

Astaro Security Gateway V8

Remote Access via PPTP

Configuring ASG and Client



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 PPTP

This guide describes step by step the configuration of a remote access to the Astaro Security Gateway by using the **Point-to-Point Tunneling Protocol (PPTP)**. PPTP allows single Internet-based hosts to access internal network services through an encrypted tunnel. The structure is described in the following chart. PPTP is easy to set-up, and requires on Microsoft Windows systems no special client software.

The **Astaro User Portal** offers the current configuration guide. You should get the log-in data for the user portal from your system administrator.

PPTP is included with versions of Microsoft Windows starting with Windows 95. In order to use PPTP with Astaro Security Gateway, the client computer must support the MS-CHAPv2 authentication protocol. Windows 95 and 98 users must apply an update to their systems in order to support this protocol. The update is available from Microsoft at:

<http://support.microsoft.com/kb/191540/EN-US/>

2.1. Configuration of the Astaro Security Gateway

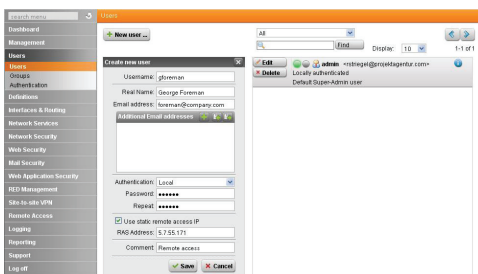
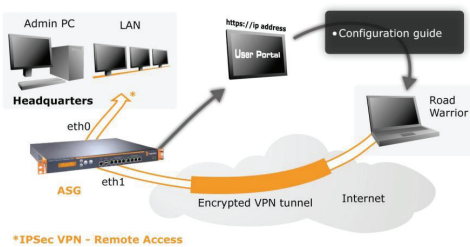
The Astaro Security Gateway is configured via the web based **WebAdmin** configuration tool from the administration PC. Opening and using this configuration tool is extensively described in the **Astaro Security Gateway V8** administration guide.

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 PPTP 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 5.



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.

Authentication: For the Remote Access via PPTP 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.

Password: Enter the password for the user. In doing so remember that also the Remote User will need this password later to log in to the Astaro UserPortal.

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.

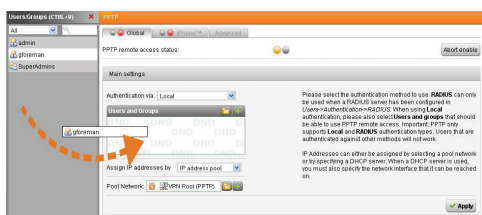
Save your settings by clicking on **Save**.

2. Configure the PPTP remote access:

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

On the **Global** tab enable the PPTP 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 PPTP Remote Access and detailed explanations of the individual settings can be found in the Astaro Security Gateway V8 administration guide in chapter 13.

I Main settings

Authentication via: Select the authentication method.

PPTP remote access supports **Local** and **RADIUS** authentication. Users that are authenticated against other methods will not work. You can use RADIUS authentication, if you have defined a RADIUS server on the *Users >> Authentication >> RADIUS* tab. The RADIUS server must support MS-CHAPv2 challenge-response authentication. The server can pass back parameters such as the client's IP address and DNS/WINS server addresses. The PPTP module sends the following string as NAS-ID to the RADIUS server: pptp. Note that when RADIUS authentication is selected, local users cannot be authenticated with PPTP anymore.

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 5.

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

Assign IP addresses by: The IP addresses can either be assigned from a predefined **IP address pool** 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.

Pool network: The default settings assign addresses from the private IP space 10.242.1.x/24. This network is called the *VPN Pool (PPTP)*. If you wish to use a different network, simply change the definition of the *VPN Pool (PPTP)* on the *Definitions >> Networks* page. Alternatively, you can create another IP address pool by clicking the plus icon.

Note:

If you wish the PPTP-connected users to be allowed to access the Internet, you additionally need to define appropriate **Masquerading** or **NAT** rules.

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.

... 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.

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

3. Configure the advanced PPTP remote access settings:

Open the **Remote Access >> PPTP >> Advanced** tab.



| Encryption strength

In the drop-down menu, select the encryption strength. The available options are **weak (40 bit)** and **strong (128 bit)**.

Security Note:

You should always set **Encryption** to **Strong** (128-bit) except when your network includes endpoints, which cannot support this. Both sides of the connection must use the same encryption strength.

Save the setting by clicking on **Apply**.

| Debug mode

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

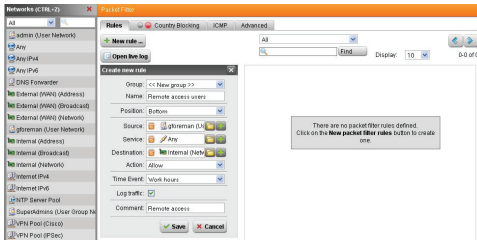
Save your setting by clicking on **Apply**.



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).

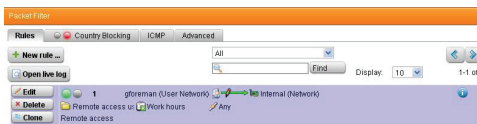
Service: Set the service.

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 Configuration Guide

The **Astaro UserPortal** 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 PPTP remote access, the user portal offers a configuration guide. You can retrieve the following log-in data for the Astaro User Portal from the administrator: IP address, user name and password.

Opening the Astaro User Portal (optional, not necessary for PPTP connection):

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 User Portal:

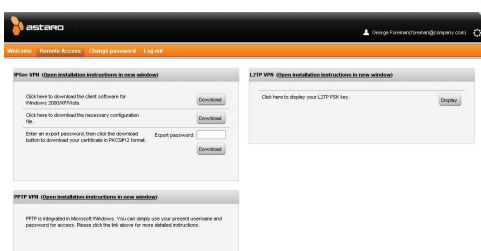
Username: Your username, which you received from the administrator.

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, as well as a valid username and password. These should be supplied by the system administrator.

2.2.2 Remote Client: Configuring Windows 2000/XP/Vista/7

This chapter describes the configuration of Microsoft Windows for using Username/Password as IPSec authentication.

Configuring a VPN connection from a client using Microsoft Windows:

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 PPTP 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**.

General: This allows you to change the hostname or destination address of the connection. In the **Connect First** window, select any network connections that need to be established before setting up the PPTP session.

Options: The dial and redial options can be defined here.

Security: Choose the **Advanced (Custom Settings)** option.

Next click the **Settings** button. Leave these settings as they are.

Network: In the **VPN Type** dialog box, leave the setting **Automatically**.

Sharing: This menu allows you to share the PPTP connection with other computers on the local network.

Using the PPTP 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.

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