Criptografia de dados satisfeita da ferramenta de segurança com SSL e TLS

Índice

Introdução

Este documento fornece definições para os métodos de criptografia do secure sockets layer (SSL) e do Transport Layer Security (TLS) e descreve como são usadas.

Vista geral SSL e TLS

Os métodos de criptografia SSL e TLS são os dois métodos alto-os mais usados para a criptografia de dados sobre uma sessão do córrego ou do transporte da rede.

O método de criptografia SSL foi desenvolvido originalmente por Netscape a fim fixar as comunicações HTTP que atravessaram o Internet durante sua adoção difundida nos anos 90. A versão de SSL 2.0 era o primeiro lançamento público, seguido logo pelo 3.0 da versão de SSL, que foi atualizado a fim endereçar algumas falhas de Segurança sérias na versão anterior.

A versão TLS 1.0 era o sucessor ao 3.0 da versão de SSL. Ofereceu o algoritmo de segurança, a alerta, e os realces da especificação. Embora as mudanças fossem suteis, eram drásticas bastante fazer um com o outro os dois protocolos incompatíveis. O método de criptografia TLS tem sido melhorado desde com as séries adicionais da cifra, tais como o Advanced Encryption Standard (AES), e algoritmos mais seguros da geração chave. A maioria de versão atual é neste tempo a versão TLS 1.2.

> Nota: Até à data de AsyncOS 8.5.6, somente o TLS v1 é apoiado. O TLS v1.1, 1.2 não é apoiado ainda. Reveja por favor o **sslconfig do** CLI, e escolha o **GUI**, **DE ENTRADA**, ou **DE PARTIDA** ver os métodos da cifra disponíveis.

Uso SSL e TLS

Hoje, a maioria de programas do servidor cliente que utilizam transportes seguros, tais como o Simple Mail Transfer Protocol (SMTP) e as transações HTTPS, são baseados no 3.0 da versão de SSL e na versão TLS 1.x. Embora muitos aplicativos tenham o suporte embutido para transportes seguros como o SSL e o TLS, todo o programa pode ser levado sobre túneis seguros. Muitos aplicativos novos evoluíram por este motivo, como fixe as comunicações do telefone como o Session Initiation Protocol (SIP) e os VPN, que utilizam um método de criptografia alterado TLS que seja levado sobre o UDP-tipo pacotes IP (dTLS).

Quando os termos SSL e TLS forem usados às vezes permutavelmente, os protocolos não são

idênticos. As diferenças principal revolvem em torno das séries da cifra (tipos de criptografia) que são negociadas pelo cliente e servidor, assim como dos métodos por que selecionam aquelas cifras. Essencialmente, o TLS é os meios preferidos para a criptografia das comunicações de rede, porque seu desenvolvimento é mais aberto e robusto e foi estandardizado pelo IETF.

Nota: Refira o RFC 5246 para detalhes nas especificações da versão TLS 1.2 e o esboço do Internet SSL para a informação do 3.0 da versão de SSL.