Cisco IOS和IOS-XE下一代加密支持

目录

简介

本文档介绍Cisco IOS®和Cisco IOS-XE平台上的下一代加密(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，多个版本（如表所示）
- Cisco IOS-XE，多个版本，如表中所述
- 如表中所述，多个思科平台

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

构成NGE的算法是30多年来全球密码学进步和发展的结果。NGE的每个组成部分都有自己的历史，描述了NGE算法的多样化历史及其长期的学术和社区回顾。NGE包括全球创建、全球审查和公开可用的算法。

NGE算法已集成到互联网工程任务组(IETF)、IEEE和其他国际标准中。因此，NGE算法已应用于保护用户数据的最新且高度安全的协议，如Internet密钥交换版本2(IKEv2)。

加密算法的类型包括：

- 对称加密 — GCM（Galois/Counter模式）中的128位或256位高级加密标准(AES)
- 散列 — 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)
- 密钥协议 — 椭圆曲线Diffie-Hellman(ECDH)

Cisco IOS和Cisco IOS-XE平台上的NGE支持

下表汇总了基于Cisco IOS和基于Cisco IOS XE的平台上的NGE支持。

平台	加密引擎类型	NGE支持	支持NGE的Cisco IOS/IOS-XE的第一版
运行Cisco IOS经典版的所有平台	Cisco IOS软件加密引擎	Yes	15.1(2)T
7200	VAM/VAM2/VSA	无	不适用
ISR G1	all	无	不适用
ISR G2 2951、3925、3945	板载[1]	Yes	15.1(3)T
ISR G2（不包括3925E/3945E）	VPN-ISM[1]	Yes	15.2(1)T1
ISR G2 1900、2901、2911、2921、3925E、3945E	板载[1]	Yes	15.2(4)M
ISR G2 CISCO87x	软件/硬件	无	不适用
ISR G2 CISCO86x/C86x	软件[2]	Yes	15.1(2)T
ISR G2 C812/C819	软件/硬件	Yes	第 1 天
ISR G2 CISCO88x/CISCO89x	软件/硬件[3]	Yes	15.1(2)T
ISR G2 C88x	软件/硬件[4]	Yes	第 1 天
6500/7600	VPN-SPA	无	不适用
ASR 1000	激活	Yes	附注[5]
ASR 1001-X、ASR 1002-X、ASR 1006-X、ASR 1009-X	激活	Yes	思科IOX-XE 3.12(15.4(2)S)
ASR 1001-HX、ASR1002-HX	可选加密模块	Yes	德纳利–16.3.1
ISR 4451-X	激活	Yes	思科IOS-XE 3.9(15.3(2)S)
ISR 4321、4331、4351、4431	激活	Yes	思科IOS-XE 3.13(15.4(3)S)
ISR 42xx	激活	Yes	思科IOS-XE Everest 16.4.1
CSR 1000v	软件	Yes	思科IOS-XE 3.12(15.4(2)S)
ISR 1100	激活	Yes	思科IOS-XE Everest 16.6.2
Catalyst 8200、8300、8500边缘平台	激活	Yes	第 1 天
Catalyst 8000v	软件	Yes	第 1 天

注释 1：在ISR G2平台上，如果配置了ECDH/ECDSA，则这些加密操作将在软件中运行，而与加密引擎无关。自版本15.4(2)T起，AES-GCM-128和AES-GCM-256加密算法就受IKEv2控制平面保护支持。
注释 2：ISR G2 CISCO86x/C86x在硬件加密引擎中不支持NGE。
注释 3：ISR G2 CISCO88x/CISCO89x仅对SHA-256提供硬件支持，支持15.2(4)M3或更高版本。
注释 4：这些C88x SKU不支持NGE的硬件：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、C887SRGst-K9、C887SRSTW-GN-A-K9、C887SRSTW-GN-E-K9、C887VSRST-K9、C887VSRSTW-GNA-K9、C887VSRSTW-GNE-K9、C887VA-V-K9、C887VA-V-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-GNA-K9、C888-CUBE-K9、C88E-Kcube-K9和C888EG+7-K9。
注释 5：版本XE3.7(15.2(4)S)引入了对NGE控制平面（ECDH和ECDSA）的支持。 初始控制平面SHA-2支持仅适用于IKEv2，在XE3.10(15.3(3)S)版本中添加了IKEv1支持。自XE3.12(15.4(2)S)和15.4(2)T版起，AES-GCM-128和AES-GCM-256加密算法就受IKEv2控制平面保护支持。NGE数据平面支持已添加到版本XE3.8(15.3(1)S)中，仅适用于基于Octeon的平台(带ESP-100或ESP-200模块的ASR1006或ASR1013);数据平面支持不适用于其他ASR1000平台。

其他NGE功能支持

NGE的GETVPN支持

- ISR G2平台上的Cisco IOS软件支持以版本15.2(4)M开头。
- ASR支持从Cisco IOS-XE软件版本3.10S(15.3(3)S)开始。

相关信息

- 下一代加密
- 技术支持和文档 - Cisco Systems