Cisco IOS en IOS-XE ondersteuning voor encryptie van de volgende generatie

Inhoud

Inleiding

In dit document wordt de ondersteuning van Next Generation Encryption (NGE) beschreven op Cisco IOS® en Cisco IOS-XE platforms.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco IOS, meerdere versies zoals in de tabel vermeld
- Cisco IOS-XE, meerdere versies zoals in de tabel vermeld
- Meervoudige Cisco-platforms zoals in de tabel vermeld

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

NGE-algoritmen

De algoritmen waaruit NGE bestaat, zijn het resultaat van meer dan 30 jaar mondiale vooruitgang en evolutie in cryptografie. Elke component van NGE heeft zijn eigen geschiedenis, die de diverse geschiedenis van de NGE-algoritmen en hun reeds lang bestaande academische en community-review weergeeft. NGE bestaat uit wereldwijd gemaakte, mondiaal bekeken en publiek

beschikbare algoritmen.

NGE-algoritmen zijn geïntegreerd in Internet Engineering Task Force (IETF), IEEE en andere internationale standaarden. Als resultaat hiervan zijn NGE-algoritmen toegepast op de meest recente en zeer veilige protocollen die gebruikersgegevens beschermen, zoals Internet Key Exchange versie 2 (IKEv2).

Typen cryptografische algoritmen omvatten:

- Symmetrische encryptie-128-bits of 256-bits Advanced Encryption Standard (AES) in GCM (Galois/Counter-modus)
- Hash - Secure Hash Algorithms (SHA)-2 (SHA-256, SHA-384 en SHA-512)
- Digitale handtekeningen -Elliptic Curve Digital Signature Algorithm (ECDSA)
- Belangrijke overeenkomst - Elliptische curve Diffie-Hellman (ECDH)

NGE-ondersteuning op Cisco IOS en Cisco IOS-XE platforms

Deze tabel vat NGE-ondersteuning samen op Cisco IOS-gebaseerde en Cisco IOS-XE gebaseerde platforms.

Platforms	Type encryptie-motor	Ondersteund door NGE	Eerste versie van Cisco IOS/IOS-XE voor ondersteuning van NGE
Alle platforms die Cisco IOS klassiek gebruiken	Cisco IOS-softwareencryptie-motor	Ja	15.1(2)T
7200	VAM/VAM2/VSA	Nee	N.v.t.
ISR G1	Alle	Nee	N.v.t.
ISR G2 2951, 3925, 3945	Aan boord[1]	Ja	15.1(3)T
ISR G2 (behalve 3925E/3945E)	VPN/ISM[1]	Ja	15.2(1)T1
ISR G2 1900, 2901, 2911, 2921, 3925E, 3945E	Aan boord[1]	Ja	15,2(4)M
ISR G2 CISCO87x	Software/hardware	Nee	N.v.t.
ISR G2 CISCO 86x/C86x-software	Software[2]	Ja	15.1(2)T
ISR G2 C812/C819	Software/hardware	Ja	Dag 1
ISR G2 CISCO88x/CISCO89x	Software/hardware[3]	Ja	15.1(2)T
ISR G2 C88x-software	Software/hardware[4]	Ja	Dag 1
6500/7600	VPN-SPA	Nee	N.v.t.
ASR 1000 router	Aan/uit	Ja	Opmerking[5]
ASR 1001-X, ASR 1002-X, ASR 1006-X, ASR 1009-X	Aan/uit	Ja	Cisco IOS-XE 3.12 (15.4(2)S)
ASR 1001-HX, ASR 1002-HX	Optionele coderingsmodule	Ja	Denali-16.3.1

ISR 4451-X router	Aan/uit	Ja	Cisco IOS-XE 3.9(15.3(2)S)
ISR 4321, 4331, 4351, 4431	Aan/uit	Ja	Cisco IOS-XE 3.13(15.4(3)S)
ISR 420-xx	Aan/uit	Ja	Cisco IOS-XE Everest 16.4.1
CSR 1000v-module	Software	Ja	Cisco IOS-XE 3.12(15.4(2)S)
ISR 1100	Aan/uit	Ja	Cisco IOS-XE Everest 16.6.2
Catalyst 8200, 8300, 8500 Edge-platforms	Aan/uit	Ja	Dag 1
Catalyst 8000v switch	Software	Ja	Dag 1

Opmerking 1: Op het ISR G2-platform, indien ECDH/ECDSA is ingesteld, worden deze cryptografische bewerkingen uitgevoerd in software ongeacht de cryptografische motor. AES-GCM-128 en AES-GCM-256 encryptie-algoritmen zijn ondersteund voor de beveiliging van IKEv2-besturingsplane sinds versie 15.4(2)T.
Noot 2: ISR G2 CISCO86x/C86x biedt geen NGE-ondersteuning voor de hardwareencryptie-machine.
Noot 3: ISR G2 CISCO88x/CISCO89x biedt alleen hardwareondersteuning voor SHA-256 met versie 15.2(4)M3 of hoger.
Noot 4: Deze C88x-SKU's hebben geen hardwareondersteuning voor 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-B-K9, C881G+7-K9, C881G+7-A-K9, C886SRST-K9, C886SRSTW-GN-E-K9, C889 86VA-CUBE-K9, C886VAG+7-K9, C887SRST-K9, C887SRSTW-GN-K9, C887SRSTW-GN-E-K9, C887VSRST-K9, C887SRV STW-GNA-K9, C887VSRSTW-GNE-K9, C887VA-V-K9, C887VA-V-W-E-K9, C887VA-CUBE-K9, C887VAG-S-K9, C887VAG+AG K9, C887VAMG+7-K9, C888SRSTW-GN-K9, C888SRSTW-GN-E-K9, C888SRST-K9, C888ESR-K9, C888ESRSTW-GNA-K K9, C888ESR-GNE-K9, C888-CUBE-K9, C888E-CUBE-K9 en C888EG+7-K9.
Opmerking 5: Er is ondersteuning voor het NGE-besturingsplane (ECDH en ECDSA) geïntroduceerd met versie XE3.7 (15.2(4)S). Ondersteuning van het initiële besturingsplane SHA-2 was alleen voor IKEv2, met ondersteuning van IKEv1 toegevoegd in versie XE3.10 (15.3(3)S). AES-GCM-128 en AES-GCM-256-encryptie algoritmen zijn ondersteund voor de beveiliging van IKEv2-besturingsplane sinds versie XE3.12 (15.4(2)S) en 15.4(2)T. NGE-ondersteuning voor dataplanen is toegevoegd in versie XE3.8 (15.3(1)S) voor alleen op Octal gebaseerde platforms (ASR1006 of ASR1013 met een ESP-100 of ESP-200 module); Ondersteuning van dataplane is niet beschikbaar voor andere ASR1000-platforms.

Ondersteuning van andere NGE-functies

GETVPN-ondersteuning voor NGE

- Cisco IOS-softwarerelease 12.2 op ISR G2-platforms begint met versie 15.2(4)M.
- ASR-ondersteuning begint met Cisco IOS-XE software, versie 3.10S (15.3(3)S).

Gerelateerde informatie

- Cryptografie van de volgende generatie
- Technische ondersteuning en documentatie – Cisco Systems