Cisco IOS 및 IOS-XE 차세대 암호화 지원

목차

[소개](#)
[사전 요구 사항](#)
[요구 사항](#)
[사용되는 구성 요소](#)
[NGE 알고리즘](#)
[Cisco IOS 및 Cisco IOS-XE 플랫폼의 NGE 지원](#)
[기타 NGE 기능 지원](#)
[NGE를 위한 GETVPN 지원](#)
[관련 정보](#)

소개

이 문서에서는 Cisco IOS® 및 Cisco IOS-XE 플랫폼에서 NGE(Next Generation Encryption) 지원에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco IOS, 표에 나와 있는 여러 버전
- Cisco IOS-XE, 표에 나와 있는 여러 버전
- 표에 나와 있는 여러 Cisco 플랫폼

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

NGE 알고리즘

NGE를 구성하는 알고리즘은 암호화에 있어서 30년 이상의 글로벌 발전과 진화의 결과입니다 .NGE의 각 구성 요소에는 NGE 알고리즘의 다양한 역사 및 오랜 학술 및 커뮤니티 검토가 나와 있습니다.NGE는 전역적으로 생성, 전역적으로 검토 및 공개적으로 사용 가능한 알고리즘으로 구성됩니다.

NGE 알고리즘은 IETF(Internet Engineering Task Force), IEEE 및 기타 국제 표준에 통합됩니다.그 결과 NGE 알고리즘은 IKEv2(Internet Key Exchange Version 2)와 같은 사용자 데이터를 보호하는

가장 최신 보안 프로토콜에 적용되었습니다.

암호화 알고리즘 유형은 다음과 같습니다.

- GCM(Galois/카운터 모드)의 대칭 암호화 -128비트 또는 256비트 AES(Advanced Encryption Standard)
- 해시 - SHA(Secure Hash Algorithms)-2(SHA-256, SHA-384 및 SHA-512)
- 디지털 서명 - ECDSA(Elliptic Curve Digital Signature Algorithm)
- 키 계약 - ECDH(Elliptic Curve Diffie-Hellman)

Cisco IOS 및 Cisco IOS-XE 플랫폼의 NGE 지원

이 표에는 Cisco IOS 기반 및 Cisco IOS-XE 기반 플랫폼에 대한 NGE 지원이 요약되어 있습니다.

플랫폼	암호화 엔진 유형	NGE에서 지원	NGE 지원을 위한 Cis IOS/IOS-XE의 첫 버전
Cisco IOS Classic을 실행하는 모든 플랫폼	Cisco IOS 소프트웨어 암호화 엔진	예	15.1(2)T
7200	VAM/VAM2/VSA	아니요	해당 없음
ISR G1	모두	아니요	해당 없음
ISR G2 2951, 3925, 3945	온보드[1]	예	15.1(3)T
ISR G2(3925E/3945E 제외)	VPN-ISM[1]	예	15.2(1)T1
ISR G2 1900, 2901, 2911, 2921, 3925E, 3945E	온보드[1]	예	15.2(4)만
ISR G2 CISCO87x	소프트웨어/하드웨어	아니요	해당 없음
ISR G2 CISCO86x/C86x	소프트웨어[2]	예	15.1(2)T
ISR G2 C812/C819	소프트웨어/하드웨어	예	1일
ISR G2 CISCO88x/CISCO89x	소프트웨어/하드웨어[3]	예	15.1(2)T
ISR G2 C88x	소프트웨어/하드웨어[4]	예	1일
6500/7600	VPN-SPA	아니요	해당 없음
ASR 1000	Onboard	예	참고[5]
ASR 1001-X, ASR 1002-X, ASR 1006-X, ASR 1009-X	Onboard	예	Cisco IOX-XE 3.12(15.4(2)S)
ASR 1001-HX, ASR1002-HX	선택적 암호화 모듈	예	16.3.1
ISR 4451-X	Onboard	예	Cisco IOS-XE 3.9(15.3(2)S)
ISR 4321, 4331, 4351, 4431	Onboard	예	Cisco IOS-XE 3.13(15.4(3)S)
ISR 42xx	Onboard	예	Cisco IOS-XE Everes 16.4.1
CSR 1000v	소프트웨어	예	Cisco IOS-XE 3.12(15.4(2)S)
ISR 1100	Onboard	예	Cisco IOS-XE Everes 16.6.2
Catalyst 8200, 8300, 8500 에지 플랫폼	Onboard	예	1일
Catalyst 8000v	소프트웨어	예	1일

참고 1:ISR G2 플랫폼에서 ECDH/ECDSA가 구성된 경우 암호화 엔진에 관계없이 소프트웨어에서 이러한

화 작업을 실행합니다.AES-GCM-128 및 AES-GCM-256 암호화 알고리즘은 버전 15.4(2)T 이후 IKEv2 컨트
플레인 보호에 대해 지원됩니다.
참고 2:ISR G2 CISCO86x/C86x는 하드웨어 암호화 엔진에서 NGE를 지원하지 않습니다.
참고 3:ISR G2 CISCO88x/CISCO89x는 버전 15.2(4)M3 이상에서만 SHA-256을 지원합니다.
참고 4:이러한 C88x SKU에는 NGE에 대한 하드웨어 지원이 없습니다.C881SRST-K9, C881SRSTW-GN-A
C881SRSTW-GN-E-K9, C881-CUBE-K9, C881-V-K9, C81G-U-K9, C88 1G-S-K9, C881G-V-K9, C881G-E
C881G+7-K9, C881G+7-A-K9, C886SRST-K9, C86SRW-GN-K9-K9, C886VA-CUBE-K9, C886VAG+7-K9
C887SRST-K9, C887SRSTW-GN-A-K9, C887SRSTW-GN-E-K9, C887VSRST9 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, C88SRSTW-GN-E-K9, C888SRST-K9, C88
K9, C888ESRSTW-GNA-K9, C888ESRSTW-GNE-K9, C888-CUBE-K9, C888E-CUBE-K9 및 C888EG+7-
참고 5:NGE 컨트롤 플레인(ECDH 및 ECDSA)에 대한 지원은 버전 XE3.7(15.2(4)S)과 함께 도입되었습니다
기 컨트롤 플레인 SHA-2 지원은 IKEv2에만 적용되었으며, 버전 XE3.10(15.3(3)S)에 IKEv1 지원이 추가되
니다.AES-GCM-128 및 AES-GCM-256 암호화 알고리즘은 버전 XE3.12(15.4(2)S) 및 15.4(2)T 이후 IKEv2
롤 플레인 보호에 대해 지원됩니다.NGE 데이터 플레인 지원은 Octeon 기반 플랫폼 전용 버전
XE3.8(15.3(1)S)에서 추가되었습니다(ESP-100 또는 ESP-200 모듈이 있는 ASR106 또는 ASR1013).다른
ASR1000 플랫폼에서는 데이터 플레인 지원을 사용할 수 없습니다.

기타 NGE 기능 지원

NGE를 위한 GETVPN 지원

- ISR G2 플랫폼에 대한 Cisco IOS 소프트웨어 지원은 버전 15.2(4)M부터 시작합니다.
- ASR 지원은 Cisco IOS-XE 소프트웨어 버전 3.10S(15.3(3)S)부터 시작합니다.

관련 정보

- 차세대 암호화
- 기술 지원 및 문서 – Cisco Systems