How to Configure TLS with SIP Proxy

https://campus.barracuda.com/doc/48203285/

This article provides steps to configure SIP with TLS encryption in an example scenario where the telephone is located in a different network from that of the PBX. The Barracuda NextGen Firewall F-Series performs NAT between both networks. The SIP Proxy in the Barracuda NextGen Firewall F-Series translates the network addresses in SIP messages to allow communication between the telephone and the PBX. The example scenario is illustrated in the following diagram:

For more security, configure all peers to verify the validity of the certificates and provide their own custom certificates. You can configure the peers not to verify the certificates, but this is a less secure setup. If you are testing TLS, it is recommended that you test the scenario with the highest security, because it is less fault-tolerant and more likely to produce problems in case of misconfiguration.

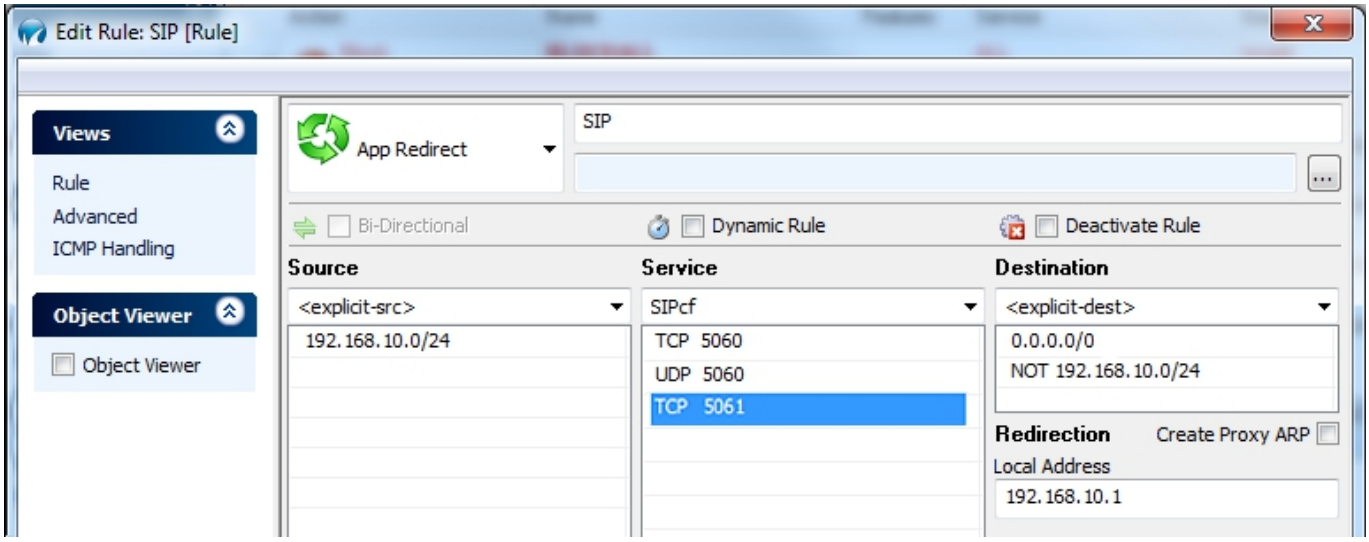
Before You Begin

- You must install OpenSSL to create a self-signed CA and the certificates. OpenSSL is already installed in most Linux distributions. In Windows, you must install it separately.
- This article provides steps for creating a self-signed root CA. If you disable the use of an external CA in the SIP Proxy, an internal root CA is generated automatically. You can use this root CA to sign the certificates for the client and the PBX instead of creating another one. The root CA environment is located in `/var/phion/preserve/sipsprx/server_service/opensips/rootCA/`.
- This article provides steps for use with PhonerLite and Asterisk, but you can use any softphone or PBX that supports TLS encryption. The configuration of Asterisk, except for the TLS settings, as well as the standard configuration of the SIP Proxy are out of the scope of this article. An already working setup with SIP over UDP or TCP is assumed.

Step 1. Create a Firewall Rule to Redirect the SIP/TLS Port to the SIP Proxy

Create an App Redirect firewall rule to redirect the SIP port to the SIP Proxy.

- If you have specified **SIPcf** as the **Service** , edit the SIPcf Service Object to add TCP port 5061.
- If you explicitly specified the ports in your redirect rule, add TCP port 5061 so that it is also redirected.



Step 2. Create Private Keys and Certificates

Create the private keys and certificates for the softphone, SIP Proxy, and PBX .

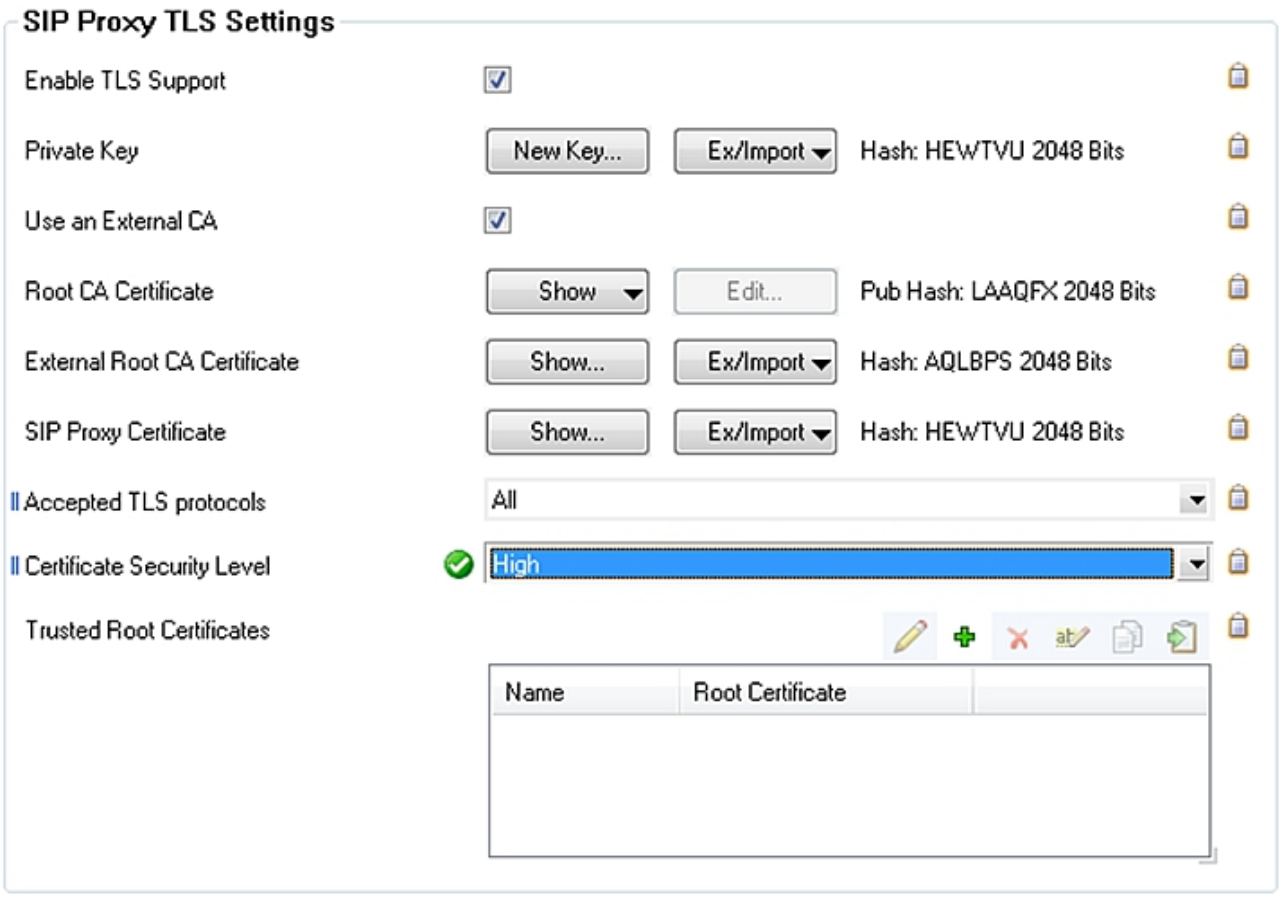
For more information on how to create self-signed X.509 certificates, see How to Create Certificates with XCA and How to Create Certificates for the SIP Proxy.

Asterisk: The certificate installed on the SIP Proxy must contain the IP address of the SIP Proxy in the **common name** field. Otherwise, Asterisk will refuse to authenticate.

Step 3. Configure the SIP Proxy to Support TLS

To configure the TLS settings for the SIP Proxy:

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > Firewall > Forwarding Settings**.
2. In the left menu, select **VoIP/SIP**.
3. Expand the **Configuration Mode** menu and click **Switch to Advanced**.
4. Click **Lock**.
5. In the **SIP Proxy TLS Settings** section, select the **Enable TLS Support** check box.



6. Next to **Private Key**, click **Ex/Import**, select **Import from File**, and then select the `sipproxy-private.pem` file that you generated.
7. Select the **Use an External CA** check box.
8. Next to **External Root CA Certificate**, click **Ex/Import** and select **Import from PEM File**.
9. Browse to the `rootCA` folder and select the `cacert.pem` file.
10. In **SIP Proxy Certificate**, import the `sipproxy-cert.pem` file in the `tls` folder.

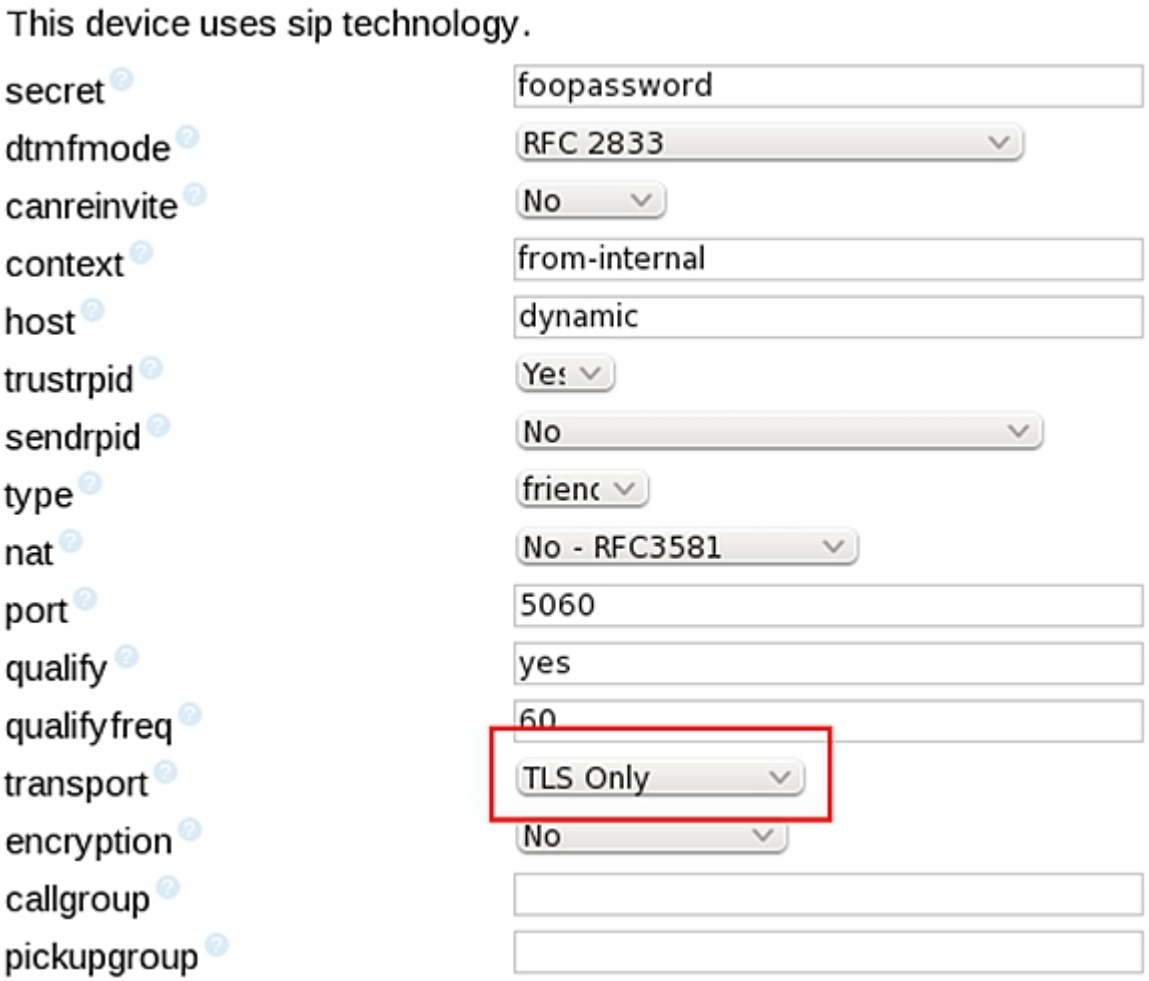
    It is recommended that you change the **Certificate Security Level** to **High**. This setting provides protection from man-in-the-middle attacks by requiring the SIP Proxy to check the validity of the certificates from the client and the server. If the certificates are invalid, they are rejected.
11. Click **Send Changes** and **Activate**.
12. To verify that the certificate file was accepted, view the log file of the SIP Proxy (*Server* \ *FirewallService* \sipproxy). The file should look similar to the following:
    ```
    INFO:core:check_for_krb: KRB5 cipher KRB5-DES-CBC3-MD5 found
    INFO:core:init_tls_domains: Processing TLS domain [0.0.0.0:0]
    WARNING:core:init_ssl_ctx_behavior: client verification NOT activated.
    Weaker security. INFO:core:init_tls_domains: Processing TLS domain
    [0.0.0.0:0] WARNING:core:init_ssl_ctx_behavior: server verification NOT
    activated. Weaker security. NOTICE:core:main: version: opensips 1.8.2-
    tls (x86_64/linux)
    ```

Step 4. Configure Asterisk to Support TLS

The following instructions are for Linux. In Windows, change the forward slash (/) path separators to backslashes (\).

To configure TLS settings for the Asterisk server:

1. Connect to the Asterisk server through SSH.
2. Change to the `/etc/asterisk` directory and create a subdirectory named `tls`.
3. Copy the following files into the `/etc/asterisk/tls` directory:
   - The `cacert.pem` file from your `rootCA` folder.
   - The `asterisk-keycert.pem` file from your `tls` folder.
4. Change the user and group of `/etc/asterisk/tls` and all of its contents to the same user Asterisk uses. Then change the permissions of both files to 0400.
   ```
   $ cd /etc/asterisk
   $ chown -R asterisk:asterisk tls/
   $ chmod 0400 /etc/asterisk/tls/*
   ```
5. If you are using FreePBX, open the `/etc/asterisk/sip_general_custom.conf` file with a text editor such as vi.
6. If you are not using FreePBX, open the `/etc/asterisk/sip.conf` file with a text editor such as vi and search for the `[general]` section.
7. Add the following lines:
   ```
   tlsenable=yes tlsbindaddr=0.0.0.0
   tlscertfile=/etc/asterisk/tls/asterisk-keycert.pem
   tlsdontverifyserver=no ;tlscipher=DES-CBC3-SHA tlsclientmethod=sslv23
   tlscafile=/etc/asterisk/tls/cacert.pem
   ```
   If you do not want Asterisk to verify the validity of the certificates, set `tlsdontverifyserver` to *yes* .
8. Change the transport protocol of your SIP peers to TLS:
   1. Open FreePBX and select **Applications > Extensions**.
   2. Edit each of your extensions.
      - If you only want to allow your SIP peers to use TLS (which is more secure but breaks the standard), set the **transport** parameter to **TLS Only**.
      - If you want to allow (but not force) TLS, set it to **All – TLS Primary**.



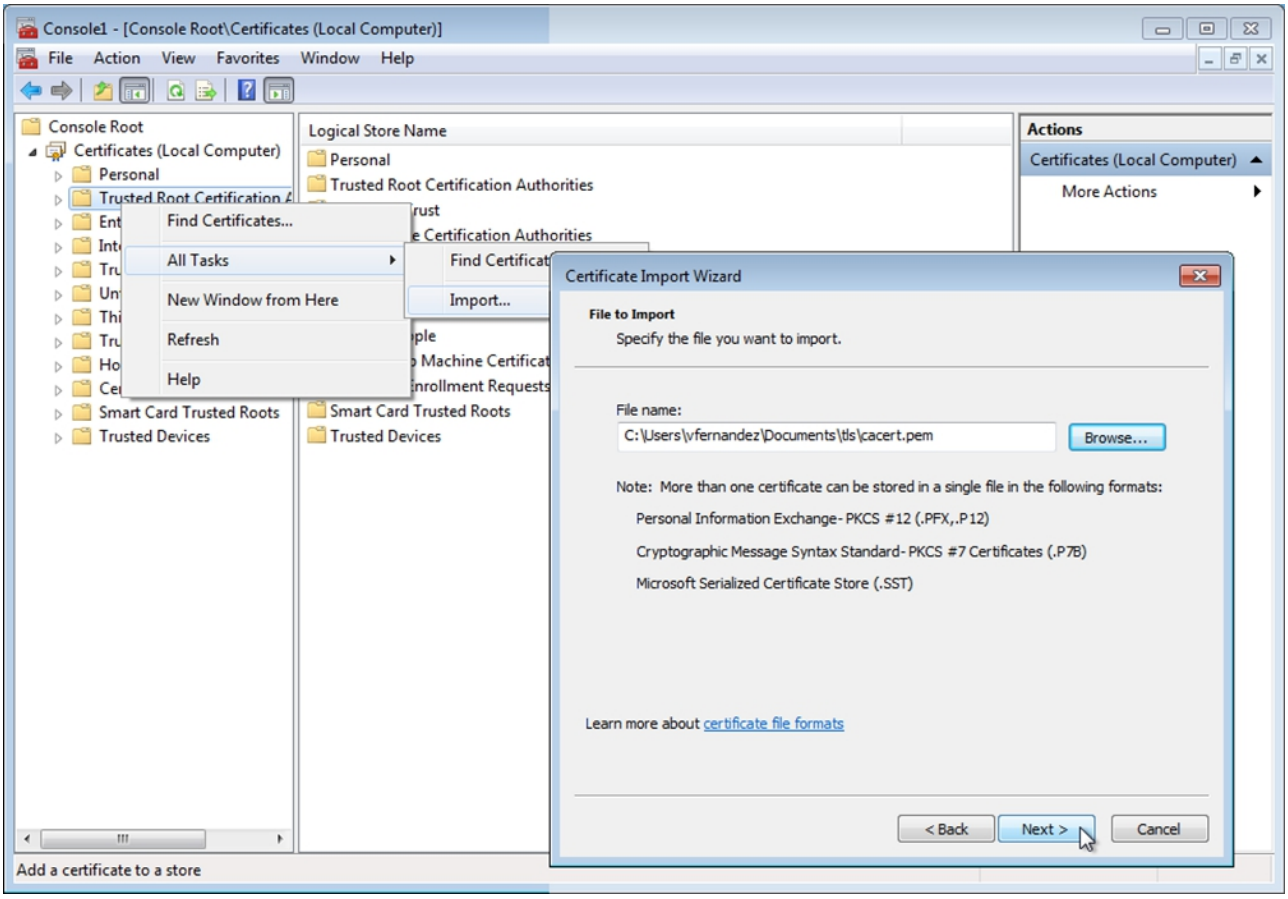
9. Apply the changes in FreePBX to reload the configuration.
10. To verify that the certificate was correctly configured:
    1. Connect to the Asterisk CLI.
       `$ asterisk -r`
    2. Reload the configuration.
       `$ sip reload`
       If the certificate was correctly configured, Asterisk displays the following message:
       `SSL certificate ok.`

Step 5. Import the Root CA into the Client (Windows)

You must import the root CA certificate that you have created in the previous configuration. Otherwise, the client will reject the certificate of the server. To import the root CA into the client:

1. In Windows, click the **Start** menu and type `mmc` in the search field.
2. When the **mmc** program appears, click it.
3. Go to **File > Add/Remove Snap-in**.

4. In the **Add/Remove Snap-in** window, click **Certificates** from the list of available snap-ins and then click **Add**.
5. In the **Certificates Snap-in** window, select **Computer account**, click **Next**, and then click **Finish**.
6. Click **OK**.
7. In the **Console** window, expand **Certificates (Local Computer)** in the left pane.
8. Right-click **Trusted Root Certification Authorities** and select **All Tasks > Import**.
9. In the **Certificate Import Wizard**, click **Next**, click **Browse**, and then select the `cacert.pem` file from the `rootCA` folder. If you do not see the `cacert.pem` file, change the file filter to `All Files (*.*)`.



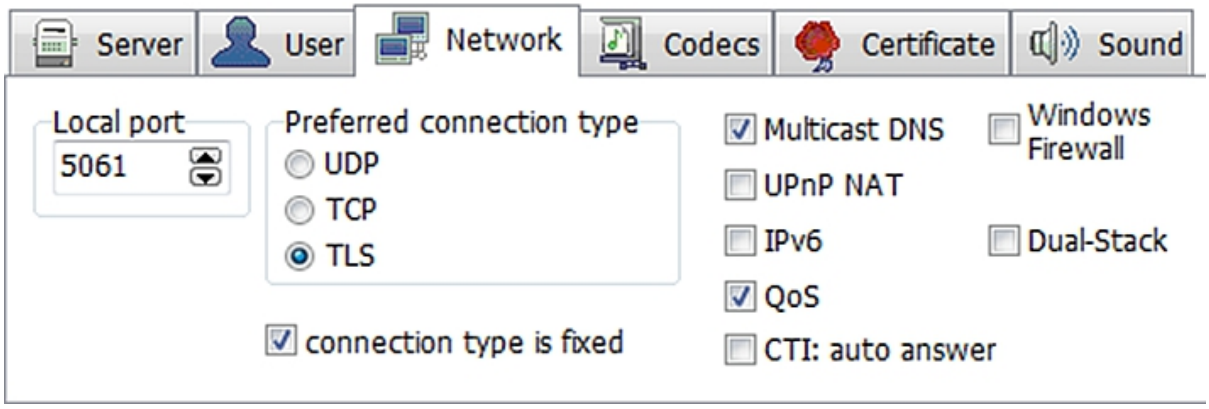
10. Click **Next** and then click **Finish**.

Step 6. Configure PhonerLite

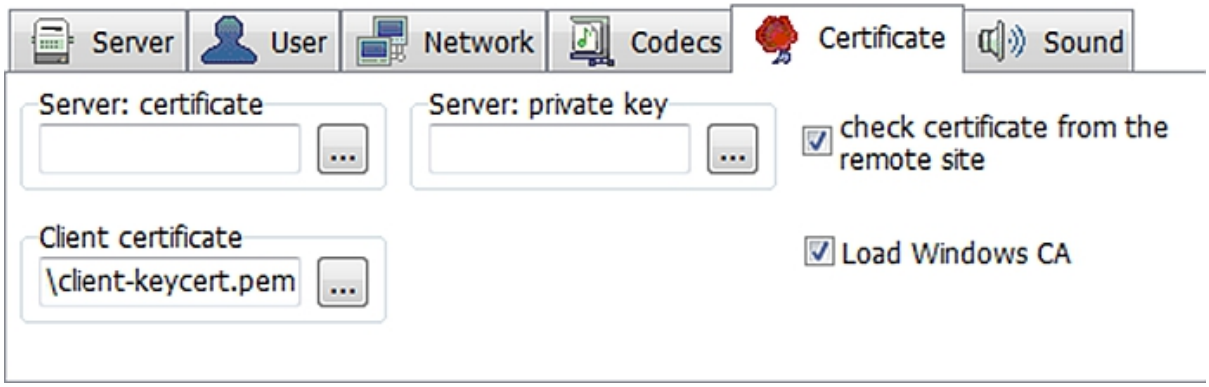
To configure PhonerLite:

1. Configure the SIP account you previously created in PhonerLite as usual.
2. Click the **Configuration** tab.
3. Click the **Network** tab and then specify the following settings:
   - **Local port**: **5061**

- **Preferred connection type**: **TLS**



4. Click the **Certificate** tab and then specify the following settings:
   - **Client certificate** – Click the ellipsis button (**...**). Then browse to and select the `client-keycert.pem` file that you previously created.
   - **check certificate from the remote site** – If you want PhonerLite to verify the validity of the certificates, select this check box.
   - **Load Windows CA** – Select this check box.



5. Click **Save**. PhonerLite should now be able to register successfully.

Troubleshooting

The most common issue that you might encounter is the client not being able to register into the PBX. As a workaround, you can remove the requirement for certificate verification but this does not solve the issue because your certificates might be misconfigured. Instead, it is strongly recommended you check the log file of the SIP Proxy to find the cause. The log file is located in `//sipproxy`. The following table describes commonly encountered issues and their solutions.

Issue and Symptom	Cause	Solution

Client Does Not Register The client does not register. The log displays one of the following error messages: • ERROR:core:tls_accept: some error in SSL (ret=0, err=5, errno=0/Success): • ERROR:core:tls_accept: New TLS connection from : failed to accept: rejected by client	The client does not accept the certificate of the server.	Ensure that you properly configured the certificates in the client and that you imported the root CA certificate.
Client Fails to Register The client fails to register and then quickly tries again. The log displays the following message: ERROR:core:tls_accept: New TLS connection to <**ip of the PBX**>:5061 failed	There can be several causes: • The PBX is not correctly configured. • The PBX is switched off or not running. • TLS support is not configured in the PBX. • A firewall is blocking the connection. • The PBX is rejecting the certificate of the SIP Proxy.	Try the following solutions: • Ensure that you have properly configured the PBX and enabled TLS support in it. The root CA certificate must be imported into the PBX. Verify that the `cacert.pem` file is located in `/etc/asterisk/tls`, and that the file is readable by Asterisk. • Verify that the PBX is up and running, and that you correctly configured TLS. • To verify that TLS support is enabled, run `netstat -an | grep 5061` in the PBX and verify that port 5061 is open. • If there is another firewall between the SIP Proxy and the PBX (for example, in the operating system of the PBX host), verify that the SIP ports are open. • Ensure that the root CA certificate is imported into the PBX. Verify that the `cacert.pem` file is located in `/etc/asterisk/tls`, and that the file is readable by Asterisk.

Client Works Properly but Error Messages are Still Displayed
The client can register and works properly, but the following error messages are displayed in the log:
`ERROR:core:tls_connect: SSL_ERROR_SYSCALL err=Success(0)`
`ERROR:core:tls_connect: New TLS connection to :5061 failed`
`ERROR:core:tls_connect: TLS error: 5 (ret=0) err=Success(0)`
`ERROR:core:tcp_send: failed to send`
	When a softphone is closed, it sends a request to unregister. However, some softphones do not wait for a response and quit immediately. The error messages indicate that the SIP Proxy is unable to contact the client because it has quit.	You do not need to worry about these error messages unless something stops working.

Asterisk Reports Client as UNREACHABLE Asterisk reports the client as UNREACHABLE, although it should be registered. The Asterisk log file (`/var/log/asterisk/full`) repeatedly displays the following message: `ERROR[xxxxx] tcptls.c: Certificate common name did not match ()`	Asterisk requires the **Common Name** field of the certificate for the SIP Proxy to match the host name of the SIP Proxy. Asterisk takes the IP address of the SIP Proxy that is seen as the hostname, but you have entered something else into that field. For this reason, Asterisk closes the connection with the SIP Proxy, causing the TCP send errors.	As of version 11.2.1, there is no way to disable this check. You must create the certificate for the SIP Proxy again. When asked to enter the Common Name, enter the IP address of the SIP Proxy that is displayed in the error message of Asterisk. After the certificate is generated, import it into the configuration of the SIP Proxy as usual.

Figures

1. fw_sip_proxy_tls.png
2. pbx_sip.png
3. pbx_sip_settings.png
4. pbx_asterisk.png
5. pbx_console.png
6. pbx_phonerlite.png
7. pbx_phonerlite_2.png