包括的にサポートされる暗号スイート

内容

はじめに

このドキュメントでは、Umbrellaでサポートされる暗号スイートについて説明します。

概要

Cisco Umbrellaは、Secure Web Gateway(SWG)、インテリジェントプロキシ、およびブロックページとの間でHTTPS接続をネゴシエートする際に、前述の暗号スイートを受け入れます。これらのサービスに正常に接続するには、クライアントは上記の暗号スイートの少なくとも1つをサポートしている必要があります。

シスコの製品セキュリティベースライン(PSB)では、機能、開発、およびテストに関するセキュリティ要件が定義されています。これらの要件の一部は、サポートされる暗号スイートのリストに適用されます。これらは情報提供の目的で記載されており、Umbrellaでは設定できません。

PSB認定の暗号スイート

ECDHE-ECDSA-AES128-SHA	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
ECDHE-ECDSA-AES128-SHA256	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
ECDHE-ECDSA-AES128-GCM-SHA256	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
ECDHE-ECDSA-AES256-SHA384	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
ECDHE-ECDSA-AES256-GCM-SHA384	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
ECDHE-RSA-AES128-SHA	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
ECDHE-RSA-AES128-SHA256	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256

ECDHE-RSA-AES128-GCM-SHA256	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
ECDHE-RSA-AES256-SHA384	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
ECDHE-RSA-AES256-GCM-SHA384	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
AES128-SHA	TLS_RSA_WITH_AES_128_CBC_SHA
AES128-SHA256	TLS_RSA_WITH_AES_128_CBC_SHA256
AES128-GCM-SHA256	TLS_RSA_WITH_AES_128_GCM_SHA256
AES256-SHA256	TLS_RSA_WITH_AES_256_CBC_SHA256
AES256-GCM-SHA384	TLS_RSA_WITH_AES_256_GCM_SHA384
AES256-GCM-SHA384	TLS_AES_256_GCM_SHA384
AES128-GCM-SHA256	TLS_AES_128_GCM_SHA256

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。