

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: 1.1, February 2012



Table of Contents

1. Use Case / Requirements	3
2. Solution models	3
2.1. SiteManager to SiteManager Relay chains	3
2.2. TrustGate to SiteManager EasyTunnel VPN	3
3. Principle of the EasyTunnel VPN	4
4. Planning the EasyTunnel VPN infrastructure	5
4.1. Decide remote site Subnets.	5
4.2. Decide on a TrustGate EasyTunnel Server.	5
4.3. Deploy the EasyTunnel server	5
4.4. Make routes to the EasyTunnel subnets	5
5. EasyTunnel Deployment	6
5.1. Install the SiteManager	6
5.2. Enable the EasyTunnel client on the SiteManager.	6
5.3. Create the EasyTunnel on the TrustGate EasyTunnel Server	6
6. Notices	8

1. Use Case / Requirements

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.

2. Solution models

2.1. SiteManager to SiteManager Relay chains

Relay links between a SiteManager Soft on the server site 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.
- No Public IP address required in either end
- Ideal for collection of log data.

Disadvantages:

- Protocols with IP addressing in the payload (such as FTP) are currently not supported.
- All communication travel via the GateManager. Use of bandwidth intensive and timing critical applications are not recommended.
- The device network behind the SiteManagers must have different subnets.
- Less ideal if logging multiple devices at each site with different services (protocols).

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

2.2. 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:

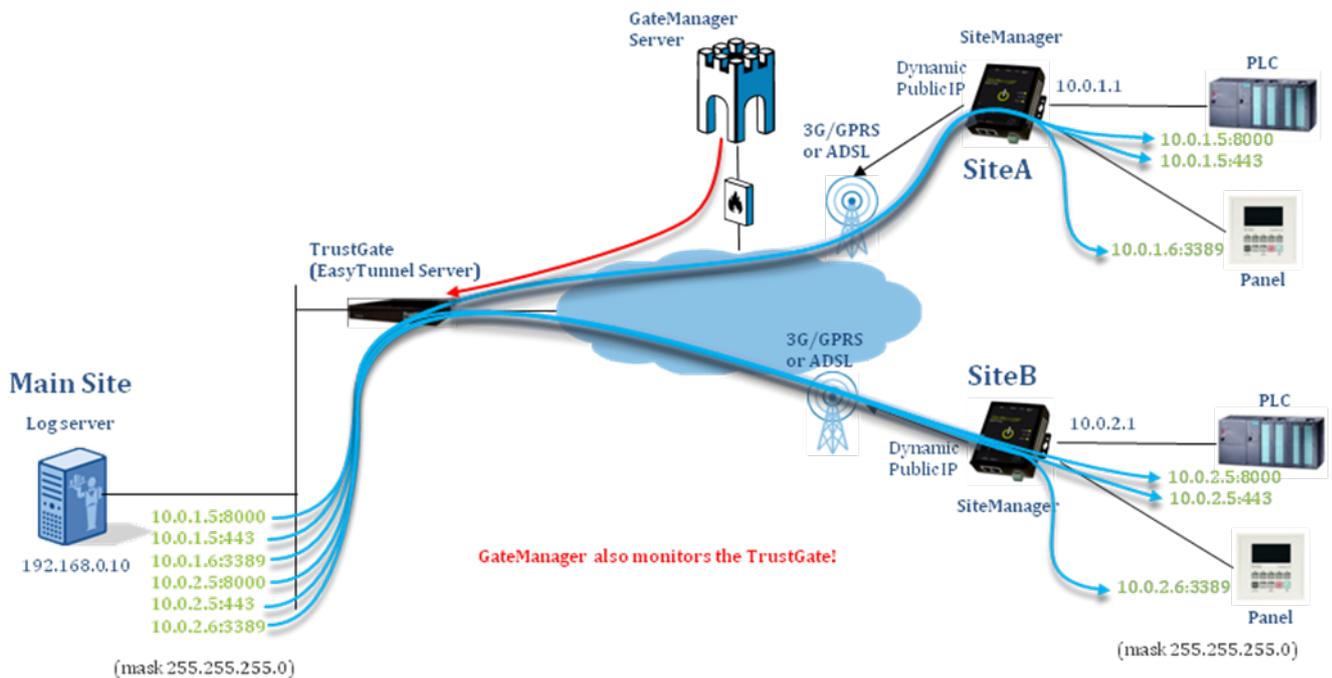
- Routing challenging protocols and services can be accessed (.e.g. FTP)
- Ideal for Video streaming and other bandwidth intensive and timing critical data
- You get access to the entire device network and therefore do not have to be concerned about allowing specific IP addresses or protocols

Disadvantages:

- The TrustGate must be available on a public address
- UDP port 500 and 4500 must 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 may dislike.

This document focuses on this solution.

3. 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 IPSecbased 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.

4. Planning the EasyTunnel VPN infrastructure

4.1. 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/>

4.2. 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

4.3. 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 includes a state full inspection firewall, as well as NAT engine.

4.4. Make routes to the EasyTunnel subnets

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.

5. EasyTunnel Deployment

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

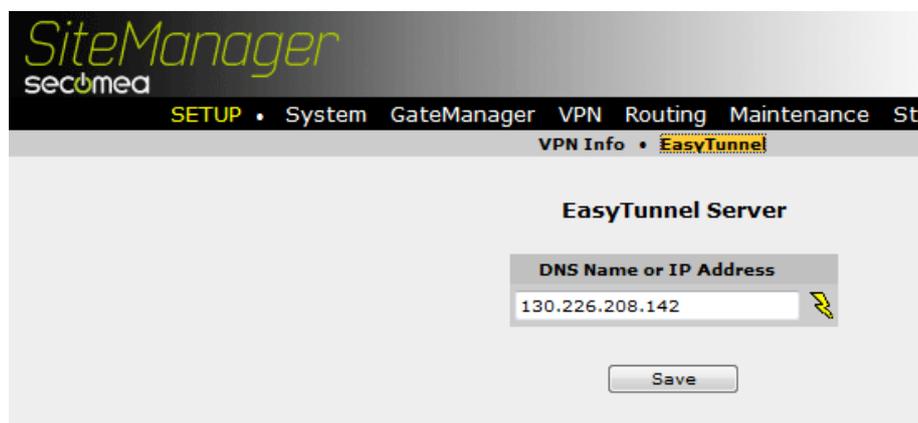
5.1. Install the SiteManager

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 set to the subnet defined by the LAN Address of the EasyTunnel configured on the EasyTunnel Server.

5.2. Enable the EasyTunnel client on the SiteManager.

From the GateManager or the LinkManager make a “Go To Appliance” to enter 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)



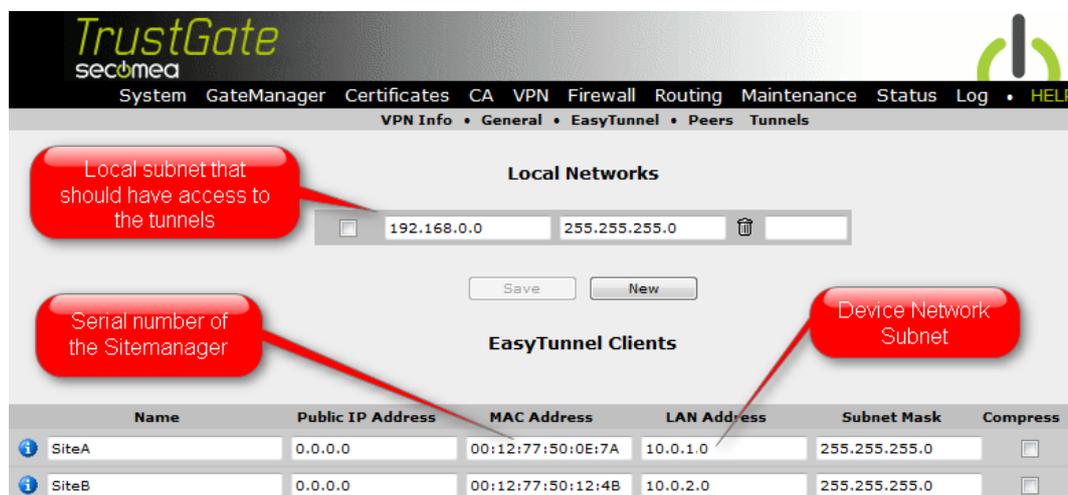
The screenshot shows the SiteManager web interface. The breadcrumb trail is: SETUP • System GateManager VPN Routing Maintenance St. The current page is VPN Info • EasyTunnel. The main heading is EasyTunnel Server. There is a text input field labeled "DNS Name or IP Address" containing the value "130.226.208.142". To the right of the input field is a lightning bolt icon. Below the input field is a "Save" button.

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

Nothing more is needed on the SiteManager

5.3. Create the EasyTunnel on the TrustGate EasyTunnel Server

From the GateManager or the LinkManager make a “Go To Appliance” to enter the Web GUI of the EasyTunnel server installed at the central site and select VPN → EasyTunnel.



The screenshot shows the TrustGate web interface. The breadcrumb trail is: VPN Info • General • EasyTunnel • Peers Tunnels. The page is divided into two sections: Local Networks and EasyTunnel Clients.

Local Networks: A text input field contains "192.168.0.0" and "255.255.255.0". A red callout bubble points to this field with the text: "Local subnet that should have access to the tunnels".

EasyTunnel Clients: A table lists two clients, SiteA and SiteB. A red callout bubble points to the LAN Address field of SiteA with the text: "Serial number of the Sitemanager". Another red callout bubble points to the LAN Address field of SiteB with the text: "Device Network Subnet".

Name	Public IP Address	MAC Address	LAN Address	Subnet Mask	Compress
SiteA	0.0.0.0	00:12:77:50:0E:7A	10.0.1.0	255.255.255.0	<input type="checkbox"/>
SiteB	0.0.0.0	00:12:77:50:12:4B	10.0.2.0	255.255.255.0	<input type="checkbox"/>

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.

6. Notices

Publication and copyright

© **Copyright Secomea A/S 2012.** All rights reserved. You may download and print a copy for your own use. As a high-level administrator, you may use whatever you like from contents of this document to create your own instructions for deploying our products. Otherwise, no part of this document may be copied or reproduced in any way, without the written consent of Secomea A/S. We would appreciate getting a copy of the material you produce in order to make our own material better and – if you give us permission – to inspire other users.

Trademarks

SiteManager™, LinkManager™ and GateManager™ are trademarks of Secomea A/S. Other trademarks are the property of their respective owners.

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.