Cisco IOSおよびIOS-XEの次世代暗号化サポート

内容

[概要](#)
[前提条件](#)
[要件](#)
[使用するコンポーネント](#)
[NGE アルゴリズム](#)
[Cisco IOSおよびCisco IOS XEプラットフォームでのNGEサポート](#)
[他の NGE 機能のサポート](#)
[NGE の GETVPN サポート](#)
[関連情報](#)

概要

このドキュメントでは、Cisco IOS®およびCisco IOS-XEプラットフォームでのNext Generation Encryption(NGE)の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特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いています。

- 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ました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

NGE 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）

Cisco IOSおよびCisco IOS XEプラットフォームでのNGEサポート

次の表に、Cisco IOSベースおよびCisco IOS XEベースのプラットフォームでのNGEサポートの概要を示します。

プラットフォーム	暗号化エンジンのタイプ	NGE によるサポート
Cisco IOSクラシックを実行するすべてのプラットフォーム	Cisco IOSソフトウェア暗号化エンジン	Yes
7200	VAM/VAM2/VSA	No
ISR G1	すべて	No
ISR G2 2951、3925、3945	オンボード[1]	Yes
ISR G2（3925E/3945Eを除く）	VPN-ISM1	Yes
ISR G2 1900、2901、2911、2921、3925E、3945E	オンボード[1]	Yes
ISR G2 CISCO87x	ソフトウェア/ハードウェア	No
ISR G2 CISCO86x/C86x	ソフトウェア[2]	Yes
ISR G2 C812/C819	ソフトウェア/ハードウェア	Yes
ISR G2 CISCO88x/CISCO89x	ソフトウェア/ハードウェア[3]	Yes
ISR G2 C88x	ソフトウェア/ハードウェア[4]	Yes
6500/7600	VPN-SPA	No
ASR 1000	導入準備	Yes
ASR 1001-X、ASR 1002-X、ASR 1006-X、ASR 1009-X	導入準備	Yes
ASR 1001-HX、ASR1002-HX	オプションの暗号化モジュール	Yes
ISR 4451-X	導入準備	Yes
ISR 4321, 4331, 4351, 4431	導入準備	Yes
ISR 42xx	導入準備	Yes
CSR 1000v	[ソフトウェア（Software）]	Yes
ISR 1100	導入準備	Yes

Catalyst 8200、8300、8500エッジプラットフォーム	導入準備	Yes	
Catalyst 8000v	[ソフトウェア（Software）]	Yes	

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、これらの暗号化操作は暗号
なくソフトウェアで実行されます。AES-GCM-128およびAES-GCM-256暗号化アルゴリズムは、バージ
IKEv2コントロールプレーン保護でサポートされています。
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-25
ています。
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
K9、C881SRSTW-GN-E-K9、C881-CUBE-K9、C881-V-K9、C881G-U-K9、C881G-S-K9、C881G-V-K
C881G+7-K9、C881G+7-A-K9、C886SRST-K9、C886SRSTW-GN-E-K9、C886VA-CUBE-K9、C886V
C887SRST-K9、C887SRSTW-GN-A-K9、C887SRSTW-GN-E-K9、C887VSRST-K9、C887VSRSTW-G
C887VSRSTW-GNE-K9、C887VA-V-K9、C887VA-V-W-E-K9、C887VA-CUBE-K9、C887VAG-S-K9、C
C887VAMG+7-K9、C888SRSTW-GN-A-K9、C888SRSTW-GN-E-K9、C888SRST-K9、C888ESRST-K
GNA-K9、C888ESRSTW-GNE-K9、C888-CUBE-K9、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)で
初期コントロールプレーンSHA-2はIKEv2専用で、IKEv1のサポートはバージョンXE3.10(15.3(3)S)で追加
AES-GCM-128およびAES-GCM-256暗号化アルゴリズムは、バージョンXE3.12(15.4(2)S)および15.4(2)T
トロールプレーン保護でサポートされています。NGEデータプレーンのサポートは、Octeonベースのプ
(ESP-100またはESP-200モジュール搭載のASR1006またはASR1013)用のバージョンXE3.8(15.3(1)で)で
のサポートは、他のASR1000プラットフォームでは利用できません。

他の NGE 機能のサポート

NGE の GETVPN 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。

関連情報

- 次世代暗号化
- テクニカル サポートとドキュメント – Cisco Systems