Stunnel configuration example using Telnet

The information in this page is updated in accordance with firmware version **07.02.7**.

□

Contents

Introduction

This article provides a guide on how to configure stunnel and use telnet protocol for devices to interact with each other securely. These configurations can be implemented on RUT, RUTX and TRB series devices.

- First you want to make sure that you have **ADVANCED mode** enabled. This will allow you to choose from a larger variety of settings.

Stunnel is an open-source proxy service that adds TLS encryption to clients and Servers already existing on a VPN network. TLS encryption provided by Stunnel can be used as an additional layer of encryption for data sent by OpenVPN. This procedure increases the security of the established connection and provides higher chances of passing a Deep packet inspection (DPI) check.

Telnet is an application protocol used on the internet or LAN to provide a bidirectional interactive text-oriented communication using virtual terminal connection like Putty. However, due to serious security concerns of using Telnet over an open network, SSH became favorable.

This article provides an extensive configuration example with details on how to create a tunnel connection using stunnel instances and then connect them using telnet protocol, with the data encrypted

Configuration Overview and Prerequisites

Before we begin, let's overview the configuration that we are attempting to achieve and the prerequisites that will make it possible. Prerequisites:

- One RUTxxx router of any type with public IP.
- Atleast one end device to configure the router
- Wireshark in your end device
- Stunnel application installation in your laptop: stunnel Download

As mentioned earlier, here, in this configuration since telnet does not provide security, we are going to develop a Stunnel in between the router and the client, and then connect them using telnet protocol, so that there is encryption provided to the data. For this we will use Wireshark to capture the packets and verify if the data has been encrypted or not.

Client and Server Configuration

First, configure the Stunnel server. The stunnel server will listen for incoming client connections on the specified port (2030 for this example) and connect them to telnet port at port 23. Configure stunnel client that will be connecting to the server.

Router Configuration

Firstly, enable local telnet access at port 23, Go to **System → Administration → Access Control**

Then, navigate to **Services → VPN → Stunnel**, and configure the router,

- Enable Stunnel global settings,

- Add new instance, give any new configuration name,

- You will be directed to stunnel configuration,

1. **Enable** Stunnel

2. Select Operating mode **(Server)**

3. Listen IP **(0.0.0.0)**

4. Select Listen Port **(2030)**

5. Connect IP'S **(127.0.0.1:23)**

6. TLS Cipher **(Secure)**

7. Insert Certificate File **(server.cert.pem and server.key.pem)**

Note: You can download the certificate file from **System → administration → Certificates**. Certificates

- Then, navigate to the menu **Network → Firewall → Traffic Rules** and add new instance or edit telnet instance.

You will be navigated to the configuration page, enable it and *save and apply* the rule.

Stunnel Configuration

For Windows:

Download Stunnel from stunnel download. Choose the latest win64 installer.exe and install.

- Install only **Stunnel.exe** deamon, you can skip **openssl.exe**.

Once the application is installed, open stunnel, go to configuration and select edit configuration. Remove all the content and paste as below:

```
; Example TLS client mode services
[my-stunnel-conf]
Client = yes
Accept = 127.0.0.1:23
Connect =84.15.X.X:2030
Cert = ca-cert1.pem
```

Connect IP depends on your configuration and write them accordingly. Here in this example, it is as above.

- Navigate to **C:\Program files (x86)\Stunnel\config** and create new file *ca-cert1.pem*.
- Copy and paste *client.cert.pem* and *client.key.pem* to it and save the file. (**Note:** Download the client certificate from your Web-UI, **System → Administration → certificate**)
- For example:

Once saved, go back to **stunnel → configuration**, and reload configuration.

If everything is working as expected, you should be able to see the log as above with successful configuration. Now you can try to telnet router.

For Linux:

Similarly, for Linux machines follow the below commands.

- Update and upgrade Ubuntu

Using these commands update your Ubuntu's package list and also upgrade the existing packages to the latest version:

apt-get update apt-get upgrade

- Install Stunnel

Install Stunnel package using the code below:

apt-get install stunnel4 -y

- Configure Stunnel

Stunnel configures itself using a file named **stunnel.conf** which by default is located in **/etc/stunnel**. Create a **stunnel.conf** file in the /etc/stunnel directory.

nano /etc/stunnel/stunnel.conf

Next, specify a service for use with stunnel. Here, it will work as client so file should look like this:

```
client = yes
[squid]
accept = 127.0.0.1:23
connect = 84.15.X.X:2030
cert = /etc/stunnel/stunnel.pem
```

- Create certificates

Stunnel uses SSL certificate to secure its connections, which you can easily create using the commands:

openssl genrsa -out key.pem 2048 openssl req -new -x509 -key key.pem -out cert.pem -days 1095

and then create file stunnel.pem

nano /etc/stunnel/stunnel.pem

copy the certificates to stunnel.pem file: cat key.pem cert.pem >> /etc/stunnel/stunnel.pem

- Restart stunnel

restart the stunnel configuration using the command:

/etc/init.d/stunnel4 restart

Testing Results

For Windows:

- Use Putty and telnet it to local host 127.0.0.1:23 as in the image below.

You will be directed to:

For Linux:

- After restart, type command:

telnet 127.0.0.1, and the results should look like this:

Wireshark Testing:

- Install Wireshark, and run. Using this packet capture, you will be able to make sure that the traffic is encrypted now.

External Links

- https://www.stunnel.org/downloads.html
- https://wiki.teltonika-networks.com/wikibase/index.php?title=RUT955_Administration&mobileaction=toggle_view_desktop#Certificates
- https://www.wireshark.org/download.html
- https://www.putty.org/