目次

概要

このドキュメントでは、Cisco IOS® および IOS-XE プラットフォームでの次世代暗号化（NGE）サポートについて説明します。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco IOS の複数のバージョン（表に記載）
- Cisco IOS XE の複数のバージョン（表に記載）
- 複数の Cisco プラットフォーム（表に記載）

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

NGE のアルゴリズム

NGE を構成するアルゴリズムは、暗号化技術における 30 年間以上の世界的な進歩と進化が結実したものです。 NGE の各要素には独自の歴史があり、それらは NGE のアルゴリズムとその長年にわたる学術的、社会的レビューの多様な歴史を表しています。 NGE は世界的規模で作成され、世界的規模で見直され、一般的に利用されているアルゴリズムです。

NGE のアルゴリズムは、インターネット技術特別調査委員会（IETF）、IEEE、その他の国際標準に取り入れられています。 その結果、NGE のアルゴリズムはインターネット鍵交換バージョン 2（IKEv2）など、ユーザのデータを保護するための最新かつ高度にセキュアなプロトコルに適用されてきました。

暗号化アルゴリズムのタイプは次のとおりです。

- 対称暗号化 - GCM（Galois/Counter mode）の 128 ビットまたは 256 ビット Advanced Encryption Standard（AES）
- ハッシュ - セキュア ハッシュ アルゴリズム（SHA）-2（SHA-256、SHA-384、および SHA-512）
- デジタル署名 - 楕円曲線デジタル署名アルゴリズム（ECDSA）
- 鍵共有 - Elliptic Curve Diffie-Hellman（ECDH）

IOS および IOS XE プラットフォームでの NGE サポート

この表は Cisco IOS ベースおよび IOS XE ベースのプラットフォームの NGE サポートをまとめたものです。

プラットフォーム	暗号化エンジンのタイプ	NGE にポート
IOS Classic が稼働するすべてのプラットフォーム	IOS ソフトウェア暗号化エンジン	○
7200	VAM/VAM2/VSA	なし
ISR G1	All	なし
ISR G2 2951、3925、3945	オンボード	○
ISR G2（3925E/3945E を除く）	VPN-ISM1	○
ISR G2 1900、2901、2911、2921、2951、3925、3945、3925E、3945E	オンボード	○
ISR G2 CISCO87x	ソフトウェア/ハードウェア	なし
ISR G2 CISCO86x/C86x	ソフトウェア	○
ISR G2 C812/C819	ソフトウェア/ハードウェア	○
ISR G2 CISCO88x/CISCO89x	ソフトウェア/ハードウェア	○
ISR G2 C88x	ソフトウェア/ハードウェア	○
6500/7600	VPN-SPA	なし
ASR 1000	オンボード	○
ISR4451-X	オンボード	○
ISR4321、4331、4351、4431	オンボード	○
CSR1000v	ソフトウェア	○

注 1： ISR G2 プラットフォームでは、ECDH/ECDSA が設定されている場合、これらの暗号操作は暗号トウェアで動作します。
注 2： ISR G2 CISCO86x/C86x はハードウェア暗号化エンジンで NGE をサポートしません。
注 3： ISR G2 CISCO88x/CISCO89x のハードウェア サポートはバージョン 15.2(4)M3 以降から SHA-2

。
注 4： 次の C88x SKU には、NGE に対するハードウェア サポートはありません。 C881SRST-K9、C88
C881SRSTW-GN-E-K9、C881-CUBE-K9、C881-V-K9、C881G-U-K9、C881G-S-K9、C881G-V-K9、C
C881G+7-A-K9、C886SRST-K9、C886SRSTW-GN-E-K9、C886VA-CUBE-K9、C886VAG+7-K9、C88
GN-A-K9、C887SRSTW-GN-E-K9、C887VSRST-K9、C887VSRSTW-GNA-K9、C887VSRSTW-GNE-K
C887VA-V-W-E-K9、C887VA-CUBE-K9、C887VAG-S-K9、C887VAG+7-K9、C887VAMG+7-K9、C888
C888SRSTW-GN-E-K9、C888SRST-K9、C888ESRST-K9、C888ESRSTW-GNA-K9、C888ESRSTW-G
C888E-CUBE-K9、C888EG+7-K9。
注 5： NGE コントロール プレーン（ECDH および ECDSA）のサポートはバージョン XE3.7 (15.2(4)S)
ロール プレーン SHA-2 のサポートは、IKEv2 のみを対象にしています（IKEv1 サポートはバージョン X
ました）。 Octeon ベースのプラットフォーム（ASR1001-X、ASR1002-X、ESP-100、および ESP-200
レーンのサポートがバージョン XE3.8 (15.3(1)S) で追加されました。 データプレーンのサポートは他の
使用できません。

他の NGE 機能のサポート

GETVPN の NGE サポート

- ISR G2 プラットフォームの Cisco IOS ソフトウェア サポートは、バージョン 15.2(4) M から開始します。
- ASR サポートは、Cisco IOS XE ソフトウェア、バージョン 3.10S（15.3(3)S）から開始します。