

IOS und IOS-XE NGE (Verschlüsselung der nächsten Generation) unterstützen technischen Hinweis zu Produkten

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[NGE-Algorithmen](#)

[NGE-Unterstützung auf Cisco IOS- und Cisco IOS-XE-Plattformen](#)

[Unterstützung weiterer NGE-Funktionen](#)

[GETVPN-Unterstützung für NGE](#)

Einführung

Dieses Dokument beschreibt die Unterstützung von NGE (Next Generation Encryption) auf Cisco IOS®- und Cisco IOS-XE-Plattformen.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco IOS, mehrere Versionen, wie in der Tabelle angegeben
- Cisco IOS-XE, mehrere Versionen wie in der Tabelle angegeben
- Mehrere Cisco Plattformen, wie in der Tabelle angegeben

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

NGE-Algorithmen

Die Algorithmen, die NGE bilden, sind das Ergebnis von mehr als 30 Jahren globalen Fortschritts und Entwicklung in der Kryptografie. Jede Komponente von NGE hat ihre eigene Geschichte, die

die vielfältige Geschichte der NGE-Algorithmen und ihre langjährige akademische und kommunale Überprüfung darstellt. NGE umfasst global erstellte, global überprüfte und öffentlich verfügbare Algorithmen.

NGE-Algorithmen sind in Internet Engineering Task Force (IETF), IEEE und andere internationale Standards integriert. Daher wurden NGE-Algorithmen auf die neuesten und hochsicheren Protokolle angewendet, die Benutzerdaten schützen, z. B. Internet Key Exchange Version 2 (IKEv2).

Zu den Verschlüsselungsalgorithmen gehören:

- Symmetrische Verschlüsselung - Advanced Encryption Standard (AES) mit 128 Bit oder 256 Bit in GCM (Galois/Counter-Modus)
- Hash - Secure Hash Algorithms (SHA)-2 (SHA-256, SHA-384 und SHA-512)
- Digitale Signaturen - Elliptic Curve Digital Signature Algorithm (ECDSA)
- Hauptvertrag - Elliptic Curve Diffie-Hellman (ECDH)

NGE-Unterstützung auf Cisco IOS- und Cisco IOS-XE-Plattformen

In dieser Tabelle ist die NGE-Unterstützung auf IOS- und Cisco IOS-XE-basierten Plattformen zusammengefasst.

Plattformen	Typ des Krypto-Moduls	Unterstützt durch NGE	Erste Version von Cisco IOS/IOS-XE zur Unterstützung von NGE
Alle Plattformen, auf denen Cisco IOS Classic	Cisco IOS Software-Verschlüsselungs-Engine	Ja	15,1(2)T
7200	VAM/VAM2/VSA	Nein	K/A
ISR G1	Alle	Nein	K/A
ISR G2 2951, 3925, 3945	An Bord ¹	Ja	15,1(3)T
ISR G2 (ohne 3925E/3945E)	VPN-ISM ¹	Ja	15,2(1)T1
ISR G2 1900, 2901, 2911, 2921, 3925E, 3945E	An Bord ¹	Ja	15,2(4)M
ISR G2 CISCO87x	Software/Hardware	Nein	K/A
ISR G2 CISCO86x/C86x	Software ²	Ja	15,1(2)T
ISR G2 C812/C819	Software/Hardware	Ja	Tag 1
ISR G2 CISCO88x/CISCO89x	Software/Hardware ³	Ja	15,1(2)T
ISR G2 C88x	Software/Hardware ⁴	Ja	Tag 1
6500/7600	VPN-SPA	Nein	K/A
ASR 1000	Integriert	Ja	Hinweis ⁵
ASR 1001-X, ASR 1002-X, ASR 1006-X, ASR 1009-X	Integriert	Ja	Cisco IOX-XE 3.12 (15.4(2)S)
ASR 1001-HX, ASR 1002-HX	Optionales Kryptomodul	Ja	Denali-16.3.1
ISR 4451-X	Integriert	Ja	Cisco IOS-XE 3.9 (15.3(2)S)

