# Suporte à criptografia de próxima geração do Cisco IOS e do IOS-XE

## Contents



## Introduction

Este documento descreve o suporte à criptografia de próxima geração (NGE) nas plataformas Cisco IOS® e Cisco IOS-XE.

## Prerequisites

### Requirements

Não existem requisitos específicos para este documento.

### Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco IOS, várias versões conforme observado na tabela
- Cisco IOS-XE, várias versões conforme observado na tabela
- Várias plataformas Cisco conforme observado na tabela

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

## Algoritmos de NGE

Os algoritmos que compõem a NGE resultam de mais de 30 anos de avanços globais e evolução na criptografia. Cada componente da NGE tem sua própria história, que retrata a história diversa dos algoritmos da NGE e sua antiga revisão acadêmica e comunitária. O NGE inclui algoritmos criados globalmente, revisados globalmente e disponíveis publicamente.

Os algoritmos NGE são integrados à Internet Engineering Task Force (IETF), IEEE e a outros padrões internacionais. Como resultado, os algoritmos NGE foram aplicados aos protocolos mais recentes e altamente seguros que protegem os dados do usuário, como o Internet Key Exchange Version 2 (IKEv2).

Os tipos de algoritmos criptográficos incluem:

- Criptografia simétrica - AES (Advanced Encryption Standard) de 128 bits ou 256 bits no GCM (modo Galois/Counter)
- Hash - Algoritmos de hash seguro (SHA)-2 (SHA-256, SHA-384 e SHA-512)
- Assinaturas digitais - ECDSA (Elliptic Curve Digital Signature Algorithm)
- Acordo-chave - Curva elíptica Diffie-Hellman (ECDH)

# Suporte de NGE em plataformas Cisco IOS e Cisco IOS-XE

Esta tabela resume o suporte de NGE em plataformas baseadas no Cisco IOS e no Cisco IOS-XE.

| Plataformas | Tipo de mecanismo de criptografia | Compatível com NGE | Primeira versão do C IOS/IOS-XE para ofe suporte ao NGE |
|---|---|---|---|
| Todas as plataformas que executam o Cisco IOS clássico | Mecanismo de criptografia do software Cisco IOS | Yes | 15.1(2)T |
| 7200 | VAM/VAM2/VSA | No | N/A |
| ISR G1 | Todos | No | N/A |
| ISR G2 2951, 3925, 3945 | Integrado[1] | Yes | 15.1(3)T |
| ISR G2 (exclui 3925E/3945E) | VPN-ISM[1] | Yes | 15.2(1)T1 |
| ISR G2 1900, 2901, 2911, 2921, 3925E, 3945E | Integrado[1] | Yes | 15,2(4)M |
| ISR G2 CISCO87x | Software/hardware | No | N/A |
| ISR G2 CISCO86x/C86x | Software[2] | Yes | 15.1(2)T |
| ISR G2 C812/C819 | Software/hardware | Yes | Dia 1 |
| ISR G2 CISCO88x/CISCO89x | Software/hardware[3] | Yes | 15.1(2)T |
| ISR G2 C88x | Software/hardware[4] | Yes | Dia 1 |
| 6500/7600 | VPN-SPA | No | N/A |
| ASR 1000 | Onboard | Yes | Nota [5] |
| ASR 1001-X, ASR 1002-X, ASR 1006-X, ASR 1009-X | Onboard | Yes | Cisco IOX-XE 3.12 (15.4(2)S) |
| ASR 1001-HX, ASR1002-HX | Módulo Crypto opcional | Yes | Denali-16.3.1 |
| ISR 4451-X | Onboard | Yes | Cisco IOS-XE 3.9 (15.3(2)S) |
| ISR 4321, 4331, 4351, 4431 | Onboard | Yes | Cisco IOS-XE 3.13 (15.4(3)S) |
| ISR 42xx | Onboard | Yes | Cisco IOS-XE Everes 16.4.1 |
| CSR 1000v | Software | Yes | Cisco IOS-XE 3.12 (15.4(2)S) |

| | | | |
|---|---|---|---|
| ISR 1100 | Onboard | Yes | Cisco IOS-XE Everes 16.6.2 |
| Plataformas de borda Catalyst 8200, 8300, 8500 | Onboard | Yes | Dia 1 |
| Catalyst 8000v | Software | Yes | Dia 1 |

**Nota 1:** Na plataforma ISR G2, se ECDH/ECDSA estiver configurado, essas operações criptográficas ser executadas no software independentemente do mecanismo criptográfico. Os algoritmos de criptografia A GCM-128 e AES-GCM-256 têm suporte para a proteção do plano de controle IKEv2 desde a versão 15.4
**Nota 2:** ISR G2 CISCO86x/C86x não tem suporte NGE no mecanismo de criptografia de hardware.
**Nota 3:** ISR G2 CISCO88x/CISCO89x tem suporte de hardware para SHA-256 SOMENTE com a versão 15.2(4)M3 ou posterior.
**Nota 4:** Esses SKUs C88x não têm suporte de hardware para NGE: C881SRST-K9, C881SRSTW-GN-A- C881SRSTW-GN-E-K9, C881-CUBE-K9, C881-V-K9, C881G-U-K9, C881G-S K9, C881G-V-K9, C881G- C881G+7-K9, C881G+7-A-K9, C886SRST-K9, C886SRSTW-GN-E-K9, C86 VA-CUBE-K9, C886VAG+7- C887SRST-K9, C887SRSTW-GN-A-K9, C887SRSTW-GN-E-K9, C887VSRST-K9, C887VSRSTW-GNA - C887VSRSTW-GNE-K9, C887VA-V-K9, C887VA-V-W-E-K9, C887VA-CUBE-K9, C887VAG-S-K9, C887VAG+7-K9, 887VAMG+7-K9, C888SRSTW-GN-A-K9, C888SRSTW-GN-E-K9, C888SRST-K9, C888ESRST-K9, C888ESRSTW-GNA-K9, C88 88ESRSTW-GNE-K9, C888-CUBE-K9, C888E-CUBE-K9 C888EG+7-K9.
**Nota 5:** O suporte para o plano de controle NGE (ECDH e ECDSA) foi introduzido com a versão XE3.7 (15.2(4)S). O suporte do plano de controle inicial SHA-2 era para IKEv2 apenas, com suporte para IKEv1 adicionado na versão XE3.10 (15.3(3)S). Os algoritmos de criptografia AES-GCM-128 e AES-GCM-256 t suporte para a proteção do plano de controle IKEv2 desde a versão XE3.12 (15.4(2)S) e 15.4(2)T. O sup de plano de dados NGE foi adicionado na versão XE3.8 (15.3(1)S) apenas para plataformas baseadas e Octeon (ASR1006 ou ASR1013 com um módulo ESP-100 ou ESP-200); o suporte a dataplane não está disponível para outras plataformas ASR1000.

# Outro suporte a recursos do NGE

## Suporte a GETVPN para NGE

- O suporte ao software Cisco IOS em plataformas ISR G2 começa com a versão 15.2(4)M.
- O suporte ASR começa com o software Cisco IOS-XE, versão 3.10S (15.3(3)S).

# Informações Relacionadas

- Criptografia de próxima geração
- Suporte Técnico e Documentação - Cisco Systems