IOS和IOS-XE NGE (下一代加密)支持产品技术说明

目录

简介

本文描述下一代在Cisco IOS和Cisco IOS XE平台的加密(NGE)支持。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco IOS，在表中注明的多个版本
- Cisco IOS XE，在表中注明的多个版本
- 在表中注明的多Cisco平台

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

NGE算法

组成NGE的算法是超过全局预付款的30年在加密算法的结果和演变。NGE每个组件有其自己的历史记录，表示NGE算法和他们长年的院和社区复核的多样化的历史记录。NGE包括全局已创建，全局查看的和公共可用的算法。

NGE算法集成到互联网工程任务组(IETF)、IEEE和其他国际标准。结果， NGE算法应用对保护用户数据的最最近的和最高安全的协议，例如互联网密钥交换版本2 (IKEv2)。

加密算法的类型包括：

- 对称加密-128-bit或在GCM (Galois的256-bit高级加密标准(AES)/计数器模式)
- 哈希-安全散列算法(SHA)-2 (SHA-256、SHA-384和SHA-512)
- 数字签名-椭圆曲线数字签名算法(ECDSA)
- 关键协议-椭圆曲线Diffie-Hellman (ECDH)

在Cisco IOS和Cisco IOS XE平台的NGE支持

此表汇总在基于Cisco IOS的和Cisco基于IOS XE的平台的NGE支持。

平台	加密引擎类型	支持由NGE	支持NGE的Cisco IOS/IOS-XE第一个版本
运行的所有平台 经典的Cisco IOS	Cisco IOS软件加密引擎	是	15.1(2)T
7200	VAM/VAM2/VSA	无	不适用
ISR G1	所有	无	不适用
ISR G2 2951， 3925， 3945	[1]	是	15.1(3)T
ISR G2 (排除3925E/3945E)	VPN-ISM1	是	15.2(1)T1
ISR G2 1900， 2901， 2911， 2921， 3925E， 3945E	[1]	是	15.2(4)M
ISR G2 CISCO87x	软件/硬件	无	不适用
ISR G2 CISCO86x/C86x	Software[2]	是	15.1(2)T
ISR G2 C812/C819	软件/硬件	是	第 1 天
ISR G2 CISCO88x/CISCO89x	软件/硬件[3]	是	15.1(2)T
ISR G2 C88x	软件/硬件[4]	是	第 1 天
6500/7600	VPN-SPA	无	不适用
ASR 1000	内置	是	注释5
ASR 1001-X， ASR 1002-X， ASR 1006-X， ASR 1009-X	内置	是	Cisco IOX-XE 3.12 (15.4(2)S)
ASR 1001-HX， ASR1002-HX	可选crypto模块	是	Denali-16.3.1
ISR 4451-X	内置	是	Cisco IOS XE 3.9 (15.3(2)S)
ISR 4321， 4331， 4351， 4431	内置	是	Cisco IOS XE 3.13 (15.4(3)S)
ISR 42xx	内置	是	Cisco IOS XE珠穆琅玛16.4.1
CSR 1000v	软件	是	Cisco IOS XE 3.12 (15.4(2)S)
ISR 1100	内置	是	Cisco IOS XE珠穆琅玛16.6.2

注释 1：在ISR G2平台上，如果ECDH/ECDSA配置，这些密码行动在软件方面将参加不考虑密码引擎。AES-GCM-128和AES-GCM-256加密算法为IKEv2控制层面保护支持从版本15.4(2)T。

注释 2：ISR G2 CISCO86x/C86x在硬件加密引擎里没有NGE支持。

注释 3：ISR G2 CISCO88x/CISCO89x有仅SHA-256的硬件支持与版本15.2(4)M3或以上。

注释4 ：这些C88x SKU没有NGE的硬件支持：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和C888EG+7-K9。

注释5 ：NGE控制层面的支持(ECDH和ECDSA)介绍与版本XE3.7 (15.2(4)S)。最初的控制层面SHA-2支持

为仅IKEv2，当IKEv1支持被添加在版本XE3.10 (15.3(3)S)。AES-GCM-128和AES-GCM-256加密算法为IKEv2控制层面保护支持从版本XE3.12 (15.4(2)S)和15.4(2)T。NGE dataplane支持在Octeon的版本XE3.8 (15.3(1)S)被添加了根据仅平台(ASR1006或ASR1013用ESP-100或ESP-200模块);dataplane支持为其他ASR1000平台不是可用的。

其他NGE功能支持

NGE的GETVPN支持

- 在ISR G2平台的Cisco IOS软件软件支持从版本15.2(4)M开始。
- ASR支持从Cisco IOS XE软件开始，版本3.10S (15.3(3)S)。