Cisco IOS和IOS-XE下一代加密支援

目錄

簡介

本檔案介紹Cisco IOS®和Cisco IOS-XE平台上的下一代加密(NGE)支援。

必要條件

需求

本文件沒有特定需求。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco IOS，表中所示的多個版本
- Cisco IOS-XE，表中所示的多個版本
- 多個思科平台（如表所示）

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

NGE演算法

NGE的演算法是密碼學全球30多年發展和進步的成果。NGE的每個元件都有自己的歷史，描述了NGE演算法的多元歷史及其長期的學術和社群評論。NGE由全球建立、全球稽核和公開可用的演算法組成。

NGE演算法整合到網際網路工程任務組(IETF)、IEEE和其他國際標準中。因此，NGE演算法已應用於保護使用者資料的最新且高度安全的協定，例如網際網路金鑰交換版本2(IKEv2)。

加密演算法的型別包括：

- 對稱加密 — GCM（Galois/Counter模式）中的128位或256位進階加密標準(AES)
- 雜湊 — 安全雜湊演算法(SHA)-2（SHA-256、SHA-384和SHA-512）
- 數位簽章 — 橢圓曲線數位簽章演算法(ECDSA)
- 金鑰協定 — 橢圓曲線Diffie-hellman(ECDH)

Cisco IOS和Cisco IOS-XE平台上的NGE支援

下表總結了基於Cisco IOS和基於Cisco IOS-XE的平台上的NGE支援。

平台	加密引擎型別	受NGE支援	支援NGE的第一版Cisco IOS/IOS-XE
所有運行Cisco IOS classic的平台	Cisco IOS軟體加密引擎	是	15.1(2)公噸
7200	VAM/VAM2/VSA	否	不適用
ISR G1	全部	否	不適用
ISR G2 2951、3925、3945	板載[1]	是	15.1(3)公噸
ISR G2（不包括3925E/3945E）	VPN-ISM[1]	是	15.2(1)T1
ISR G2 1900、2901、2911、2921、3925E、3945E	板載[1]	是	15.2(4)米
ISR G2 CISCO87x	軟體/硬體	否	不適用
ISR G2 CISCO86x/C86x	軟體[2]	是	15.1(2)公噸
ISR G2 C812/C819	軟體/硬體	是	第1天
ISR G2 CISCO88x/CISCO89x	軟體/硬體[3]	是	15.1(2)公噸
ISR G2 C88x	軟體/硬體[4]	是	第1天
6500/7600	VPN-SPA	否	不適用
ASR 1000	入門	是	附註[5]
ASR 1001-X、ASR 1002-X、ASR 1006-X、ASR 1009-X	入門	是	Cisco IOX-XE 3.12(15.4(2)S)
ASR 1001-HX、ASR1002-HX	可選加密模組	是	Denali-16.3.1
ISR 4451-X	入門	是	Cisco IOS-XE 3.9(15.3(2)S)
ISR 4321、4331、4351、4431	入門	是	Cisco IOS-XE 3.13(15.4(3)S)
ISR 42xx	入門	是	Cisco IOS-XE Everest 16.4.1
CSR 1000v	軟體	是	Cisco IOS-XE 3.12(15.4(2)S)
ISR 1100	入門	是	Cisco IOS-XE Everest 16.6.2
Catalyst 8200、8300、8500邊緣平台	入門	是	第1天
Catalyst 8000v	軟體	是	第1天

附註1:在ISR G2平台上，如果配置了ECDH/ECDSA，則這些加密操作將在軟體中運行，與加密引擎無關。自15.4(2)T版起，AES-GCM-128和AES-GCM-256加密演算法已支援IKEv2控制平面保護。
附註2:ISR G2 CISCO86x/C86x在硬體加密引擎中不支援NGE。
附註3:ISR G2 CISCO88x/CISCO89x僅對15.2(4)M3或更高版本的SHA-256提供硬體支援。
附註4:這些C88x SKU沒有適用於NGE的硬體支援：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、C8 1G-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、C8888ESR STW-GNA-K9、C888ESRSTW-GNE-K9、C888-CUBE-K9、C888E-CUBE-K9和C888EG+7-K9。
附註5:XE3.7(15.2(4)S)版引入了對NGE控制平面（ECDH和ECDSA）的支援。 初始控制平面SHA-2支援僅適用於IKEv2，而IKEv1支援在XE3.10(15.3(3)S)版本中新增。自XE3.12(15.4(2)S)和15.4(2)T版本起，AES-GCM-128和AES-GCM-256加密演算法已支援IKEv2控制平面保護。NGE資料平面支援是在XE3.8(15.3(1)S)版中增加的，僅適用於基於八位元的平台(ASR1006或具有ESP-100或ESP-200模組的ASR1013);其他ASR1000平台不支援資料平面。

其他NGE功能支援

適用於NGE的GETVPN支援

- ISR G2平台上的Cisco IOS軟體支援從版本15.2(4)M開始。
- ASR支援從Cisco IOS-XE軟體版本3.10S(15.3(3)S)開始。

相關資訊

- 下一代加密技術
- 技術支援與文件 - Cisco Systems