

# Securing PAD using SSH Tunneling



Model	Chameleon CTM Devices
Revision:	Rev 1.1

3066 Beta Avenue Burnaby, B.C. V5G 4K4  
Phone: 604.294.4465  
Fax: 604.294.4471  
[support@cypress.bc.ca](mailto:support@cypress.bc.ca)

## Revision Control

Description	Revision	Date
Customer Release	Rev 1.0	Mar. 4, 2011
Updated web page configuration section, added persistent SSH connections section	Rev 1.1	Oct. 13, 2011

## Contents

Revision Control .....	2
1 Overview .....	2
2 System Requirements .....	3
3 How SSH Tunneling Works.....	3
4 Configuration Steps.....	4
4.1 Device Configuration.....	4
4.1.1 Configuration via Commands.....	4
4.1.2 Configuration via Web Page.....	4
4.2 Windows PC Configuration .....	5
4.3 Linux PC Configuration.....	5
5 Persistent SSH Connections .....	6
6 Technical Support/Warranty.....	6

## I Overview

Chameleon CTM devices provide a high-speed data communications link for many different fixed and mobile applications over the public Internet. When sensitive data is being transmitted, one of two mechanisms may be used on the CTM device to secure its communication with a remote server:

1. Using a virtual private network (VPN) application on the modem (refer to the “VPN Application Note” for details)
2. Using SSH tunneling between the modem and a remote server running an SSH client

SSH tunneling (also referred to as SSH port forwarding) can be used in many different applications to secure public TCP/IP traffic through an encrypted SSH connection. This mechanism is easy to set up and can be used with existing software applications running on your remote server.

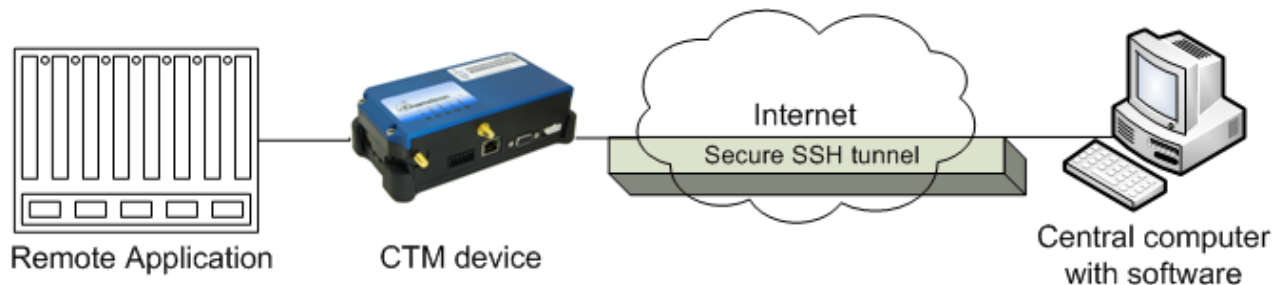
This application note describes how SSH tunneling can be used to secure packet assembly and disassembly (PAD) communications between a CTM device and a remote server.

## 2 System Requirements

To set up a SSH tunnel between a CTM device and your remote server, the following are required:

- CTM device with the following configuration:
  - Remote SSH access enabled
  - TCP PAD server mode configured
  - Remote access to PAD port disabled
- Wireless data device installed in CTM device with a routable IP address that can be accessed by the remote server
- SSH client (e.g. PuTTY, OpenSSH, SSH Tectia, etc.) installed on the remote server
- Third-party software to maintain persistent SSH tunnels (e.g. autossh, MyEnTunnel, etc.) installed on the remote server

## 3 How SSH Tunneling Works



A SSH tunnel between a remote server and CTM device is set up by configuring the following parameters for the SSH local port forwarding settings:

- **Source/Local Port** is an arbitrary, unused local TCP port that the SSH client will listen on
- **Destination/Remote Host** is the IP address of the destination host
- **Destination/Remote Port** is a TCP port on the destination host

The SSH tunnel is then established when the SSH client establishes the SSH connection with the SSH server using the specified local port forwarding settings.

In SSH local port forwarding, the SSH client listens on a source port on the remote server for data. When another application running on the remote server sends data to this specified source port, the SSH client forwards the data through the SSH connection to the specified destination host and port.

In this application note the following parameters are used for the SSH tunnel:

- **Source/Local Port** is a TCP port on the remote server
- **Destination/Remote Host** is the IP address of the CTM device

- **Destination/Remote Port** is a TCP port on the CTM device associated with an application (e.g. TCP port 5005 for TCP PAD, etc.)

A SSH tunnel can only be established with a destination TCP port. Therefore, SSH tunneling can only be used to secure TCP applications on the CTM device.

## 4 Configuration Steps

For this application note, steps are outlined for setting up a SSH tunnel when using the Chameleon TCP PAD application. There are two parts to the configuration: device configuration and PC configuration (Windows or Linux).

### 4.1 Device Configuration

This section provides the minimum device configuration settings that are required to secure TCP PAD communications using SSH tunneling.

#### 4.1.1 Configuration via Commands

```
cmd rmtssh 1
cmd telnettimeout 0
cmd port 9600 8 n 1 2 (optional)
cmd mode 4
cmd pad port 8888 (optional, default port is 5005)
cmd pad mode 1
cmd pad secure 1
cmd save
cmd pwrmode 2
```

#### 4.1.2 Configuration via Web Page

1. From the Network | Firewall web page, enable remote SSH access and disable the session timeout on the device:

**Remote SSH: Enabled**  
**Session Timeout: 0**

Click on **Save Changes**.

2. From the Config, Serial Port, and PAD web pages within Config, configure the connection mode, serial port settings, and PAD mode, respectively:

Config | Serial Port page:

Select proper serial port configuration settings for your serial port device

Click on **Save Changes**

Config | Main page:

Serial Port 1 Mode: 4: PAD host interface

Click on **Save Changes**

Config | PAD page:

Mode: 1: TCP PAD Mode

Click on **Save Changes**

3. Configure secure access to the TCP PAD port, that is, configure the TCP PAD port from not being directly accessible from the Internet via Telnet access to 192.168.1.1 and using the commands

```
cmd pad secure 1
```

```
cmd save
```

4. Using the Config | Reboot web page, power cycle the device.

## 4.2 Windows PC Configuration

The following steps are provided for PuTTY:

1. Set up a typical SSH connection to the device at its WAN IP address and TCP port 22
2. In the Configuration dialog, expand the PuTTY SSH control and select **Tunnels**
3. Under the **Add new forwarded port section** of the dialog:
  - a. Enter Source port: 5555
  - b. Enter Destination: <WAN IP address>:<TCP PAD port> (e.g. 123.456.789.100:5005)
  - c. Click on Add button
4. Save your configuration
5. Open the SSH connection to the device

After a successful SSH connection, the SSH tunnel has been established. The SSH client window must be kept open for the SSH tunnel to remain established.

Any data sent on the PC to TCP port 5555 to localhost or 127.0.0.1 will be forwarded to 123.456.789.100:5005. Any data from the device's serial port will be forwarded to the PC on the arbitrary TCP port used to connect to 127.0.0.1:5555.

For other Windows SSH clients, please refer to the documentation for more details on how to configure SSH tunneling or SSH port forwarding.

## 4.3 Linux PC Configuration

From a Linux command line console, enter the following command to establish a SSH tunnel :

```
ssh -L <Source Port>:localhost:<Destination Port> <Destination Host>
```

For example, with a source port of 5555, TCP PAD port of 5005, and a device WAN IP of 123.456.789.100, use the following command:

```
ssh -L 5555:localhost:5005 123.456.789.100
```

After a successful SSH connection, the SSH tunnel has been established. The SSH client session must be kept open for the SSH tunnel to remain established.

Any data sent on the PC to TCP port 5555 to localhost or 127.0.0.1 will be forwarded to 123.456.789.100:5005. Any data from the device's serial port will be forwarded to the PC on the arbitrary TCP port used to connect to 127.0.0.1:5555.

## 5 Persistent SSH Connections

To make the SSH tunnel connection robust against any wireless network disconnections, third-party software needs to be used (e.g. MyEnTunnel in Windows and autossh in Linux). This third-party software, to be installed on the remote server, detects when the SSH tunnel has dropped or stops responding to client requests and automatically re-establishes a new SSH connection.

Please refer to documentation for third-party software used to maintain persistent SSH connections for details.

## 6 Technical Support/Warranty

**Cypress Solutions Service  
Support Group**

1.877.985.2878 or 604.294.4465

9.00am to 5.00pm PST

support@cypress.bc.ca