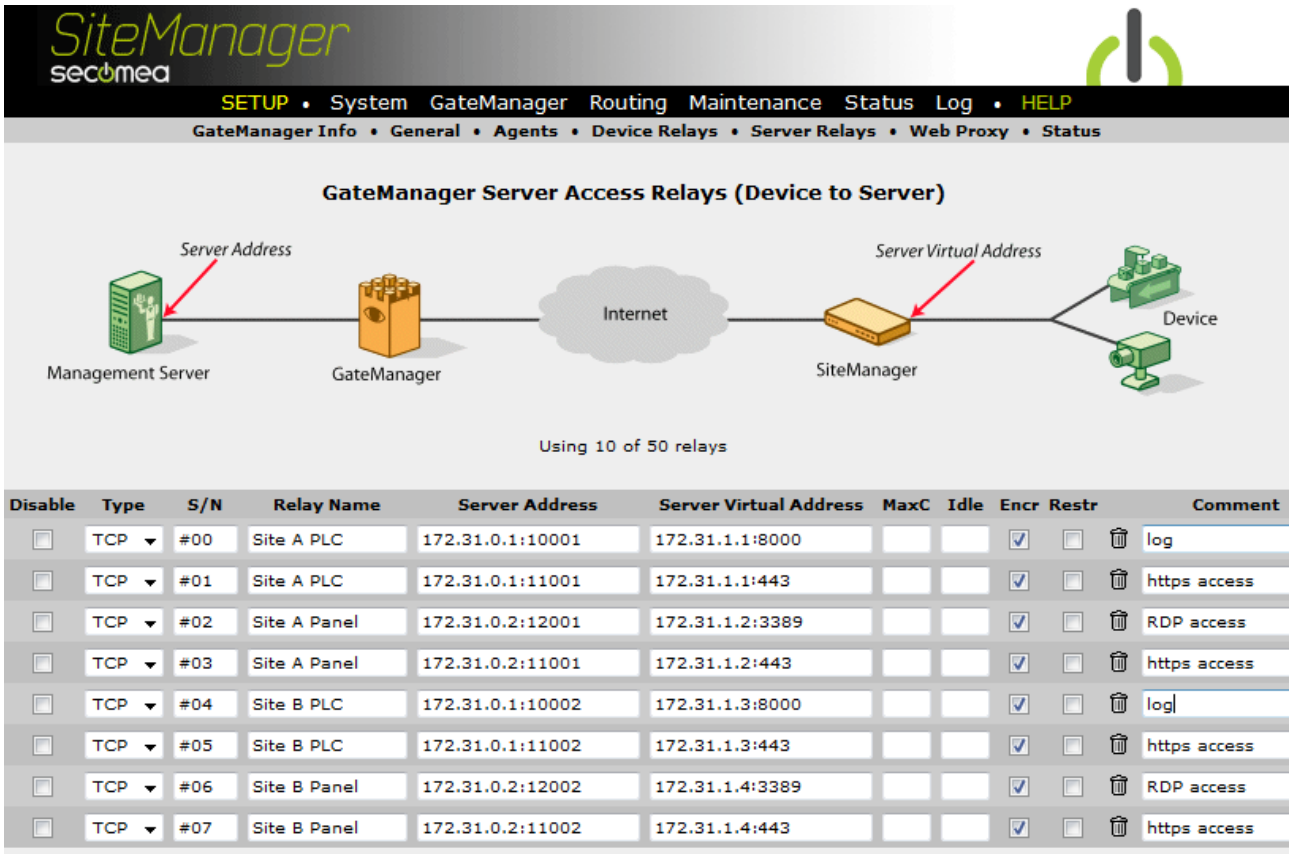
4.2.1. Install SiteManager at the remote site.

The SiteManager is installed on site as normal. Configure the DEV address to correspond to the device subnet. In this example 10.0.0.1

4.2.2. Configure Server Relays on the central SiteManager

From the GateManager or the LinkManager enter the Web GUI of the SiteManager and browse to **GateManager → Server Relays**

Insert the definitions for Site A and Site B:

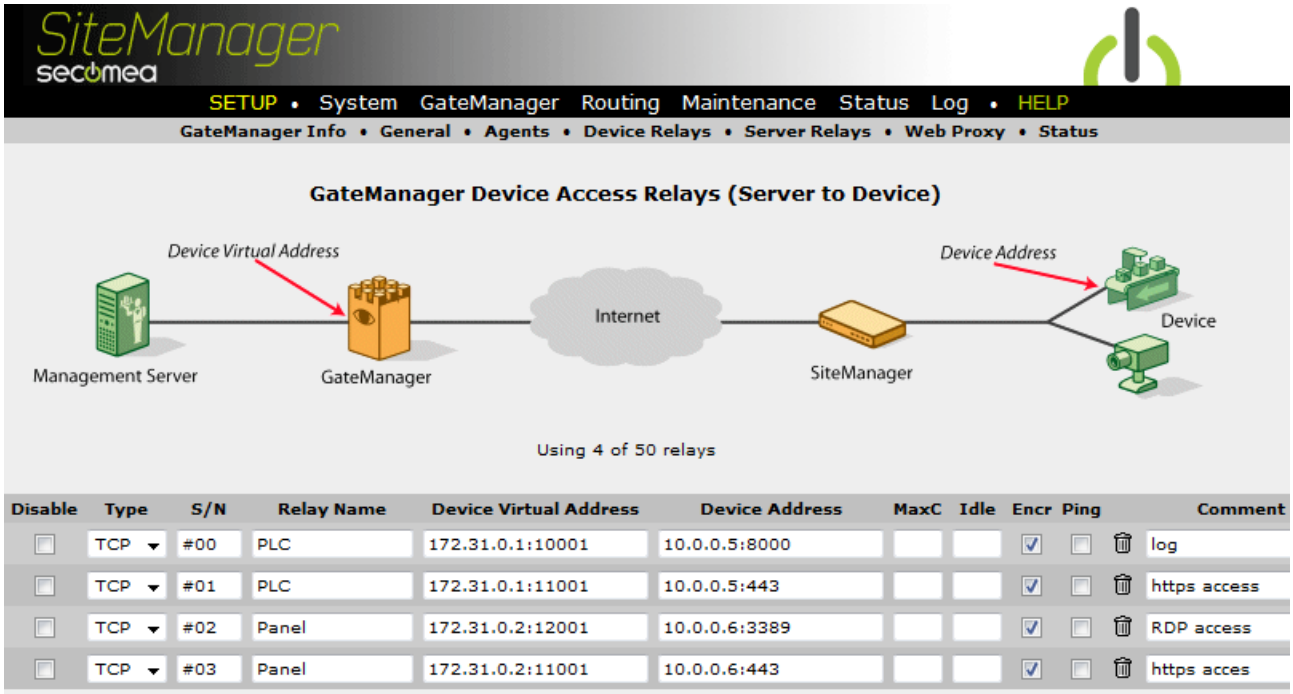


Disable	Type	S/N	Relay Name	Server Address	Server Virtual Address	MaxC	Idle	Encr	Restr	Comment
☐	TCP	#00	Site A PLC	172.31.0.1:10001	172.31.1.1:8000			☑	☐	log
☐	TCP	#01	Site A PLC	172.31.0.1:11001	172.31.1.1:443			☑	☐	https access
☐	TCP	#02	Site A Panel	172.31.0.2:12001	172.31.1.2:3389			☑	☐	RDP access
☐	TCP	#03	Site A Panel	172.31.0.2:11001	172.31.1.2:443			☑	☐	https access
☐	TCP	#04	Site B PLC	172.31.0.1:10002	172.31.1.3:8000			☑	☐	log
☐	TCP	#05	Site B PLC	172.31.0.1:11002	172.31.1.3:443			☑	☐	https access
☐	TCP	#06	Site B Panel	172.31.0.2:12002	172.31.1.4:3389			☑	☐	RDP access
☐	TCP	#07	Site B Panel	172.31.0.2:11002	172.31.1.4:443			☑	☐	https access

4.2.3. Insert the Device Relays on the remote SiteManagers

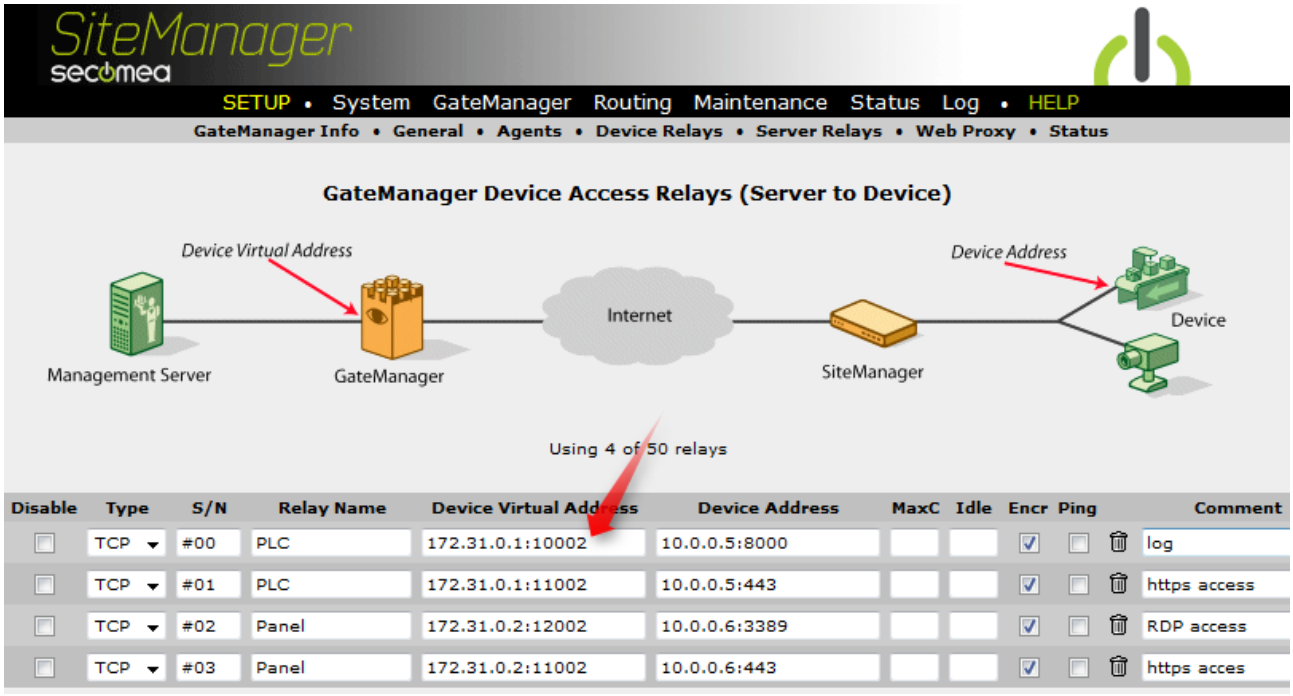
From the GateManager or the LinkManager enter the Web GUI of the Site-Manager at Site A, and browse to **GateManager → Device Relays**

Insert the definitions for the PLC and the Panel:



Disable	Type	S/N	Relay Name	Device Virtual Address	Device Address	MaxC	Idle	Encr	Ping	Comment
☐	TCP	#00	PLC	172.31.0.1:10001	10.0.0.5:8000			☑	☐	log
☐	TCP	#01	PLC	172.31.0.1:11001	10.0.0.5:443			☑	☐	https access
☐	TCP	#02	Panel	172.31.0.2:12001	10.0.0.6:3389			☑	☐	RDP access
☐	TCP	#03	Panel	172.31.0.2:11001	10.0.0.6:443			☑	☐	https acces

Do the same on the SiteManager at Site B:



Disable	Type	S/N	Relay Name	Device Virtual Address	Device Address	MaxC	Idle	Encr	Ping	Comment
☐	TCP	#00	PLC	172.31.0.1:10002	10.0.0.5:8000			☑	☐	log
☐	TCP	#01	PLC	172.31.0.1:11002	10.0.0.5:443			☑	☐	https access
☐	TCP	#02	Panel	172.31.0.2:12002	10.0.0.6:3389			☑	☐	RDP access
☐	TCP	#03	Panel	172.31.0.2:11002	10.0.0.6:443			☑	☐	https acces

Notice that the only difference from SiteA and SiteB is the last three digits of the port number (001 or 002).

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