与SSL和TLS的内容安全工具数据加密

目录

简介

本文为安全套接字协议层(SSL)和传输层安全(TLS)加密方法提供定义并且描述如何使用他们。

SSL和TLS概述

SSL和TLS加密方法是数据加密的两个高使用的方法在网络数据流或传输会话。

Ssl encryption方法由Netscape为了在其普遍采用时横断互联网20世纪90年代的安全HTTP通信最初开发。SSL版本2.0是第一个公共版本，短期跟随由SSL版本3.0，更新为了寻址在以前版本的一些严重的安全漏洞。

TLS版本1.0是后继路由对SSL版本3.0。它提供安全算法，警告和规格增强。虽然更改是细微的，他们是足够猛烈的互相使两份协议不兼容。TLS加密方法从那以后改善与另外的密码器套件，例如高级加密标准(AES)和更加安全的密钥生成算法。此时的多数当前版本是TLS版本1.2。

> **注意**： 自AsyncOS 8.5.6，支持仅TLS v1。 1.2不支持TLS v1.1。 请查看从CLI的**sslconfig**，并且选择**GUI**，**入站**或者**出站**查看可用密码器的方法。

SSL和TLS使用情况

今天，使用安全传输，例如简单邮件传输协议(SMTP)和HTTPS处理的多数客户端服务器程序，根据SSL版本3.0和TLS版本1.x。 虽然许多应用程序有安全传输的内置支持类似SSL和TLS，所有程序可以是转入的安全隧道。许多新应用为此演变，例如安全电话通信类似会话初始化协议(SIP)和VPN，利用一个已修改TLS加密方法是转入的UDP类型IP信息包(dTLS)。

当可互换时有时使用期限SSL和TLS，协议不是相同的。主要的区别围绕由客户端和服务器协商的密码器套件(加密类型)，以及他们选择那些密码器的方法。本质上，因为其开发是稳健的更多开放和和由IETF，标准化TLS是网络通信加密的首选的平均值。

注意：详细信息在TLS版本1.2规格和SSL互联网草案的参考的RFC 5246对于SSL版本3.0信息。