

# Unterstützung von Cisco IOS und IOS-XE Verschlüsselung der nächsten Generation

## 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](#)

[Zugehörige Informationen](#)

## Einführung

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

## Voraussetzungen

### Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

### Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- 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 beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen 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	Erste Version	
		Unterstützt von Cisco durch NGE	IOS/IOS-XE zur Unterstützung von NGE
Alle Plattformen mit Cisco IOS Classic 7200	Cisco IOS Software-Verschlüsselungs-Engine VAM/VAM2/VSA	Ja	15,1(2)T
ISR G1	Alle	Nein	–
ISR G2 2951, 3925, 3945	An Bord <sup>1</sup>	Ja	15,1(3)T
ISR G2 (ohne 3925E/3945E)	VPN-ISM <sup>1</sup>	Ja	15,2(1)T1
ISR G2 1900, 2901, 2911, 2921, 3925E, 3945E	An Bord <sup>1</sup>	Ja	15,2(4)M
ISR G2 CISCO87x	Software/Hardware	Nein	–
ISR G2 CISCO86x/C86x	Software <sup>2</sup>	Ja	15,1(2)T
ISR G2 C812/C819	Software/Hardware	Ja	Tag 1
ISR G2 CISCO88x/CISCO89x	Software/Hardware <sup>3</sup>	Ja	15,1(2)T
ISR G2 C88x	Software/Hardware <sup>4</sup>	Ja	Tag 1
6500/7600	VPN-SPA	Nein	–
ASR 1000	Onboarding	Ja	Hinweis <sup>5</sup>
ASR 1001-X, ASR 1002-X, ASR 1006-X, ASR 1009-X	Onboarding	Ja	Cisco IOX-XE 3.12 (15.4(2)S)
ASR 1001-HX, ASR	Optionales Kryptomodul	Ja	Denali-16.3.1



# Zugehörige Informationen

- [Verschlüsselung der nächsten Generation](#)
- [Technischer Support und Dokumentation für Cisco Systeme](#)