Cisco IOS and IOS-XE Next Generation Encryption Support

Contents

Introduction

This document describes Next Generation Encryption (NGE) support on Cisco IOS® and Cisco IOS-XE platforms.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco IOS, multiple versions as noted in the table
- Cisco IOS-XE, multiple versions as noted in the table
- Multiple Cisco platforms as noted in the table

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.

NGE Algorithms

The algorithms that make up NGE are the result of more than 30 years of global advances and evolution in cryptography. Each component of NGE has its own history, which depicts the diverse history of the NGE algorithms and their longstanding academic and community review. NGE comprises globally created, globally reviewed, and publicly available algorithms.

NGE algorithms are integrated into Internet Engineering Task Force (IETF), IEEE, and other international standards. As a result, NGE algorithms have been applied to the most recent and highly-secure protocols that protect user data, such as Internet Key Exchange Version 2 (IKEv2).

Types of cryptographic algorithms include:

- Symmetric encryption -128-bit or 256-bit Advanced Encryption Standard (AES) in GCM (Galois/Counter mode)
- Hash - Secure Hash Algorithms (SHA)-2 (SHA-256, SHA-384, and SHA-512)
- Digital signatures -Elliptic Curve Digital Signature Algorithm (ECDSA)
- Key agreement - Elliptic Curve Diffie-Hellman (ECDH)

NGE Support on Cisco IOS and Cisco IOS-XE Platforms

This table summarizes NGE support on Cisco IOS-based and Cisco IOS-XE-based platforms.

Platforms	**Crypto Engine Type**	**Supported by NGE**	**First Version of Cisc IOS/IOS-XE to Supp NGE**
All platforms that run Cisco IOS classic	Cisco IOS software crypto engine	Yes	15.1(2)T
7200	VAM/VAM2/VSA	No	N/A
ISR G1	All	No	N/A
ISR G2 2951, 3925, 3945	Onboard[1]	Yes	15.1(3)T
ISR G2 (excludes 3925E/3945E)	VPN-ISM[1]	Yes	15.2(1)T1
ISR G2 1900, 2901, 2911, 2921, 3925E, 3945E	Onboard[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	Day 1
ISR G2 CISCO88x/CISCO89x	Software / Hardware[3]	Yes	15.1(2)T
ISR G2 C88x	Software / Hardware[4]	Yes	Day 1
6500/7600	VPN-SPA	No	N/A
ASR 1000	Onboard	Yes	Note[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	Optional Crypto module	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
Catalyst 8200, 8300, 8500	Onboard	Yes	Day 1

Edge Platforms			
Catalyst 8000v	Software	Yes	Day 1

Note 1: On the ISR G2 platform, if ECDH/ECDSA is configured, these cryptographic operations will be ru software irrespective of the cryptographic engine. AES-GCM-128 and AES-GCM-256 encryption algorith have been supported for IKEv2 control plane protection since Version 15.4(2)T.

Note 2: ISR G2 CISCO86x/C86x does not have NGE support in the hardware crypto engine.

Note 3: ISR G2 CISCO88x/CISCO89x has hardware support for SHA-256 ONLY with Version 15.2(4)M3 later.

Note 4: These C88x SKUs have no hardware support for 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- C881G+7-K9, C881G+7-A-K9, C886SRST-K9, C886SRSTW-GN-E-K9, C886VA-CUBE-K9, C886VAG+ 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, 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, C888EG+7-K9.

Note 5: Support for the NGE control plane (ECDH and ECDSA) has been introduced with Version XE3.7 (15.2(4)S). Initial control plane SHA-2 support was for IKEv2 only, with IKEv1 support added in Version X (15.3(3)S). AES-GCM-128 and AES-GCM-256 encryption algorithms have been supported for IKEv2 con plane protection since Version XE3.12 (15.4(2)S) and 15.4(2)T. NGE dataplane support was added in Ve XE3.8 (15.3(1)S) for Octeon based platforms only (ASR1006 or ASR1013 with an ESP-100 or ESP-200 module); dataplane support is not available for other ASR1000 platforms.

Other NGE Feature Support

GETVPN Support for NGE

- Cisco IOS software support on ISR G2 platforms starts with Version 15.2(4)M.
- ASR support starts with Cisco IOS-XE software, Version 3.10S (15.3(3)S).

Related Information

- **Next Generation Cryptography**
- **Technical Support & Documentation - Cisco Systems**