Astaro Security Gateway V8

Software version: 8.000 or higher

Remote Access via SSL

Configuring ASG and Client

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

Contents

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Introduction ........................................................................ 2</td>
</tr>
<tr>
<td>2.</td>
<td>Remote Access via SSL .................................................. 2</td>
</tr>
<tr>
<td>2.1.</td>
<td>Configuration of the Astaro Security Gateway ...................... 3</td>
</tr>
<tr>
<td>2.2.</td>
<td>Configuration of the Remote Client ................................. 10</td>
</tr>
<tr>
<td>2.2.1.</td>
<td>Astaro User Portal: Getting Software and Certificates .......... 10</td>
</tr>
<tr>
<td>2.2.2.</td>
<td>SSL VPN Client: Installing the Software ............................ 12</td>
</tr>
</tbody>
</table>

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 SSL

This guide describes step by step the configuration of a remote access to the Astaro Security Gateway by using the **Secure Sockets Layer (SSL)** protocol. The SSL remote access feature in Astaro Security Gateway provides security by a double authentication using X.509 certificates and username/password. Astaro's SSL VPN feature reuses the TCP port 443 to establish an encrypted tunnel to your company, allowing you to access internal resources.

The **Astaro User Portal** offers the **Astaro SSL VPN Client** software, the configuration files, the necessary keys and configuration guides.

You should get the log-in data for the user portal from your system administrator.
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 SSL 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. When you specify an e-mail address, an 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 Remote Access >> Certificate Management >> Certificates tab.

**Authentication**: 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**: With a Remote Access via SSL it is not possible to assign a static IP address to the user. Leave this option deactivated if the user uses only the remote access via SSL.

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

Save your settings by clicking on the Save button.

2. **Configure the SSL remote access**:

Open the Remote Access >> SSL >> Global page.

On the Global tab enable the SSL remote access by clicking Enable.

The status light shows amber and the page becomes editable.

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

Use the Remote access settings section to select the authorized users and assign the access conditions.

Users and groups: Select the users and user groups that should be able to use SSL remote access (in this example: gforeman).

Local networks: Select the local networks that should be reachable to SSL clients (in this example: Internal (Network)).

Note:
If you wish the SSL-connected users to be allowed to access the Internet, you need to select Any in the Local networks dialog box. Additionally, you need to define appropriate Masquerading or NAT rules.

Automatic packet filter rules: Once the SSL VPN tunnel is successfully established, the packet filter rules for the data traffic will automatically be added. After the completion of the connection, the packet filter rules will be removed.

3. Configure the SSL settings:

SSL

Server settings

- Interface Address: <Any>
- Protocol: TCP
- Port: 443
- Override hostname

Virtual IP pool

- Pool network: <VPN Pool (SSL)>

Duplicate CN

- Allow multiple concurrent connections per user

Select the network protocol, address, and port that all SSL VPN clients must use. By default, this is set to TCP port 443 on any address. Note that port 16443 and the port used by WebAdmin cannot be used.

For all SSL VPN connections, the override hostname setting overrides the built-in choice of preferring a configured DNS host name over the system host name.

Virtual IP addresses for peers are selected from this IP pool. It may be changed or replaced to resolve conflicts. For SSL site-to-site connections it is possible to assign a peer a static virtual IP address, which suppresses use of this pool.

When enabled, duplicate common names are allowed in different SSL VPN sessions. This allows users to open multiple concurrent SSL VPN sessions from different hosts. Otherwise, only one SSL VPN session is allowed per user.
Open the **Remote Access >> SSL >> Settings** tab.

<table>
<thead>
<tr>
<th><strong>Server settings</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Interface address:</strong></td>
</tr>
<tr>
<td><strong>Protocol</strong>: Select the network protocol that all SSL VPN clients must use. By default, this is set to <strong>TCP</strong>.</td>
</tr>
<tr>
<td><strong>Port</strong>: Select the port that all SSL VPN clients must use. By default, this is set to <strong>443</strong>.</td>
</tr>
<tr>
<td><strong>Override hostname</strong>:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Virtual IP pool</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Pool network</strong>: The default settings assign addresses from the private IP space 10.242.2.x/24. This network is called the <strong>VPN Pool (SSL)</strong>. If you wish to use a different network, simply change the definition of the <strong>VPN Pool (SSL)</strong> on the <strong>Definitions &gt;&gt; Networks</strong> page.</td>
</tr>
<tr>
<td><strong>Local certificate</strong>: In order to authenticate for VPN clients, the SSL server needs a local certificate (in this example: <strong>Local X.509 Cert</strong> – this certificate is automatically preset).</td>
</tr>
</tbody>
</table>

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

The status light shows green and the remote access is activated.

4. **Configure the advanced SSL remote access settings:**

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

<table>
<thead>
<tr>
<th><strong>Cryptographic settings</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Encryption algorithm</strong>: Supported algorithms are (all in Cipher Block Chaining (CBC) mode): <strong>DES-EDE3 168bit (3DES)</strong>, <strong>AES (Rijndael) 128bit/192bit/256bit</strong> and <strong>Blowfish (BF)</strong>.</td>
</tr>
<tr>
<td><strong>Authentication algorithm</strong>: Supported algorithms are <strong>MD5 128bit</strong> and <strong>SHA1 160bit</strong>.</td>
</tr>
<tr>
<td><strong>Key size</strong>: The key size (key length) is the length of the Diffie-Hellman key exchange. The longer this key is, the more secure the symmetric keys are. The length is specified in bits. You can choose between a key size of 1024 or 2048 bits.</td>
</tr>
<tr>
<td><strong>Server certificate</strong>:</td>
</tr>
<tr>
<td><strong>Key Lifetime</strong>:</td>
</tr>
</tbody>
</table>

Save your setting by clicking on the **Apply** button.
<table>
<thead>
<tr>
<th>Network settings</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Use data compression</strong>: All data sent through the SSL VPN tunnel will be compressed prior to encryption.</td>
</tr>
<tr>
<td>Save your setting by clicking on <strong>Apply</strong>.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Debug settings</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enable Debug mode</strong>: This option controls how much debug output is generated in the log file. Select this option if you encounter connection problems and need detailed information about the negotiation of client parameters.</td>
</tr>
<tr>
<td>Save your setting by clicking on the <strong>Apply</strong> button.</td>
</tr>
</tbody>
</table>

5. **Configure the advanced remote access settings**: 
Open the **Remote Access >> Advanced** page.

![Advanced settings](image)

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.

6. **Define the packet filter rule (optional)**: 
You must define this packet filter rule if you have disabled the **Automatic packet filter rule** function during the configuration of the SSL remote access in step 2. 
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.

---

7. **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 (in this example: `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.

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.

---

8. **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 Software and Certificates

The **Astaro User Portal** is available for the remote access users. You can use this portal to download guides and tools for the configuration of your client. Especially for the SSL remote access, the user portal offers a configuration guide and a customized SSL VPN client software, which already includes software, certificates and configuration handled by a simple installation procedure. This client supports most business applications such as native Outlook, native Windows Filesharing and many more. You should get the following log-in data for the **Astaro User Portal** from your system administrator: IP address, user name and password.

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**.

3. **Load the tools for the SSL Remote Access to your client:**

   The **SSL VPN** tab will contain the software and keys for your client; to do so have two options. Either you download a complete software package with the pertinent key for a new installation or you update an already installed SSL VPN client with new keys. The SSL VPN Client is available for Microsoft Windows 2000/XP/Vista and 7.

   Start the download process by clicking on **Download**.
For the configuration of SSL VPN on Linux, MacOS X, BSD and Solaris please see installation instructions on http://openvpn.net (all necessary files are available over the Astaro User Portal.

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 security system administrator.
2.2.2. SSL VPN Client: Installing the Software

The first part of the installation uses the Installation Menu to configure basic settings. The setup program will check the hardware of the system, and then install the necessary software on your PC.

Unpack the installation package (for example by using WinZip), if you have received it as a .ZIP file. Open a file browser and go to the appropriate directory. Launch the file `setup.exe` from this directory.

You should see the installation wizard now.

Click on **Next** to proceed.

You will see the software license.

If you agree to the terms of the license, click on **I Agree**.

Choose the install location.

Click on **Install** to proceed.
Then the installation process will be started.

The installation wizard will copy the necessary files on your system. A virtual network card will be installed during the installation process. Since the relevant driver is not certified by Microsoft, a corresponding caution message will appear during the installation process. You can ignore this message.

Click on **Continue Installation**.

When installation process is finished, you are asked to complete. Click on **Next** to do so.

When installation process is finished, you are asked to close the installation wizard. Click on **Finish** to do so.

After the software installation the client is automatically started. Then the **SSL VPN** icon (__) will be displayed in your Task bar. A double click on this icon opens the **User Authentication** dialogue box.
Log in with your **Username** and **Password**, which you use also for the **Astaro User Portal** and then start the connection by clicking **OK**. The connection status is indicated by the **SSL VPN** icon: Disconnected ( ), connecting ( ) and connected ( ).

The **Connection** dialogue box allows you to monitor the set-up of the connection. The SSL VPN Remote Access can be disconnected by clicking **Disconnect**.

Further information is usually available from the network administrator.

The basic settings for the remote access via SSL are now finished. Depending on the security policy of your organization and the requirements of your network you might have to make additional settings.