

CRES : Chiffrements SSL utilisés

Contenu

[Introduction](#)

[Chiffrements SSL utilisés](#)

[Informations connexes](#)

[Cisco relatif prennent en charge des discussions de la Communauté](#)

Introduction

Ce document décrit qui les chiffrements SSL sont en service avec le service d'enveloppe recommandée de Cisco (CRES) par rapport à l'appliance de sécurité du courrier électronique de Cisco (ESA).

Chiffrements SSL utilisés

Suites de chiffrement (suites SSL 3+ dans la commande serveur-préférée ; suites désapprouvée et SSL 2 à l'extrémité) :

TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c) 128
TLS_RSA_WITH_RC4_128_SHA (0x5) 128 FAIBLES
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d) 256
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d) 256
TLS_RSA_WITH_AES_256_CBC_SHA (0x35) 256
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (0x84) 256
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c) 128
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) 128
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (0x41) 128
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa) 112

Des informations complètes peuvent être obtenues à tout moment des laboratoires SSL : [État SSL : res.cisco.com \(184.94.241.74\)](https://res.cisco.com/184.94.241.74)

[Informations connexes](#)

- [Appliance de sécurité du courrier électronique de Cisco - Guides d'utilisateur](#)
- [Support et documentation techniques - Cisco Systems](#)