Logging via SiteManager EasyTunnel Client
Deployment Overview

This guide describes the deployment process when using the SiteManager EasyTunnel VPN Client function for fetching log data from devices to a central server, and optionally to access other services at the devices from the central network.

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: 1.4, August 2014

secomea

Table of Contents

Introduction

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

Relay Chains vs. EasyTunnel

Relay Chains are not covered in this document for more information about this see the Secomea website for “Logging via SiteManager Relay Chains”. This document focuses on the EasyTunnel VPN solution.

A. Relay chains

Relay links between a SiteManager at the server side via GateManager 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.

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

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.

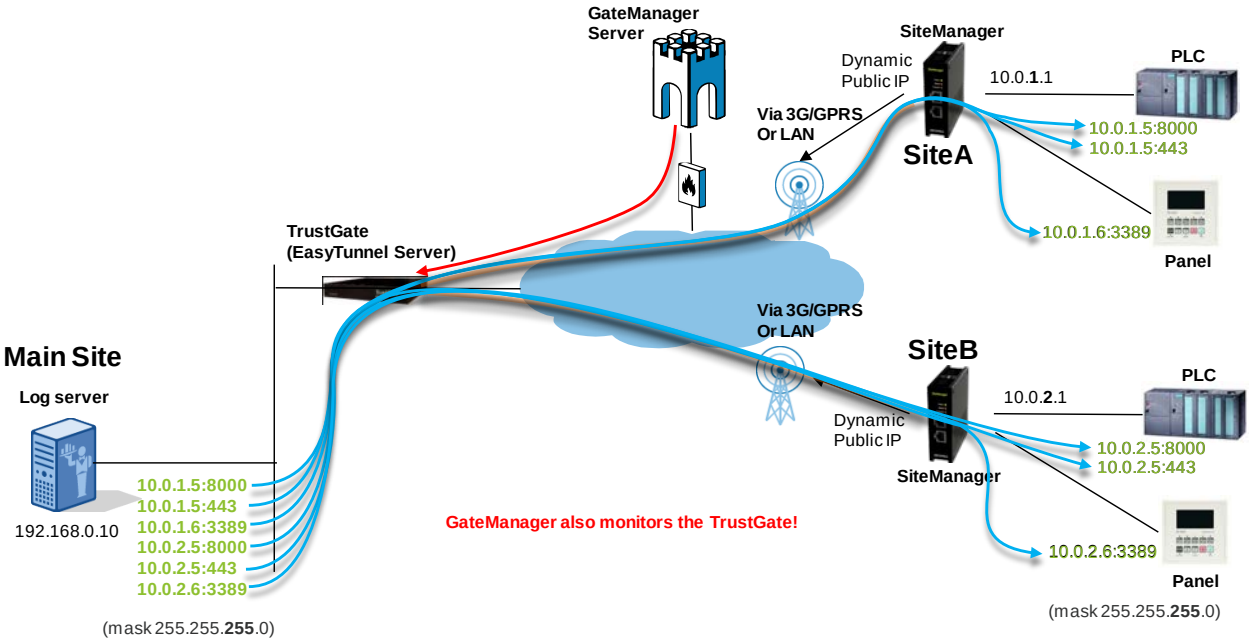
Advantages:

- 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.

1. Principle of the EasyTunnel VPN



- EasyTunnel is basically IPSec based VPN with AES encryption that is packaged in a way that makes it extremely easy to deploy.
- The TrustGate EasyTunnel Server is a Secomea product and has the same user interface as the SiteManager. It also supports many of the same features for administration.
- The EasyTunnel Client establishes an IPSec based and AES encrypted VPN tunnel from the SiteManager's DEV1 network to an EasyTunnel Server in form of a Secomea TrustGate appliance. Refer to the Office Network Solutions section on www.secomea.com for more information about compatible TrustGate products.
- EasyTunnel works completely independent of the GateManager connection to the SiteManager. The VPN tunnel is made directly between the SiteManager and the EasyTunnel Server, and is not dependent of the SiteManager being connected to a GateManager.
- The EasyTunnel Server must be accessible by a Public IP address. The EasyTunnel Client in the SiteManager does not need to have a public IP address but can be placed behind a NAT firewall. The firewall must allow UDP 500 and UDP 4500 outgoing.
- Although EasyTunnel is considerably easier to configure than ordinary IPSec based VPN, it requires the same precautions as standard VPN tunnels to be taken, in order to avoid subnet conflicts between the local networks at each end of the tunnel. Any NAT rules to solve subnet conflicts must be made at the EasyTunnel Server end.

2. Planning the EasyTunnel VPN infrastructure

2.1. Decide remote site Subnets.

You should decide on subnet architecture for the remote sites. The subnets of the remote sites must be unique, and should not be clashing with any subnet already used or reachable via routers on the central site.

So you can define a table like this:

Remote Site A:	10.0.1.0 / 255.255.255.0
Remote Site B:	10.0.2.0 / 255.255.255.0

Etc.

This will provide you 253 addresses at each site.

If you do not want to use an entire Class C subnet as each site, you could define the range narrower or tunnel to the IP address directly. In this example you will have 2 addresses at each site:

Remote Site A:	10.0.1.0 / 255.255.255.252 (10.0.1.1 & 10.0.1.2)
Remote Site B:	10.0.1.4 / 255.255.255.252 (10.0.1.5 & 10.0.1.6)

Etc.

Refer to publically available information to learn more about designing your VPN network. For subnet calculations this is a good tool: http://www.subnet-calculator.com/

2.2. Decide on a TrustGate EasyTunnel Server.

Different models exists supporting different number of EasyTunnels:

TrustGate 61	25 tunnels
TrustGate 160	100 tunnels
TrustGate 260	600 tunnels
TrustGate 460R	2000 tunnels

2.3. Deploy the EasyTunnel server

The TrustGate EasyTunnel server must either have a public IP address for the EasyTunnel clients to access, or be placed behind a firewall with a public IP address, and which forwards to the TrustGate UDP port 500, 4500 and a selectable service port (aka EasyTunnel deployment port), which could be e.g. port 444.

Note that you can in fact use the TrustGate as your corporate firewall as it is includes a state full inspection firewall, as well as NAT engine.

If you are already using port 500 and 4500, i.e. for a VPN concentrator, you can move the EasyTunnel communication to port 501/4501. In order to do so, append the number **:501** to the IP address of the EasyTunnel server.

2.4. Make routes to the EasyTunnel remote networks

If the TrustGate is used as DHCP server, the central LAN network will automatically get the TrustGate as gateway to the tunnels.

If not, you will have to add information into your corporate server or firewall, about the TrustGate LAN address being the gateway to the tunnel subnets.

If it is only a single server that should have access to the tunnels, you only have to add the route entries for the tunnel subnets on that PC.

3. EasyTunnel Deployment

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

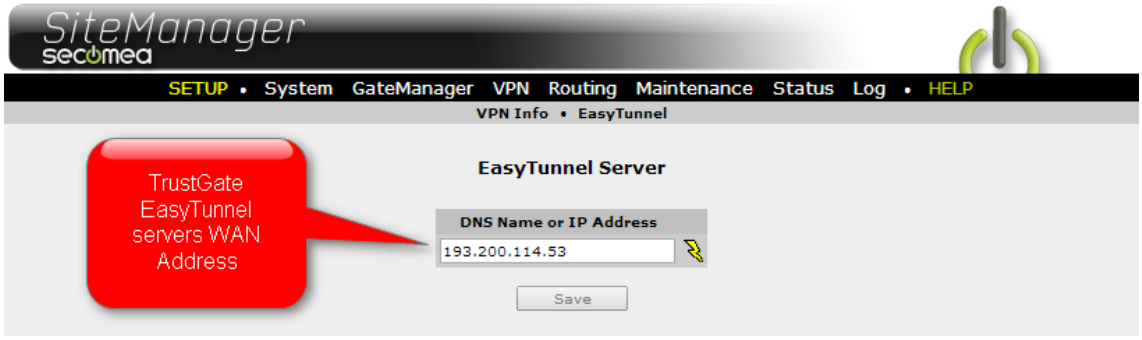
3.1. Install the SiteManager

The SiteManager is installed on site as normal. Actually you do not need to configure the DEV network, as the DEV1 network of the SiteManager will automatically be forced to the subnet defined by the LAN Address of the EasyTunnel Client configured on the EasyTunnel Server.

3.2. Enable the EasyTunnel client on the SiteManager.

From the GateManager or the LinkManager access the Web GUI of the SiteManager installed at the remote site and select VPN → EasyTunnel.

When asked about the EasyTunnel Server address, enter the IP address of the EasyTunnel Server (The WAN address of the TrustGate), or if another NAT Firewall is placed in front of the TrustGate, enter the IP address on the NAT Firewall that is forwarded to the TrustGate WAN address.



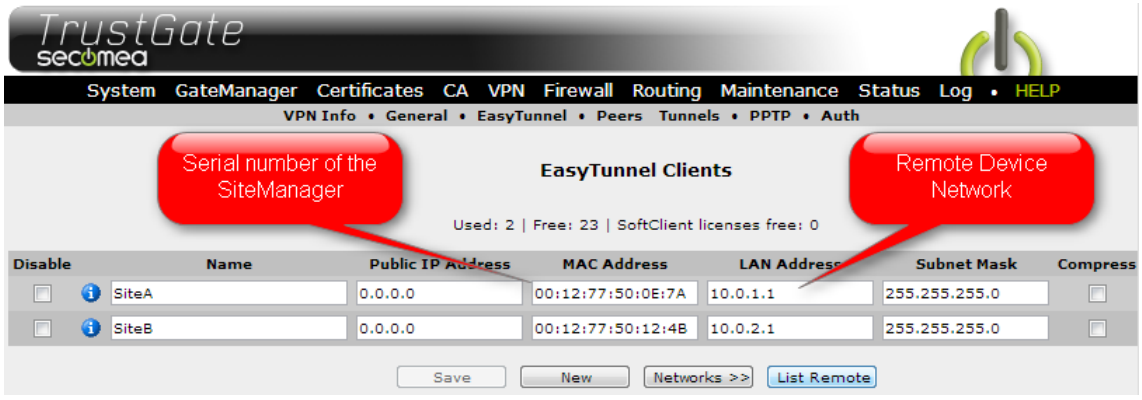
Note: If you have moved the EasyTunnel server to port 501/4501 (see. section 2.3), you need to tell the SiteManager to connect to port 501. In order to do so, append the number :501 to the IP address of the EasyTunnel server (in this case 193.200.114.53:501)

Click the lightning icon to make the SiteManager start the polling process towards the server.

Nothing more is needed on the SiteManager

3.3. Create the EasyTunnel on the TrustGate EasyTunnel Server

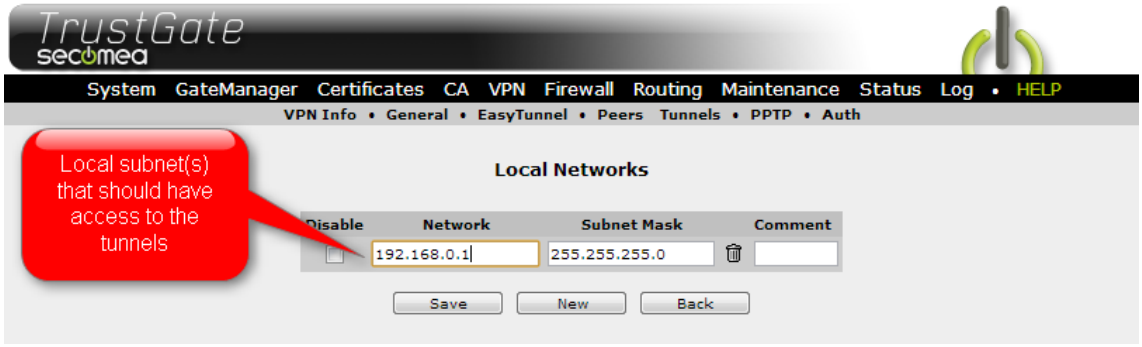
From the GateManager or the LinkManager access the Web GUI of the EasyTunnel server installed at the central site and select VPN → EasyTunnel.



Note that the Public IP address is set to **0.0.0.0**. This is because the SiteManagers most likely do not have public addresses, but are located behind NAT firewalls.

When pressing Save, the tunnels are established from the SiteManagers to the EasyTunnel server.

Click on the [Networks >>] button below the EasyTunnel Clients and define the local networks on the TrustGate LAN side, that should have access to the tunnels. This would typically the LAN network where the logging server that should collect data via the tunnels is located.



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.