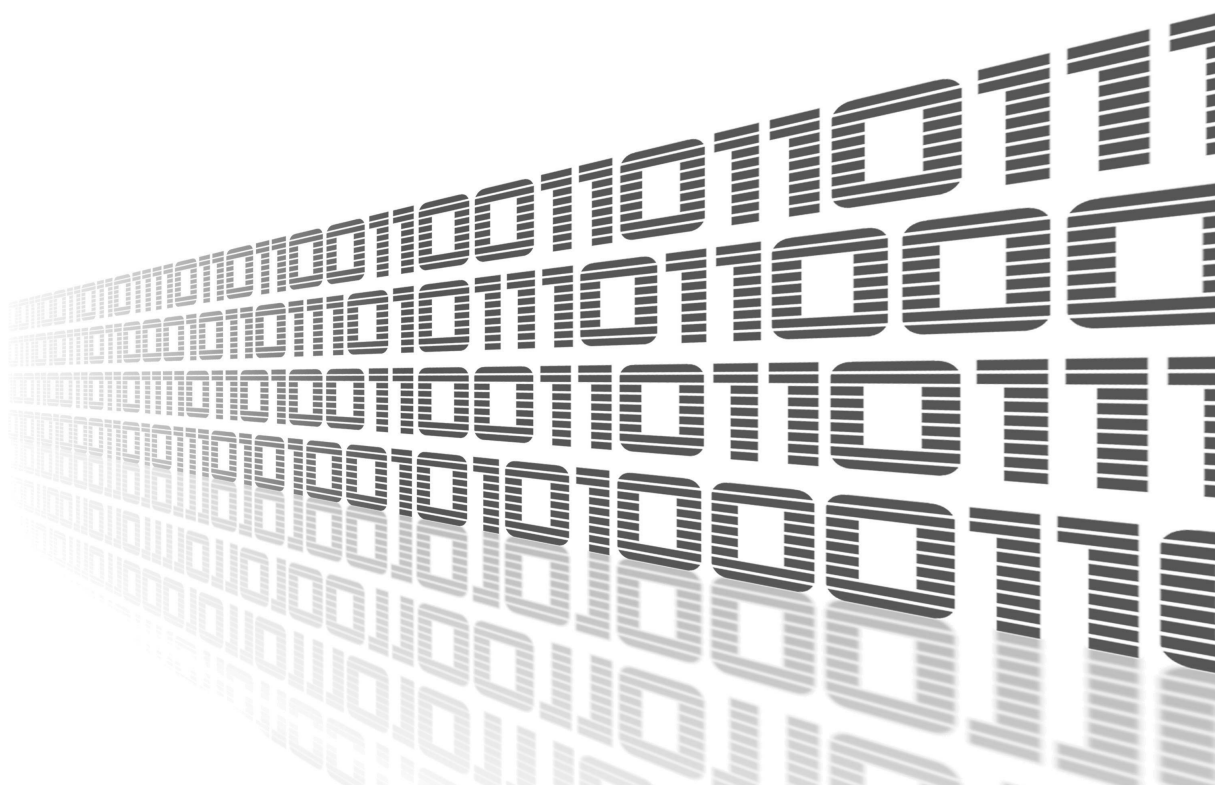




User Module

Stunnel

APPLICATION NOTE



ADVANTECH

Used symbols



Danger – Information regarding user safety or potential damage to the router.



Attention – Problems that may arise in specific situations.



Information or notice – Useful tips or information of special interest.



Example – Example of function, command or script.



Advantech Czech s.r.o., Sokolska 71, 562 04 Usti nad Orlici, Czech Republic

Document No. APP-0066-EN, revised on November 9, 2021. Released in the Czech Republic.

Contents

1	Description of user module	2
2	Configuration	4
2.1	Model example	5
3	System Log	7
4	Licenses	8
5	Related Documents	9

List of Figures

1	Change in communication after activation of stunnel	2
2	Web interface	3
3	Configuration form	4
4	Example of stunnel configuration	5
5	Example of SMTP configuration	6
6	Diagram of an example of stunnel configuration	6
7	System Log	7
8	Licenses	8

List of Tables

1	Description of items in the configuration form	4
---	--	---

1. Description of user module



User module *Stunnel* is not contained in the standard router firmware. Uploading of this user module is described in the Configuration manual (see [1, 2]). The user module is v2, v3 and v4 router platforms compatible.

This module allows the router to create an encrypted network tunnel for which it applies that at one end – either the input or output – data is wrapped in SSL. This means that data on the input is either encrypted, then it is decrypted on the output, or vice versa. Stunnel is primarily designed for adding SSL encryption to communication channels that can not support it. This results in a significant increase of communication security (within these channels). It can be used as additional functionality for commonly used servers, which are running by inetd daemon (Linux daemon which listens to the communication on the network interface and if it is necessary, runs servers for handling requirements). These have included POP2, POP3 or IMAP. Thanks to this module it is also possible to add SSL encryption to NNTP, SMTP and HTTP services which are run by standalone daemons or to PPP tunnels.

The example below shows a change in communication after activation of stunnel.

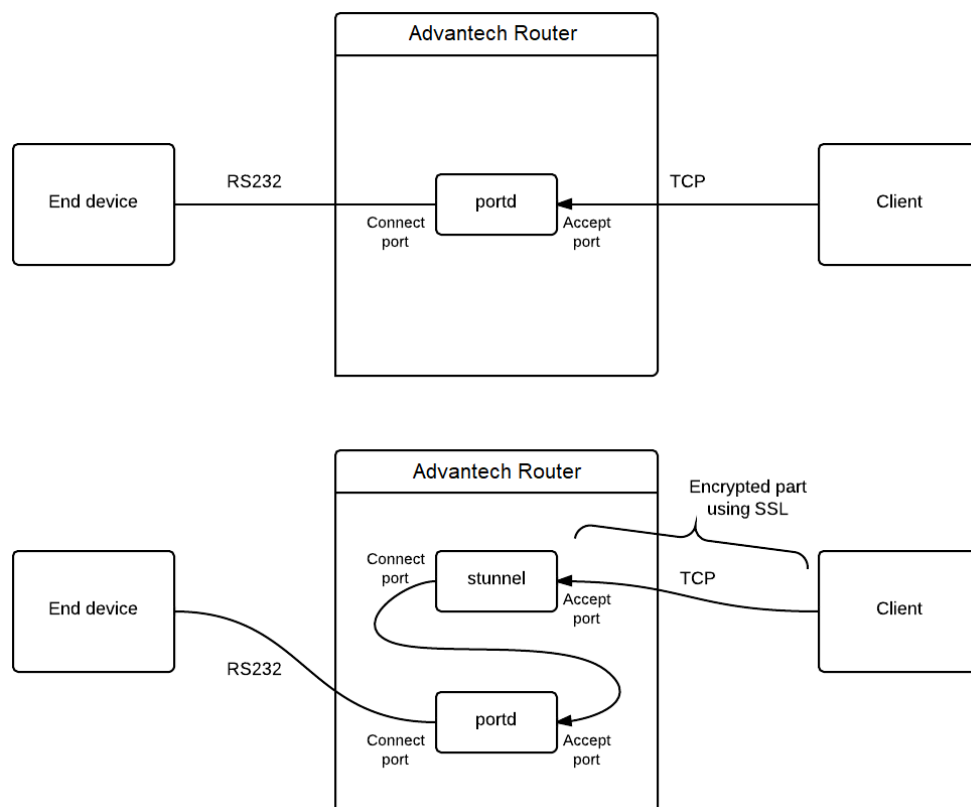


Figure 1: Change in communication after activation of stunnel

For configuration *Stunnel* is available web interface, which is invoked by pressing the module name on the *User modules* page of the router web interface. The left part of this user module web interface contains the menu, where are items – *Status*, *Configuration*, *Information* and *Customization*. *Status* contains *System Log*, *Configuration* contains *Global*, where all the settings of the module are located, *Information* section contains informations about licenses and finally *Customization* contains only *Return* item, which switches this web interface to the interface of the router.

Stunnel

Status	Stunnel Configuration					
System Log	☐ Enable Stunnel					
Configuration	Role	Name	Accept Port	Connect Port	Host **	Protocol *
Global	☐ server				127.0.0.1	
Information	☐ server				127.0.0.1	
Licenses	☐ server				127.0.0.1	
Customization	☐ server				127.0.0.1	
Return	☐ server				127.0.0.1	
	☐ server				127.0.0.1	
	☐ server				127.0.0.1	
	☐ server				127.0.0.1	
	☐ server				127.0.0.1	
	☐ server				127.0.0.1	

* can be blank
 ** defaults to 127.0.0.1 when left blank

Figure 2: Web interface

2. Configuration

Configuration of *Stunnel* user module is performed via the configuration form in the module web interface. The first item in this form – *Enable Stunnel* – is used to activate these user module. Other items have the following meanings:

Item	Description
Enable Stunnel	Enables/Disables defined stunnel
Role	Select server/client role of the stunnel
Name	An arbitrary name of defined stunnel
Accept Port	Port number on which connections are accepted
Connect Port	Number of a remote port where data is sent
Host	Address of a server to which stunnel connects to
Protocol	Specifies application protocol used for transporting. It is possible to choose between <i>SMTP</i> , <i>IMAP</i> , <i>POP3</i> , <i>CIFS</i> , <i>NNTP</i> or not to define the protocol.

Table 1: Description of items in the configuration form

Stunnel Configuration

☐ Enable Stunnel

Role	Name	Accept Port	Connect Port	Host **	Protocol *
☐ server				127.0.0.1	
☐ server				127.0.0.1	
☐ server				127.0.0.1	
☐ server				127.0.0.1	
☐ server				127.0.0.1	
☐ server				127.0.0.1	
☐ server				127.0.0.1	
☐ server				127.0.0.1	
☐ server				127.0.0.1	
☐ server				127.0.0.1	
☐ server				127.0.0.1	

* can be blank

** defaults to 127.0.0.1 when left blank

Apply

Figure 3: Configuration form

2.1 Model example

Let's assume that you use SMTP internet protocol for transferring e-mail messages and you want to wrap transmitted data to SSL. Stunnel needs to be set as follows:

- Choose a *client* as a *Role*.
- Select a *Name* in any form, e.g. *snmp_test*.
- *Accept port* has the value 25.
- Set *Connect port* to the value 465.
- *Host* item must be filled in depending on the provider of email service. For example: Write *smtp.gmail.com* for Gmail.
- Finally, do not forget to check the ☐ box to enable configured stunnel and also check the *Enable Stunnel* item for module activation.

Stunnel Configuration						
☒ Enable Stunnel						
Role	Name	Accept Port	Connect Port	Host **	Protocol *	
☒ client	ClientTunnel	25	465	smtp.gmail.com		
☒ server	ServerTunnel	31313	30303	192.168.2.2		
☐ server				127.0.0.1		
☐ server				127.0.0.1		
☐ server				127.0.0.1		
☐ server				127.0.0.1		
☐ server				127.0.0.1		
☐ server				127.0.0.1		
☐ server				127.0.0.1		
☐ server				127.0.0.1		
☐ server				127.0.0.1		

* can be blank
 ** defaults to 127.0.0.1 when left blank

Apply

Figure 4: Example of stunnel configuration

It is also necessary to configure the SMTP in the router web interface. In our case, this means the following:

- *SMTP Server Address* box must contain the address of localhost, i.e. 127.0.0.1.
- To *Username* and *Password* boxes fill in your login information.
- To *Own Email Address* item fill in your email.

SMTP Configuration	
SMTP Server Address	127.0.0.1
SMTP Port	25
Secure Method	SSL/TLS ▼
Username	username
Password	
Own Email Address	name@gmail.com
Apply	

Figure 5: Example of SMTP configuration

The figure below shows a schematic diagram of the situation corresponding to the described example.

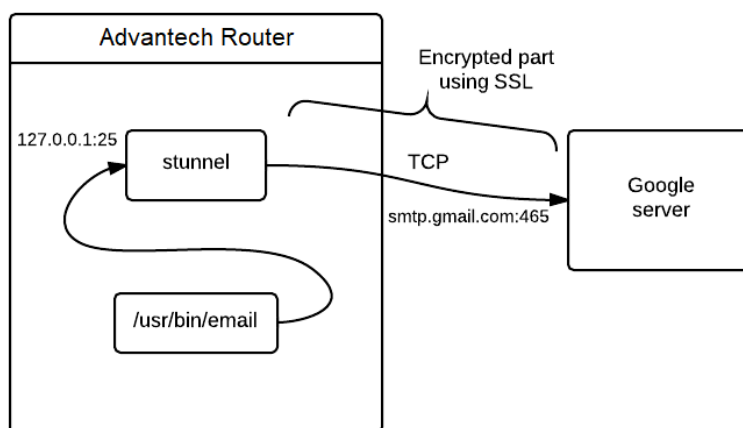


Figure 6: Diagram of an example of stunnel configuration

3. System Log

In case of any problems with connection it is possible to view the system log by pressing the *System Log* menu item. In the window are displayed detailed reports from individual applications running in the router. Activity of *Stunnel* module is indicated in rows starting with word "stunnel". Press *Save Log* button to save the system log to your computer.

System Log

System Messages

```

2021-11-09 00:33:44 usb1d[1456]: connection established
2021-11-09 00:33:44 usb1d[1456]: local IPv4 address 10.80.0.21
2021-11-09 00:33:44 usb1d[1456]: primary DNSv4 address 10.0.0.1
2021-11-09 00:33:44 usb1d[1456]: script /etc/scripts/ip-pre-up-mwan started
2021-11-09 00:33:44 bard[1020]: usb0 connection is available on mwan
2021-11-09 00:33:44 usb1d[1456]: script /etc/scripts/ip-pre-up-mwan finished
2021-11-09 00:33:44 usb1d[1456]: script /etc/scripts/ip-up-mwan started
2021-11-09 00:33:44 usb1d[1456]: script /etc/scripts/ip-up-mwan finished
2021-11-09 00:33:45 bard[1020]: backup route selected: "Mobile WAN"
2021-11-09 00:33:45 bard[1020]: script /etc/scripts/ip-up usb0 started
2021-11-09 00:33:46 bard[1020]: script /etc/scripts/ip-up usb0 finished, status = 0x0
2021-11-09 00:33:47 dnsmasq[1294]: reading /etc/resolv.conf
2021-11-09 00:33:47 dnsmasq[1294]: using nameserver 10.0.0.1#53
2021-11-09 00:33:49 sshd[1609]: Accepted keyboard-interactive/pam for root from 10.64.0.1 port 45773 ssh2
2021-11-09 00:33:49 pam_unix(sshd:session): session opened for user root by (uid=0)
2021-11-09 07:01:12 http: user 'root' logged in from 10.64.0.1
2021-11-09 07:02:57 http: user 'root' added user module 'stunnel.v3.tgz'
2021-11-09 07:18:08 stunnel: LOG5[1259:3070153408]: stunnel 4.57 on arm-unknown-linux-gnu platform
2021-11-09 07:18:08 stunnel: LOG5[1259:3070153408]: Compiled/running with OpenSSL 1.0.2u 20 Dec 2019
2021-11-09 07:18:08 stunnel: LOG5[1259:3070153408]: Threading:PTHREAD Sockets:POLL,IPv6 SSL:ENGINE,OCSP
2021-11-09 07:18:08 stunnel: LOG5[1259:3070153408]: Reading configuration from file /var/stunnel/stunnel_client.conf
2021-11-09 07:18:08 stunnel: LOG5[1259:3070153408]: Configuration successful
2021-11-09 07:30:00 http: user 'root' updated configuration of SMTP
2021-11-09 07:36:27 sshd[1609]: pam_unix(sshd:session): session closed for user root

```

Save Log

Save Report

Figure 7: System Log

4. Licenses

Summarizes Open-Source Software (OSS) licenses used by this module.

Stunnel Licenses		
Project	License	More Information
stunnel	GPLv2	License
openssl	OpenSSL	License

Figure 8: Licenses

5. Related Documents

- [1] Advantech Czech: **v2 Routers Configuration Manual** (MAN-0021-EN)
- [2] Advantech Czech: **SmartFlex Configuration Manual** (MAN-0023-EN)
- [3] Advantech Czech: **SmartMotion Configuration Manual** (MAN-0024-EN)
- [4] Advantech Czech: **SmartStart Configuration Manual** (MAN-0022-EN)
- [5] Advantech Czech: **ICR-3200 Configuration Manual** (MAN-0042-EN)



Product-related documents can be obtained on *Engineering Portal* at icr.advantech.cz address.