VMS Software

Stunnel V5.75 for VSI OpenVMS

Release Notes

Publication Date: July 2025

Operating Systems: VSI OpenVMS Alpha Version 8.4-2L1 or higher
VSI OpenVMS IA-64 Version 8.4-1H1 or higher
VSI OpenVMS x86-64 Version 9.2-2 or higher

Software Version: Stunnel V5.75 for VSI OpenVMS

Kit Names: VSI-AXPVMS-STUNNEL-V0575-0-1.PCSI
VSI-I64VMS-STUNNEL-V0575-0-1.PCSI
VSI-X86VMS-STUNNEL-V0575-0-1.PCSI

VMS Software, Inc. (VSI)
Boston, Massachusetts, USA

Table of Contents

1. Introduction

Thank you for your interest in this port of stunnel to VSI OpenVMS. The current release of stunnel for VSI OpenVMS is based on the stunnel 5.75 distribution.

Stunnel (https://www.stunnel.org/) is a proxy designed to add SSL/TLS encryption functionality to existing client and server applications without any changes to application code. Stunnel is optimized for security and scalability, making it well-suited for large numbers of concurrent connections. Stunnel uses the OpenSSL library for encryption and is distributed under the GNU GPL version 2 license or later with an OpenSSL exception.

This port of the stunnel for VSI OpenVMS includes all functionality provided by the open-source release, with the exception of IPv6 support which will be included in a future release. Additional information about stunnel can be found at https://www.stunnel.org/.

2. Acknowledgements

VSI would like to acknowledge the work of stunnel author Michał Trojnara and all community members for their ongoing efforts in developing and supporting this open-source software project. VSI would also like to thank Duncan Morris for his thorough testing of stunnel on VSI OpenVMS, which identified a significant thread-related issue that could cause a deadlock situation. In addition to identifying the problem, Duncan also kindly provided a fix that is included in this release.

3. What's New in This Release

For a detailed description of the features and bug fixes included in this release, please refer to https://www.stunnel.org/NEWS.html.

SSL/TLS support is statically linked into this release of stunnel for VSI OpenVMS and uses OpenSSL 3.0. This release of stunnel for VSI OpenVMS is multi-threaded and can take full advantage of multiple processor cores or CPUs to achieve high levels of scalability.

4. Requirements

The kit you that are receiving has been compiled and built using the operating system and product versions listed below:

- VSI OpenVMS Alpha V8.4-2L1 or higher, VSI OpenVMS IA-64 V8.4-1H1 or higher, OpenVMS x86-64 V9.2-2 or higher
- VSI TCP/IP Services
- VSI recommends that the software is installed on an ODS-5-enabled file system.

While it is highly likely that you will have no problems installing and using the kit on systems running higher versions of the operating system or products listed above, VSI does not recommend running older versions.

5. Recommended Reading

Before using stunnel for VSI OpenVMS, it is recommended that users read the documentation available at https://www.stunnel.org/docs.html in order to better understand how to use and configure the software.

6. Installing the Kit

The kit is provided as an architecture-specific OpenVMS PCSI kit (VSI-AXPVMS-STUNNEL-V0575-0-1.PCSI, VSI-I64VMS-STUNNEL-V0575-0-1.PCSI, and VSI-X86VMS-STUNNEL-V0575-0-1.PCSI) that can be installed by a suitably privileged user via the following command:

```
$ PRODUCT INSTALL STUNNEL
```

The installation will then proceed as follows (output may differ slightly from that shown, depending on platform and other factors):

```
Performing product kit validation of signed kits ...

The following product has been selected:
    VSI I64VMS STUNNEL V5.75-0            Layered Product

Do you want to continue? [YES]

Configuration phase starting ...

You will be asked to choose options, if any, for each selected
product and for any products that may be installed to satisfy
software dependency requirements.

Configuring VSI I64VMS STUNNEL V5.75-0: STUNNEL for OpenVMS

    © 1998-2025 Michal Trojnara, 2025 VMS Software Inc.

    VSI Software Inc.

* This product does not have any configuration options.

Execution phase starting ...

The following product will be installed to destination:
    VSI I64VMS STUNNEL V5.75-0            DISK$IA21_842L1:[VMS$COMMON.]

Portion done: 0%...90%...100%

The following product has been installed:
    VSI I64VMS STUNNEL V5.75-0            Layered Product

VSI I64VMS STUNNEL V5.75-0: STUNNEL for OpenVMS

    Post-installation tasks are required.

    To start STUNNEL at system boot time, add the following
    lines to SYS$MANAGER:SYSTARTUP_VMS.COM:

        $ file := SYS$STARTUP:STUNNEL$STARTUP.COM
        $ if f$search("'file'") .nes. "" then @'file'

    To shutdown STUNNEL at system shutdown, add the following
    lines to SYS$MANAGER:SYSHUTDWN.COM:

        $ file := SYS$STARTUP:STUNNEL$SHUTDOWN.COM
        $ if f$search("'file'") .nes. "" then @'file'
```

```
Before starting STUNNEL you will need to create the
configuration file STUNNEL$ROOT:[ETC]STUNNEL.CONF.
```

6.1. Post-Installation Steps

After the installation has successfully completed, you must include the commands displayed at the end of the installation procedure in SYSTARTUP_VMS.COM and SYSHUTDWN.COM. This is to ensure that stunnel is started and stopped when OpenVMS is booted and shut down.

Before you can use stunnel it is necessary to create a configuration file that defines the services stunnel will support. By default the configuration file used by stunnel for VSI OpenVMS will be STUNNEL$ROOT:[ETC]STUNNEL.CONF; however you can modify the file SYS$STARTUP:STUNNEL$RUN.COM to specify another configuration file name if you so wish, but keep in mind that any such changes may be overwritten if a new stunnel kit is installed, and it is therefore recommended to use STUNNEL$ROOT:[ETC]STUNNEL.CONF.

The specific details of defining stunnel services depends somewhat on the type of the service, and it is recommended that you read thoroughly the documentation provided at https://www.stunnel.org/docs.html in order to become familiar with the configuration process. Sample configurations for various services can also be found on the internet and adapted as necessary.

To get you started, stunnel for VSI OpenVMS includes several sample configuration files, including the files TELNET-CLIENT.CONF and TELNET-SERVER.CONF (both can be found in STUNNEL$ROOT:[ETC]), that can be used to set up a secure telnet tunnel between two OpenVMS servers. To use these sample configurations, on the client OpenVMS system TELNET-CLIENT.CONF should be copied or renamed to STUNNEL.CONF and edited to change the `ACCEPT` and `CONNECT` parameters as appropriate to your environment (specifically the host name should be changed to that of the target server), and similarly on the server system TELNET-SERVER.CONF should be copied or renamed to STUNNEL.CONF and edited to change the `ACCEPT` parameter as appropriate to match your client configuration. You should then be able to start stunnel on both nodes, and if on the client system you telnet to *localhost* using the port specified `ACCEPT` port number you should be connected through to the server node via the tunnel.

The template configuration file (STUNNEL$ROOT:[ETC] STUNNEL^.CONF.TEMPLATE) is also provided, which includes details for a number of services. This file may be copied to STUNNEL$ROOT:[ETC]STUNNEL.CONF and modified as necessary.

Note

Stunnel for VSI OpenVMS includes a self-signed certificate. This should only be used for basic testing purposes; the use of self-signed certificates for any other purpose is not recommended. It should also be noted that the self-signed certificate included with the kit has an expiration date.

6.2. Privileges and Quotas

The privileges TMPMBX, NETMBX, BYPASS, SYSPRV, and DETACH are required in order to run the stunnel start-up and shutdown scripts; the stunnel process (run as a detached process) will inherit the default privileges for the username under which it is started.

The stunnel process can require considerable resources in order to operate efficiently when supporting large numbers of connections. The quota values below should be adequate for most purposes; however, resource usage should be carefully monitored, and quotas adjusted as necessary.

```
Maxjobs:           0  Fillm:         256  Bytlm:         128000
Maxacctjobs:       0  Shrfillm:       0  Pbytlm:             0
Maxdetach:         0  BIOlm:         150  JTquota:         4096
Prclm:            50  DIOlm:         150  WSdef:           4096
Prio:              4  ASTlm:         300  WSquo:           8192
Queprio:           4  TQElm:         100  WSextent:       16384
CPU:          (none)  Enqlm:        4000  Pgflquo:       256000
```

If the stunnel process is expected to support large numbers of concurrent connections then it may also be necessary to increase the CHANNELCNT system parameter (this parameter can usually be safely set to its maximum value of 65535).

6.3. Installing in an Alternative Location

By default, stunnel will be installed in SYS$SYSDEVICE:[VMS$COMMON]. If you wish to install the software in an alternative location, this can be achieved by using the **/DESTINATION** qualifier with the **PRODUCT INSTALL** command to specify the desired location; however, it is important to note that an additional manual step will then be required to complete the installation. Specifically, when an alternative destination is specified, start-up, shutdown, and related command procedures will be placed into subdirectories residing under the specified destination directory. If you wish to run these files from your standard SYS$STARTUP and SYS$MANAGER directories they will need to be copied from the destination subdirectories into the appropriate locations.

7. What's Missing in this Release?

The supplied kit for VSI OpenVMS does not currently support IPv6. It is anticipated that this problem will be resolved in future releases.