Encripción de datos contenta del dispositivo de seguridad con el SSL y TLS

Contenido

Introducción

Este documento proporciona las definiciones para los métodos de encripción de Secure Sockets Layer (SSL) y de Transport Layer Security (TLS) y describe cómo se utilizan.

Descripción SSL y de TLS

Los métodos de encripción SSL y de TLS son los dos métodos alto-más usados para la encripción de datos sobre una sesión de la secuencia o del transporte de la red.

El método de encripción de SSL fue desarrollado originalmente por Netscape para asegurar las comunicaciones HTTP que atravesaron el Internet durante su adopción extensa en los años 90. El SSL versión 2.0 era la primera difusión pública, seguida pronto por el 3.0 del SSL versión, que era actualizada para dirigir algunos errores de seguridad serios en la versión anterior.

El TLS versión 1.0 era el sucesor al 3.0 del SSL versión. Ofreció el algoritmo de seguridad, alertar, y las mejoras de la especificación. Aunque los cambios fueran sutiles, eran bastante drásticos hacer los dos protocolos incompatibles el uno con el otro. El método de encripción de TLS se ha mejorado desde entonces con las habitaciones adicionales de la cifra, tales como Advanced Encryption Standard (AES), y algoritmos más seguros de la generación de claves. La mayoría de la versión actual ahora es el TLS versión 1.2.

> Nota: A partir de AsyncOS 8.5.6, solamente se soporta el v1 de TLS. El v1.1 de TLS, 1.2 todavía no se soporta. Revise por favor el **sslconfig del** CLI, y elija el **GUI**, **ENTRANTE**, o **SALIENTE** para ver los métodos de la cifra disponibles.

Uso SSL y de TLS

Hoy, la mayoría de los programas del servidor del cliente que utilizan los transportes seguros, tales como Simple Mail Transfer Protocol (SMTP) y transacciones HTTPS, se basan en el 3.0 y el TLS versión 1.x del SSL versión. Aunque muchas aplicaciones tengan soporte incorporado para los transportes seguros como el SSL y TLS, cualquier programa puede ser túneles seguros transportados. Muchas nuevas aplicaciones se han desarrollado por este motivo, por ejemplo asegure las comunicaciones del teléfono como el Session Initiation Protocol (SIP) y los VPN, que hacen uso de un método de encripción modificado de TLS que sea paquetes del IP transportados del UDP-tipo (dTLS).

Mientras que los términos SSL y TLS se utilizan a veces alternativamente, los protocolos no son idénticos. Las diferencias principales giran alrededor de las habitaciones de la cifra (tipos de encripción) que son negociadas por el cliente y servidor, así como de los métodos por los cuales seleccionan esas cifras. Esencialmente, TLS es los medios preferidos para el cifrado de las comunicaciones de la red, pues su desarrollo es más abierto y robusto y ha sido estandardizado por el IETF.

Nota: Refiera al RFC 5246 para los detalles en las especificaciones del TLS versión 1.2 y a los Borradores de Internet SSL para la información del 3.0 del SSL versión.