Soporte de Cifrado de Cisco IOS y IOS-XE Next Generation

Contenido

Introducción

Este documento describe la compatibilidad con el cifrado Next Generation (NGE) en las plataformas Cisco IOS® y Cisco IOS-XE.

Prerequisites

Requirements

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, varias versiones como se indica en la tabla
- Cisco IOS-XE, varias versiones como se indica en la tabla
- Varias plataformas de Cisco como se indica en la tabla

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 NGE

Los algoritmos que conforman el NGE son el resultado de más de 30 años de avances globales y evolución en criptografía. Cada componente de NGE tiene su propia historia, que describe la diversidad de la historia de los algoritmos de NGE y su larga revisión académica y comunitaria. NGE comprende algoritmos creados a nivel mundial, revisados a nivel mundial y disponibles

públicamente.

Los algoritmos de NGE se integran en el Grupo de trabajo de ingeniería de Internet (IETF), el IEEE y otros estándares internacionales. Como resultado, los algoritmos NGE se han aplicado a los protocolos más recientes y altamente seguros que protegen los datos de los usuarios, como el intercambio de claves de Internet versión 2 (IKEv2).

Los tipos de algoritmos criptográficos incluyen:

- Cifrado simétrico: estándar de cifrado avanzado (AES) de 128 bits o 256 bits en GCM (modo Galois/Counter)
- Hash - Algoritmos de hash seguros (SHA)-2 (SHA-256, SHA-384 y SHA-512)
- Firmas digitales: algoritmo de firma digital de curva elíptica (ECDSA)
- Acuerdo clave - Diffie-Hellman de curva elíptica (ECDH)

Compatibilidad con NGE en plataformas Cisco IOS y Cisco IOS-XE

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

Plataformas	Tipo de motor criptográfico	Compatible con NGE	Primera versión de C IOS/IOS-XE para adr NGE
Todas las plataformas que ejecutan Cisco IOS classic	motor criptográfico del 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 y 3945	Incorporado[1]	Yes	15.1(3)T
ISR G2 (no incluye 3925E/3945E)	VPN-ISM[1]	Yes	15.2(1)T1
ISR G2 1900, 2901, 2911, 2921, 3925E, 3945E	Incorporado[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	Día 1
ISR G2 CISCO88x/CISCO89x	Software / Hardware [3]	Yes	15.1(2)T
ISR G2 C88x	Software / Hardware [4]	Yes	Día 1
6500/7600	VPN-SPA	No	N/A
ASR 1000	Integración de dispositivos	Yes	Nota [5]
ASR 1001-X, ASR 1002-X, ASR 1006-X y ASR 1009-X	Integración de dispositivos	Yes	Cisco IOX-XE 3.12 (15.4(2)S)
ASR 1001-HX, ASR 1002-HX	Módulo Crypto opcional	Yes	Denali-16.3.1
ISR 4451-X	Integración de dispositivos	Yes	Cisco IOS-XE 3.9 (15.3(2)S)
ISR 4321, 4331, 4351 y 4431	Integración de dispositivos	Yes	Cisco IOS-XE 3.13 (15.4(3)S)

ISR 42xx	Integración de dispositivos	Yes	Cisco IOS-XE Everes 16.4.1
CSR 1000v	Software	Yes	Cisco IOS-XE 3.12 (15.4(2)S)
ISR 1100	Integración de dispositivos	Yes	Cisco IOS-XE Everes 16.6.2
Plataformas de extremo Catalyst 8200, 8300 y 8500	Integración de dispositivos	Yes	Día 1
Catalyst 8000v	Software	Yes	Día 1

Nota 1: En la plataforma ISR G2, si se configura ECDH/ECDSA, estas operaciones criptográficas se ejecutarán en software independientemente del motor criptográfico. Los algoritmos de cifrado AES-GCM- AES-GCM-256 son compatibles con la protección del plano de control IKEv2 desde la versión 15.4(2)T.
Nota 2: ISR G2 CISCO86x/C86x no admite NGE en el motor de criptografía de hardware.
Nota 3: ISR G2 CISCO88x/CISCO89x SÓLO admite hardware para SHA-256 con la versión 15.2(4)M3 o posterior.
Nota 4: Estas SKU C88x no admiten hardware para NGE: C881SRST-K9, C881SRSTW-GN-A-K9, C881SRSTW-GN-E-K9, C881-CUBE-K9, C881-V-K9, C881G-U-K9, C888881G -S-K9, C881G-V-K9, C88 B-K9, C881G+7-K9, C881G+7-A-K9, C886SRST-K9, C886SRSTW-GN-E-K9, C888888888886 86VA-CU K9, C886VAG+7-K9, C887SRST-K9, C887SRSTW-GN-A-K9, C887SRSTW-GN-E-K9, C887VSRST-K9, C8887VSR7VST STW-GNA-K9, C887VSRSTW-GNE-K9, C887VA-V-K9, C887VA-V-W-E-K9, C887VA-C K9, C887VAG-S-K9, C887VAG+7 - K9, C887VAMG+7-K9, C888SRSTW-GN-A-K9, C888SRSTW-GN-E- C888SRST-K9, C888ESRST-K9, C888ESRSTW-GNA K9, C888ESRSTW-GNE-K9, C888-CUBE-K9, C8 CUBE-K9 y C888EG+7-K9.
Nota 5: La compatibilidad con el plano de control NGE (ECDH y ECDSA) se ha introducido con la versión XE3.7 (15.2(4)S). El soporte inicial del plano de control SHA-2 fue solo para IKEv2, con soporte IKEv1 agregado en la versión XE3.10 (15.3(3)S). Los algoritmos de cifrado AES-GCM-128 y AES-GCM-256 se soportado para la protección del plano de control IKEv2 desde la versión XE3.12 (15.4(2)S) y 15.4(2)T. E soporte del plano de datos NGE se agregó en la versión XE3.8 (15.3(1)S) para las plataformas basadas Octeon solamente (ASR1006 o ASR1013 con un módulo ESP-100 o ESP-200); el soporte del plano de d no está disponible para otras plataformas ASR1000.

Compatibilidad con otras funciones de NGE

Soporte de GETVPN para NGE

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

Información Relacionada

- Criptografía de última generación
- Soporte Técnico y Documentación - Cisco Systems