Astaro Security Gateway V8

Remote Access via L2TP over IPSec

Configuring ASG and Client

Author: Richard Striegel
Contact: documentation@astaro.com
Document version: 1.000
Date: 2011-01-26
Status: Public

Contents

Page

1. Introduction ................................................................. 2
2. Remote Access via L2TP over IPSec ................................. 2
  2.1. Configuration of the Astaro Security Gateway .............. 3
  2.2. Configuration of the Remote Client ............................. 11
  2.2.1. Astaro User Portal: Getting Preshared Keys .......... 11
  2.2.2. Remote Client: Windows XP/Vista/7 with Preshared Key..12
  2.2.3. Remote Client: Windows 2000/XP/Vista/7 with X.509 Certificates ......................................................... 14
  2.2.4. Remote Client: Windows 2000 with Preshared Keys .. 16

This document may not be copied or distributed by any means, electronically or mechanically, in whole or in part, for any reason, without the express written permission of Astaro GmbH & Co. KG.

© 2011 Astaro GmbH & Co. KG. All rights reserved. An der RaumFabrik 33a, 76227 Karlsruhe, Germany, http://www.astaro.com

Astaro Security Gateway and WebAdmin are trademarks of Astaro.
All further trademarks are the property of their respective owners.

No guarantee is given for the correctness of the information contained in this document.
1. Introduction

This guide contains complementary information on the Administration Guide and the Online Help. If you are not sure whether you have the current version of this guide, you can download it from the following Internet address:

http://www.astaro.com/kb

If you have questions or find errors in the guide, please, contact us under the following e-mail address:

documentation@astaro.com

For further help use our support-forum under ...

http://www.astaro.org

... or use the Astaro Support offers ...

http://www.astaro.com/support

2. Remote Access via L2TP over IPSec

This guide describes step by step the configuration of a remote access to the Astaro Security Gateway by using **L2TP over IPSec**. **L2TP over IPSec** is a combination of the **Layer 2 Tunneling Protocol** and of the **IPSec standard protocol**. **L2TP over IPSec** allows you, while providing the same functions as PPTP, to give individual hosts access to your network through an encrypted IPSec tunnel. The structure is described in the following chart. On Microsoft Windows systems, **L2TP over IPSec** is easy to set-up, and requires no special client software.

The **Astaro User Portal** offers the necessary keys and configuration guides. You should get the log-in data for the user portal from your system administrator.

For the Microsoft Windows systems 98, ME and NT Workstation 4.0, **Microsoft L2TP/IPSec VPN Client** must first be installed. This client is available from Microsoft at:

2.1. Configuration of the Astaro Security Gateway

The Astaro Security Gateway is configured via the web based WebAdmin configuration tool from the administration PC. Opening and using this configuration tool is extensively described in the Astaro Security Gateway V8 administration guide.

1. **Define the user account for the remote host:**

Open the **Users >> Users** page.

Define a new user account for the remote client. With remote access via L2TP this user account is necessary for accessing the Astaro User Portal and for VPN.

More detailed information on the configuration of a User Account and detailed explanations of the individual settings can be found in the Astaro Security Gateway V8 administration guide in chapter xx.

Make the following settings:

**Username:** Enter a specific user name (e.g. *gforeman*). In doing so remember that the remote user will need this username later to log in to the Astaro User Portal.

**Real name:** Enter the full name of the remote user (e.g. *George Foreman*).

**Email address:** Enter the e-mail address of the user. When you specify an e-mail address, a X.509 certificate for this user will be generated automatically while creating the
user account, using the e-mail address as the certificate's VPN ID. The certificate will be displayed on the Certificate Management >> Certificates tab.

**Authentication**: For the Remote Access via L2TP over IPSec the Local and RADIUS authentication methods are supported. With the Local authentication method the following two entry menus will be displayed for the definition of the password. In doing so remember that also the remote user will need this user name later to log in to the Astaro User Portal.

**Password**: Enter the password for the user. In doing so remember that the remote user will need this password later to log in to the Astaro User Portal.

**Repeat**: Confirm the password.

**Use static remote access IP (optional)**: Each remote access user can be assigned to a specific IP address. The assigned IP address must not originate from the IP address pool. During the dial-up the address is automatically assigned to the host. Enter the static IP address in the RAS address box.

**Comment (optional)**: Enter a description or additional information on the user.

Save your settings by clicking on Save.
2. **Configure the L2TP over IPSec remote access:**

Open the Remote Access >> L2TP over IPSec page.

On the Global tab enable the IPSec over IPSec remote access by clicking the Enable button.

The status light shows amber and the page becomes editable.

More detailed information on the configuration of a L2TP over IPSec Remote Access and detailed explanations of the individual settings can be found in the Astaro Security Gateway V8 administration guide in chapter 13.

<table>
<thead>
<tr>
<th>Server settings</th>
</tr>
</thead>
</table>

**Interface**: Select the network interface to use for L2TP access.

**Authentication mode**: L2TP over IPSec remote access supports authentication based on **Preshared Keys** or **X.509 CA Check**. The settings in this section depend on the authentication method. To use **L2TP over IPSec** as an easy PPTP alternative in Windows XP, select **Preshared Key** as the authentication mode.

**Preshared Key**: Enter the shared secret. This shared secret is a secure phrase or password that is used to set up a secure tunnel.
Repeat: Confirm the shared secret.

Security Note:
Use a secure password! Your name spelled backwards is, for example, not a secure password – while something like xFT35!4z would be. Ensure that this password does not fall into the hands of unauthorized third parties. With this password, an attacker can build a connection to the internal network. We recommend changing this password at regular intervals.

If you choose **X.509 CA Check**, the following dialog box will be displayed.

**Certificate**: Select the local X.509 certificate to authenticate the server.

Save your settings by clicking on **Apply**.

| IP address assignment

**Assign IP addresses by**: The IP addresses can either be assigned from a predefined **VPN IP Pool (L2TP)** during the dial-up or can be automatically requested from a **DHCP server**. Please note that the local DHCP server is not supported. The DHCP server to be specified here must be running on a physically different system.

**IP address pool**: The default settings assign addresses from the private IP space 10.242.3.x/24. This network is called the **VPN Pool (L2TP)**. If you wish to use a different network, simply change the definition of the **VPN Pool (L2TP)** on the **Definitions >> Networks** page.

Note: If you use private IP addresses for the **IP address pool** and you wish **L2TP**-connected computers to be allowed to access the Internet, appropriate **Masquerading** or **NAT** rules must be in place.

**DHCP server**: This section will be displayed if you have selected the **DHCP server** setting in the **Assign IP addresses by** section. Select the DHCP server here. Clicking the folder icon opens a list that displays all networks and hosts, which had been defined on the **Definitions >> Networks** page. Alternatively, you can create another IP address pool by clicking the plus icon.

... **reachable on interface**: Define the network card through which the DHCP server is connected. Note that the DHCP does not have to be directly connected to the interface - it can also be accessed through a router.

Save your settings by clicking on **Apply**.

| Access control

Use the **Access control** section to select an authentication method.
L2TP remote access supports **Local** and **RADIUS** authentication. Users that are authenticated against other methods will not work. For local users, Astaro Security Gateway supports the authentication protocols MS-CHAPv2 and PAP (local authentication). By default, a MS Windows client negotiates MS-CHAPv2.

You can use RADIUS authentication, if you have defined a RADIUS server on the **Users >> Authentication >> RADIUS** tab. In conjunction with RADIUS authentication, Astaro Security Gateway supports the authentication protocols MS-CHAPv2, MS-CHAP, CHAP and PAP. The authentication requests are forwarded to the RADIUS server. The L2TP module sends the following string as NAS-ID to the RADIUS server: **l2tp**. The authentication algorithm gets automatically negotiated between client and server.

The configuration of the **Microsoft IAS RADIUS** server and the configuration of RADIUS within **WebAdmin** is described in the **Astaro Security Gateway V8** administration guide in chapter xx.

**Authentication via**: Select the authentication method.

**Users and groups**: When using **Local** authentication, please also select the users and groups that should be able to use L2TP remote access.

Save your settings by clicking on **Apply**.

3. **Configure the advanced L2TP over IPSec remote access settings**:

   Open the **Remote Access >> L2TP over IPSec >> Advanced** tab.

   **Debug mode**

   This options controls how much debug output is generated in the log files. Select this option if you encounter connection problems and need detailed information about the negotiation of client parameters, for example.

   Save your setting by clicking on **Apply**.
4. **Configure the advanced remote access settings:**

Open the **Remote Access >> Advanced** page.

This page allows you to define name servers (DNS and WINS) and the name service domain, which should be assigned to hosts during the connection establishment.

5. **Define the packet filter rule:**

Open the **Network Security >> Packet Filter >> Rules** tab.

After clicking on the **New rule** button the dialog box for new rules will appear. Create a new rule for the access to the local internal network.

**Source:** Remote host or user (in this example: gforeman).
Service: Set the service.

Destination: The allowed internal network (in this example: Internal (Network)).

Action: Allow.

Confirm your settings by clicking on Save.

New rules will be added at the end of the list and remain disabled (status light shows red) until they are explicitly enabled by clicking on the status light.

Active rules are processed in the order of the numbers (next to the status light) until the first matching rule. Then the following rules will be ignored! The sequence of the rules is thus very important. Therefore never place a rule such as Any – Any – Any – Allow at the beginning of the rules since all traffic will be allowed through and the following rules ignored!

More detailed information on the definition of Packet Filter Rules and detailed explanations of the individual settings can be found in the Astaro Security Gateway V8 administration guide in chapter 7.

6. Define the masquerading rule (optional):

Masquerading is used to mask the IP addresses of one network (in this example: gforeman) with the IP address of a second network (e.g. External). Thus remote users, who have only private IP addresses can surf on the Internet with an official IP address.

More detailed information on the definition of Masquerading Rules and detailed explanations of the individual settings can be found in the Astaro Security Gateway V8 administration guide in chapter 7.

Open the Network Security >> NAT >> Masquerading tab.

Make the following settings:

Network: Select the network of the remote endpoint (in this example: gforeman).
**Interface**: Select the interface that shall be used to mask the clients. (in this example: *External*).

Then confirm your settings by clicking on **Save**.

New masquerading rules will be added at the end of the list and remain disabled (status light shows red) until they are explicitly enabled by clicking on the status light.

7. **Activate the proxies (optional)**:

   If the remote employees shall access URL services via the remote access you may configure the required proxies on the Astaro Security Gateway – this would be the **DNS** and **HTTP proxy** for example.

   More detailed information on the configuration of **Proxies** and detailed explanations of the individual settings can be found in the **Astaro Security Gateway V8** administration guide.

After configuring the VPN server (Headquarters) you must configure the road warrior. Depending on the security policy of your organization and the requirements of your network you might have to make additional settings.
2.2. Configuration of the Remote Client

2.2.1. Astaro User Portal: Getting Preshared Keys

The **Astaro User Portal** is available for the remote access user. You can use this portal to download guides and tools for the configuration of your client. Especially for the L2TP remote access with authentication based on **Preshared Keys**, the user portal offers a configuration guide and the shared secret. For authentication with **X.509 certificate**, the user portal offers the necessary certificate. You can retrieve the following log-in data for the **Astaro User Portal** from the administrator: IP address, user name and password. Additionally, to download the certificate (PKCS#12 file) you need also the assigned password.

**Opening the Astaro User Portal:**

1. **Start your Browser and open the Astaro User Portal:**
   
   Start your browser and enter the management address of the Astaro User Portal as follows: **https://IP address** (example: https://218.93.117.220).
   
   A **security notice** will appear.
   
   Accept the **security notice** by clicking **OK** (Mozilla Firefox) or **Yes** (Internet Explorer).

2. **Log in to the Astaro User Portal:**
   
   **Username**: Your username, which you received from the administrator.
   
   **Password**: Your password, which you received from the administrator.

   Please note that passwords are case-sensitive!

   Click **Login**.

   Close the **Astaro User Portal** session by clicking on **Logout**.
The rest of the configuration takes place on the remote user client. This will require the IP address or hostname of the server. These should be supplied by the system administrator.

2.2.2. Remote Client: Windows XP/Vista/7 with Preshared Key

This chapter describes the configuration of Microsoft Windows XP and higher for using a Preshared Key as IPSec authentication.

Configuring a client using Microsoft Windows XP and higher:

1. Click **Start**, and then click **Control Panel**.
2. In Control Panel, double-click **Network Connections**.
3. Click **Create a new connection**.
   The **Network Connection Wizard** will open.
   Then click **Next**.
4. Click **Connect to network at my workplace**.
   Then click **Next**.
5. Define the dial-up Internet connection:
   If you have a permanent connection to the Internet, select the **Do not dial the initial connection** option. Otherwise, click **Automatically dial this initial connection**, and then select your dial-up Internet connection from the list.
   Then click **Next**.
6. Enter the name of the company or a descriptive name for the L2TP connection.
   Then click **Next**.
7. Enter the host name or the IP address of the gateway that you want to connect to.
   Then click **Next**.
8. Select whether the connection should be available to all local users, or just this account.
   Click **Anyone’s use** if you want the connection to be available to anyone who logs on the client. Otherwise, click **My use only**, to make available only when you log on to the client.
   Then click **Next**.
9. If you want to create a shortcut on the desktop, click **Add a shortcut to this connection to my desktop**.
   Then click **Finish**.
   The login window will appear.
10. Enter the **Username** and **Password** (**Remote User Account**).
11. In the login window, click on **Properties**.
12. Open the **Security** tab.
13. Disable the **Require data encryption (disconnect if none)** option.

14. Click on **IPSec Settings**.

15. Click **Use pre-shared Key for authentication** and enter the **Preshared Key**.
   Then click **OK**.

16. Open the **Networking** tab.

17. In the **VPN Type** section select **Layer-2 Tunneling Protocol (L2TP)**.

18. To close the properties dialog box click on **OK**.

**Using the L2TP connection:**

1. Use one of the following methods:
   - Click **Start**, point to **Connect To**, and then click the appropriate connection.
   - If you added a connection shortcut to the desktop, double-click the shortcut on the desktop.

2. If you are not currently connected to the Internet, MS Windows offers to connect to the Internet.
   After your computer connects to the Internet, the VPN server prompts you for your user name and password. Type your user name and password, and then click **Connect**. Your network resources should be available to you in just like they are when you connect directly to the network.

3. To disconnect from the VPN, right-click the icon for the connection, and then click **Disconnect**.

Further information is usually available from the network administrator.
2.2.3. Remote Client: Windows 2000/XP/Vista/7 with X.509 Certificates

This chapter describes the configuration of Microsoft Windows 2000/XP/Vista/7 for using X.509 certificates as IPSec authentication. The configuration is generated in two steps:

**Step 1 – Importing the certificate into Microsoft Windows 2000/XP/Vista/7:**

1. Click **Start**, and then click **Run**.
2. Enter **mmc**.
   The management console opens.
3. From the menu, select **Console >> Add/Remote Snap-in**.
4. Select **Certificates**, then click **Add**.
5. Select **Computer account** and click **Next**.
6. Select **Local Computer (the computer this console is running on)**, then click on **Finish**.
7. Click on **Close**.
8. Click on **OK**.
9. In the tree view on the left side, right-click on **Personal** in the category **Certificates (Local Computer)**.
10. From the menu select **All Tasks >> Import**.
    This opens the **Certificate Import** wizard.
11. Click on **Next**.
12. Select **Browse** and select the **PKCS#12 container file** to import.
13. Click on **Next**.
14. Enter the **PKCS#12 password**.
15. Click on **Next**.
16. Select **Automatically select the certificate store based on the type of certificate**.
17. Click on **Next**.
18. Click on **Finish**.
19. Select **Action >> Refresh**.
    Now, the newly imported certificate should be visible.
20. Close the management console.
    You don’t need to save it.
21. Move the CA certificate to the root CA folder, if necessary.
Step 2 – Configuring the L2TP connection:

1. Click **Start**, and then click **Control Panel**.
2. In Control Panel, double-click **Network Connections**.
3. Click **Create a new connection**.
   The **Network Connection Wizard** will open. Then click **Next**.
4. Click **Connect to network at my workplace**. Then click **Next**.
5. Define the dial-up Internet connection:
   - If you have a permanent connection to the Internet, select the **Do not dial the initial connection** option. Otherwise, click **Automatically dial this initial connection**, and then select your dial-up Internet connection from the list. Then click **Next**.
6. Enter the name of the company or a descriptive name for the L2TP connection. Then click **Next**.
7. Enter the host name or the IP address of the gateway that you want to connect to. Then click **Next**.
8. Select whether the connection should be available to all local users, or just this account.
   - Click **Anyone’s use** if you want the connection to be available to anyone who logs on the client. Otherwise, click **My use only**, to make available only when you log on to the client. Then click **Next**.
9. If you want to create a shortcut on the desktop, click **Add a shortcut to this connection to my desktop**. Then click **Finish**.
10. If you are prompted to connect, click **No**.
11. In the login window, click on **Properties**.
12. Open the **Security** tab.
13. Disable the **Require data encryption (disconnect if none)** option.
14. Open the **Networking** tab.
15. In the **VPN Type** section select **Layer-2 Tunneling Protocol (L2TP)**.
16. To close the properties dialog box click on **OK**.

Using the L2TP connection:
Click on **Connect**.

Further information is usually available from the network administrator.
2.2.4. Remote Client: Windows 2000 with Preshared Keys

This chapter describes the configuration of Microsoft Windows 2000 for using Preshared Keys (PSK) as IPSec authentication. Since MS Windows 2000 (in contrast to MS Windows XP) does not offer the selection of a PSK in the network connection wizard, the PSK and the IPSec connection need to be configured manually. The configuration is generated in four steps:

Step 1 – Enabling the usage of local IPSec policies in Microsoft Windows 2000:
1. Click **Start**, and then click **Run**.
2. Traverse to: `key_local_machine\system\CurrentControlSet\Services\RasMan\Parameters`.
3. Add a new registry entry in this section by selecting **Edit >> New >> DWORD Value** and enter **ProhibitIpSec**.
4. Double click on the new item and change its value data to **1**
5. Exit regedit
6. Reboot your computer for the changes to take effect.

Step 2 – Configuring the L2TP policy:
1. Click **Start**, and then click **Run**.
2. Enter `mmc`.
   The management console opens.
3. From the menu, select **Console >> Add/Remote Snap-in**.
4. Click on **Add**.
5. Select **IP Security Policy Management** from the list.
6. Click on **Add**, then on **Finish**, afterwards on **Close**, then on **OK**.
8. Select **Create IP Security Policy**.
    The IPSec Policy Wizard shows up.
9. Click on **Next**.
10. Enter a name for your new policy, e.g. **L2TP road warrior**.
11. Click on **Next**.
12. Disable the option **Activate the default response rule**.
13. Click on **Next**.
14. Make sure that **Edit properties** is selected and click on **Finish**.
15. In the dialog box, click on **Add**.
    The Security Rule Wizard shows up.
16. Click on **Next**.
17. Select **This rule does not specify a tunnel** and click on **Next**.
18. Select **All network connections** and click on **Next**.
19. Select **Use this string to protect the key exchange (preshared key)**.
20. Enter the IPSec PSK in the corresponding field and click on **Next**.
21. In the **IP Filter List** dialog box, click on **Add**.
22. Enter the name of your filter list (e.g. *L2TP filter list*) and click on **Add**.
   The IP Filter Wizard show up.
23. Click on **Next**.
24. As **Source address**, select **My IP Address** and click on **Next**.
25. As **Destination address**, select A specific IP Address and enter the IP address of your L2TP/IPSec gateway.
26. Click on **Next**.
27. Select **UDP** as protocol type and click on **Next**.
28. Select **From this port** and enter **1701** in the corresponding field.
29. Select **To this port** and enter **1701** in the corresponding field.
30. Afterwards click on **Next**.
31. Make sure that the **Edit properties** option is disabled and click **Finish**.
32. To close the **IP Filter List** dialog box, click on **Close**.
33. In the Security Rule Wizard, select your newly created filter list and click on **Next**.
34. Select the **Require Security** option and click on **Edit**.
35. Disable the **Accept unsecured communication, but always respond using IPSec** option and click on **OK** to close the dialog box.
36. Click on **Next**.
37. Make sure that the **Edit properties** option is deactivated, and click **Finish**.
38. To close the dialog box, click on **Close**.
   Your new policy should show up on the right side of the mmc window.
39. Right-click on the policy and select **Assign** to activate it.
40. Close the mmc.

**Step 3 – Configuring the L2TP policy:**
1. Click **Start**, and then click **Run**.
2. Enter **services.msc**.
3. Restart **IPSec Policy Agent**.
Step 4 – Configuring the L2TP connection:

1. Click Start, and then click Control Panel.
2. In Control Panel, double-click Network Connections.
3. Click Create a new connection.
   The Network Connection Wizard will open.
   Then click Next.
4. Click Connect to a private network through the Internet.
   Then click Next.
5. Define the dial-up Internet connection:
   If you have a permanent connection to the Internet, select the Do not dial the initial connection option. Otherwise, click Automatically dial this initial connection, and then select your dial-up Internet connection from the list.
   Then click Next.
6. Enter the host name or the IP address of the gateway that you want to connect to.
   Then click Next.
7. Select whether the connection should be available to all local users, or just this account.
   Click Anyone’s use if you want the connection to be available to anyone who logs on the client. Otherwise, click My use only, to make available only when you log on to the client.
   Then click Next.
8. Enter the name of the company or a descriptive name for the L2TP connection.
   Then click Finish.
9. If you are prompted to connect, click No.
10. In the login window, click on Properties.
11. Open the Security tab.
12. Disable the Require data encryption (disconnect if none) option.
13. Open the Networking tab.
15. To close the properties dialog box click on OK.
16. In the Preshared Key dialog box, enter your username and password.

Using the L2TP connection:

Click on Connect.

Further information is usually available from the network administrator.