SOPHOS

simple + secure

Astaro Security Gateway V7

Remote Access via L2TP over IPSec

Configuring ASG and Client

1. Introduction

The guides contain 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.com

... 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 client to 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. On Microsoft Windows systems, L2TP over IPSec is easy to set-up, and requires no special client software.

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:

http://www.microsoft.com/technet/prodtechnol/windows2000serv/support/vpnclientag.mspx

2.1. Configuration of the Remote Client

2.1.1. 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:

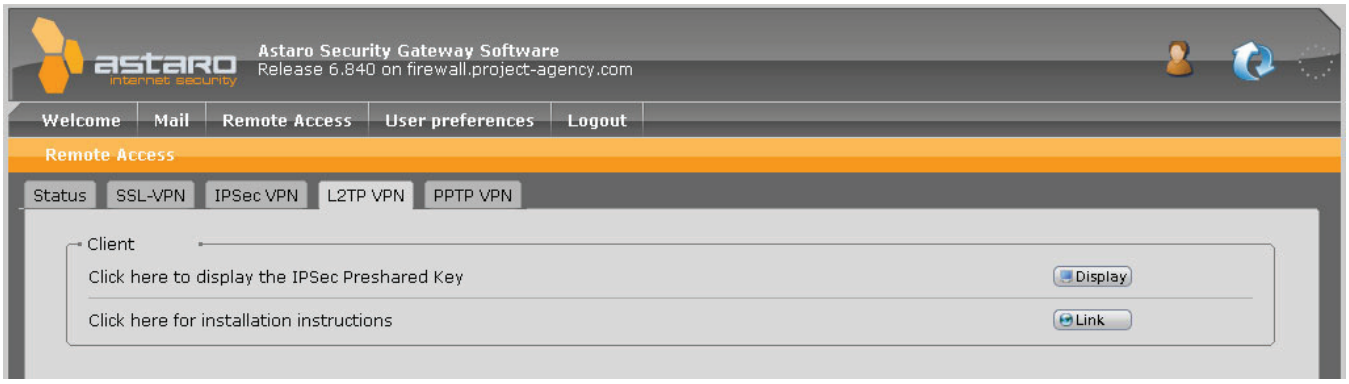
1. Start your Browser and open the Astaro User Portal:

Start your browser and enter the management address of the Astaro User Portal as follows: **https://IP address** (example: https://192.168.2.100).
A **security notice** will appear.
Accept the security notice by clicking **OK** (Mozilla Firefox) or **Yes** (Internet Explorer).

2. Log in to the Astaro UserPortal:

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.

2.1.2. Remote Client: Windows XP with Preshared Key

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

Configuring a client using Microsoft Windows XP:

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.

2.1.3. Remote Client: Windows 2000/XP with X.509 Certificates

This chapter describes the configuration of Microsoft Windows 2000/XP 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:

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.
    Click on **Next**.
11. Select Browse and select the **PKCS#12 container file** to import.
    Click on **Next**.
12. Enter the **PKCS#12 password.**
    Click on **Next.**
13. Select **Automatically select the certificate store based on the type of certificate**.
    Click on **Next**.
14. Click on **Finish**.
15. Select **Action >> Refresh**.
    Now, the newly imported certificate should be visible.
16. Close the management console.
    You don't need to save it.
17. 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**.
10. Then click **Finish**.
11. If you are prompted to connect, click **No**.
12. In the login window, click on **Properties.**
13. Open the **Security** tab.
14. Disable the **Require data encryption (disconnect if none)** option.
15. Open the **Networking** tab.
16. In the **VPN Typ** section select **Layer-2 Tunneling Protocol (L2TP)**.
17. 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.

2.1.4. 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\systemßCurrentControlSet\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.**
7. Right click on **IP Security Policies on Local Machine** in the tree view.
8. Select **Create IP Security Policy**.
   The IPSec Policy Wizard shows up.
   Click on **Next.**
9. Enter a name for your new policy, e.g. L2TP road warrior.
   Click on **Next**.
10. Disable the option **Activate the default response rule**.
    Click on **Next.**
11. Make sure that **Edit properties** is selected and click on **Finish.**
12. In the dialog box, click on **Add.**
    The Security Rule Wizard shows up.
    Click on **Next.**
13. Select **This rule does not specify a tunnel** and click on **Next.**
14. Select **All network connections** and click on **Next.**
15. Select **Use this string to protect the key exchange (preshared key).**
16. Enter the IPSec PSK in the corresponding field and click on **Next.**
17. In the **IP Filter List** dialog box, click on **Add.**
18. Enter the name of your filter list (e.g. *L2TP filter list*) and click on **Add**.
    The IP Filter Wizard show up.
    Click on **Next**.
19. As *Source address*, select **My IP Address** and click on **Next**.
20. As *Destination address*, select A specific IP Address and enter the IP address of your L2TP/ IPSec gateway.
    Click on **Next.**
21. Select **UDP** as protocol type and click on **Next**.
22. Select **From this port** and enter **1701** in the corresponding field.
23. Select **To this port** and enter **1701** in the corresponding field.
    Afterwards click on **Next.**
24. Make sure that the **Edit properties** option is disabled and click **Finish.**
25. To close the **IP Filter List** dialog box, click on **Close.**
26. In the Security Rule Wizard, select your newly created filter list and click on **Next**.
27. Select the **Require Security** option and click on **Edit.**
28. Disable the **Accept unsecured communication, but always respond using IPSec** option and click on **OK** to close the dialog box.
    Click on **Next.**
29. Make sure that the **Edit properties** option is deactivated, and click **Finish.**
30. To close the dialog box, click on **Close**.
    Your new policy should show up on the right side of the mmc window.
31. Right-click on the policy and select **Assign** to activate it.
32. 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.
9. 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 Typ** section select **Layer-2 Tunneling Protocol (L2TP)**.
16. To close the properties dialog box click on **OK**.
17. 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.

United Kingdom Sales:
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales:
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia & New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Boston, USA | Oxford, UK

SOPHOS