# Contenido



# Introducción

Este documento describe el soporte del cifrado de la última generación (NGE) en el ® del Cisco IOS y las Plataformas IOS-XE.

# Prerrequisitos

## Requisitos

No hay requisitos específicos para este documento.

## Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco IOS, versiones múltiples como se apunta en la tabla
- Cisco IOS XE, versiones múltiples como se apunta en la tabla
- Plataformas de Cisco múltiples como se apunta en la tabla

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

# Algoritmos NGE

Los algoritmos que componen NGE son el resultado de más de 30 años de avances globales y evolución en la criptografía. Cada componente de NGE tiene su propio historial, que representa el historial diverso de los algoritmos NGE y de su prolongado estudio del academic y de la

comunidad. NGE comprende global creado, global revisado, y público - los algoritmos disponibles.

Los algoritmos NGE son integrados en la Fuerza de tareas de ingeniería en Internet (IETF) (IETF), IEEE, y otras Normas internacionales. Como consecuencia, los algoritmos NGE se han aplicado a los protocolos más recientes y alto-más seguros que protegen los datos del usuario, tales como intercambio de claves de Internet versión 2 (IKEv2).

Los tipos de algoritmos criptográficos incluyen:

- Encripción simétrica -128-bit o Advanced Encryption Standard (AES) del 256-bit en GCM (Galois/modo contrario)
- Hash - Algoritmos de troceo seguro (SHA)-2 (SHA-256, SHA-384, y SHA-512)
- Firmas digitales - Digital Signature Algorithm elíptico de la curva (ECDSA)
- Acuerdo dominante - Curva elíptica Diffie Hellman (ECDH)

## Soporte NGE en las Plataformas IOS e IOS-XE

Esta tabla resume el soporte NGE en las Plataformas basadas en IOS y IOS-XE-basadas de Cisco.

| Plataformas | Tipo del motor de criptografía | Soportado por NGE | Primera versión de C IOS/IOS-XE para sop NGE |
|---|---|---|---|
| Todas las Plataformas que funcionan con la obra clásica IOS | Motor de criptografía del software IOS | Sí | 15.1(2)T |
| 7200 | VAM/VAM2/VSA | No | N/A |
| ISR G1 | Todos | No | N/A |
| ISR G2 2951, 3925, 3945 | A bordo de | Sí | 15.1(3)T |
| ISR G2 (excluye 3925E/3945E) | VPN-ISM1 | Sí | 15.2(1)T1 |
| ISR G2 1900, 2901, 2911, 2921, 2951, 3925, 3945, 3925E, 3945E | A bordo de | Sí | el 15.2(4)M |
| ISR G2 CISCO87x | Software/soporte físico | No | N/A |
| ISR G2 CISCO86x/C86x | Software | Sí | 15.1(2)T |
| ISR G2 C812/C819 | Software/soporte físico | Sí | Día 1 |
| ISR G2 CISCO88x/CISCO89x | Software/soporte físico | Sí | 15.1(2)T |
| ISR G2 C88x | Software/soporte físico | Sí | Día 1 |
| 6500/7600 | VPN-SPA | No | N/A |
| ASR 1000 | A bordo | Sí | Nota |
| ISR 4451-X | A bordo | Sí | IOS-XE 3.9 (15.3(2)S |
| ISR 4321, 4331, 4351, 4431 | A bordo | Sí | IOS-XE 3.13 (15.4(3) |
| CSR 1000v | Software | Sí | IOS-XE 3.12 (15.4(2) |

Nota 1: En la plataforma ISR G2, si se configura ECDH/ECDSA, estas operaciones criptográficas serán funcionadas con en el software con independencia del motor criptográfico.

**Nota 2:** El ISR G2 CISCO86x/C86x no tiene soporte NGE en el motor de criptografía del hardware.
**Nota 3:** El ISR G2 CISCO88x/CISCO89x tiene soporte del hardware para el SHA-256 SOLAMENTE con versión 15.2(4)M3 o posterior.
**Nota 4:** Estos C88x SKUs no tienen ningún soporte del hardware para NGE: C881SRST-K9, C881SRSTW-GN-A-K9, C881SRSTW-GN-E-K9, C881-CUBE-K9, C881-V-K9, C881G-U-K9, C881G-S-K9, C881G-V-K9, C881G-B-K9, C881G+7-K9, C881G+7-A-K9, C886SRST-K9, C886SRSTW-GN-E-K9, C886VA-CUBE-K9, C886VAG+7-K9, C887SRST-K9, C887SRSTW-GN-A-K9, C887SRSTW-GN-E-K9, C887VSRST-K9, C887VSRSTW-GNA-K9, C887VSRSTW-GNE-K9, C887VA-V-K9, C887VA-V-W-E-K9, C887VA-CUBE-K9, C887VAG-S-K9, C887VAG+7-K9, C887VAMG+7-K9, C888SRSTW-GN-A-K9, C888SRSTW-GN-E-K9, C888SRST-K9, C888ESRST-K9, C888ESRSTW-GNA-K9, C888ESRSTW-GNE-K9, C888-CUBE-K9, C888E-CUBE-K9, y C888EG+7-K9.
**Nota 5**: El soporte para el avión del control NGE (ECDH y ECDSA) se ha introducido con la versión XE3.8 (15.2(4)S). El soporte plano SHA-2 del control está para IKEv2 solamente, con el soporte IKEv1 agregado en la versión XE3.10 (15.3(3)S). El soporte de Dataplane se agrega en la versión XE3.8 (15.3(1)S) para Octeon basó las Plataformas solamente (ASR1001-X, ASR1002-X, ESP-100, y ESP-200); el soporte del dataplane está disponible para otras Plataformas ASR.

# El otro soporte de característica NGE

## Soporte GETVPN para NGE

- El soporte del Cisco IOS Software en las Plataformas ISR G2 comienza con la versión 15.2(4)M.
- El soporte ASR comienza con el Software Cisco IOS XE, la versión 3.10S (15.3(3)S).