Prise en charge du cryptage nouvelle génération Cisco IOS et IOS-XE

Contenu

Introduction

Ce document décrit la prise en charge du chiffrement de nouvelle génération (NGE) sur les plates-formes Cisco IOS® et Cisco IOS-XE.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco IOS, plusieurs versions comme indiqué dans le tableau
- Cisco IOS-XE, plusieurs versions comme indiqué dans le tableau
- Plusieurs plates-formes Cisco, comme indiqué dans le tableau

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Algorithmes NGE

Les algorithmes qui composent NGE sont le résultat de plus de 30 ans d'avancées et d'évolution mondiales en matière de cryptographie. Chaque composante de l'END a sa propre histoire, qui dépeint l'histoire variée des algorithmes de l'END et leur étude universitaire et communautaire de longue date. NGE comprend des algorithmes créés, révisés globalement et accessibles au public.

Les algorithmes NGE sont intégrés à l'IETF (Internet Engineering Task Force), à l'IEEE et à d'autres normes internationales. En conséquence, les algorithmes NGE ont été appliqués aux protocoles les plus récents et hautement sécurisés qui protègent les données utilisateur, tels que IKEv2 (Internet Key Exchange Version 2).

Les types d'algorithmes cryptographiques sont les suivants :

- Cryptage symétrique - norme de cryptage avancé (AES) 128 bits ou 256 bits dans GCM (mode Galois/Counter)
- Hash - SHA (Secure Hash Algorithms)-2 (SHA-256, SHA-384 et SHA-512)
- Signatures numériques - Algorithme de signature numérique de courbe elliptique (ECDSA)
- Accord clé - Diffie-Hellman (ECDH) de courbe elliptique

Prise en charge NGE sur les plates-formes Cisco IOS et Cisco IOS-XE

Ce tableau récapitule la prise en charge NGE sur les plates-formes Cisco IOS et Cisco IOS-XE.

Plates-formes	Type de moteur de chiffrement	Prise en charge par NGE	Première version de IOS/IOS-XE pour pre en charge NGE
Toutes les plates-formes exécutant Cisco IOS classique	Moteur de chiffrement du logiciel Cisco IOS	Oui	15.1(2)T
7200	VAM/VAM2/VSA	Non	S/O
ISR G1	all	Non	S/O
ISR G2 2951, 3925, 3945	embarqué[1]	Oui	15.1(3)T
ISR G2 (excluant 3925E/3945E)	VPN-ISM[1]	Oui	15.2(1)T1
ISR G2 1900, 2901, 2911, 2921, 3925E, 3945E	embarqué[1]	Oui	15.2(4)M
ISR G2 CISCO87x	Logiciels / Matériel	Non	S/O
ISR G2 CISCO86x/C86x	Logiciel[2]	Oui	15.1(2)T
ISR G2 C812/C819	Logiciels / Matériel	Oui	Jour 1
ISR G2 CISCO88x/CISCO89x	Logiciel / Matériel[3]	Oui	15.1(2)T
ISR G2 C88x	Logiciels / Matériel[4]	Oui	Jour 1
6500/7600	VPN-SPA	Non	S/O
ASR 1000	Intembarqué	Oui	Note [5]
ASR 1001-X, ASR 1002-X, ASR 1006-X, ASR 1009-X	Intembarqué	Oui	Cisco IOX-XE 3.12 (15.4(2)S)
ASR 1001-HX, ASR1002-HX	Module Crypto en option	Oui	Denali-16.3.1
ISR 4451-X	Intembarqué	Oui	Cisco IOS-XE 3.9 (15.3(2)S)
ISR 4321, 4331, 4351, 4431	Intembarqué	Oui	Cisco IOS-XE 3.13 (15.4(3)S)
ISR 42xx	Intembarqué	Oui	Cisco IOS-XE Everes 16.4.1
CSR 1000v	le logiciel Cisco IOS	Oui	Cisco IOS-XE 3.12

ISR 1100	Intembarqué	Oui	(15.4(2)S) Cisco IOS-XE Everes 16.6.2
Plates-formes de périphérie Catalyst 8200, 8300 et 8500	Intembarqué	Oui	Jour 1
Catalyst 8000v	le logiciel Cisco IOS	Oui	Jour 1

Remarque 1 : Sur la plate-forme ISR G2, si ECDH/ECDSA est configuré, ces opérations de cryptographie seront exécutées dans un logiciel quel que soit le moteur de cryptographie. Les algorithmes de chiffremer AES-GCM-128 et AES-GCM-256 sont pris en charge pour la protection du plan de contrôle IKEv2 depuis version 15.4(2)T.
Remarque 2 : ISR G2 CISCO86x/C86x ne prend pas en charge NGE dans le moteur de cryptage matérie
Remarque 3 : ISR G2 CISCO88x/CISCO89x prend en charge le matériel SHA-256 UNIQUEMENT avec l version 15.2(4)M3 ou ultérieure.
Remarque 4 : Ces références C88x ne prennent pas en charge le matériel pour NGE : C881SRST-K9, C881SRSTW-GN-A-K9, C881SRSTW-GN-E-K9, C881-CUBE-K9, C881-V-K9, C881G-U-K9, C881G - S- C881G-V-K9, C881G-B-K9, C881G+7-K9, C881G+7-A-K9, C886SRST-K9, C886SRSTW-GN-E-K9, C88 86VA-CUBE-K9, C886VAG+7-K9, C887SRST-K9, C887SRSTW-GN-A-K9, C887SRSTW-GN-E-K9, C887VSRST-K9, C887VSRST STW-GNA-K9, C887VSRSTW-GNE-K9, C887VA-V-K9, C887VA-V-W-E-K C887VA-CUBE-K9, C887VAG-S-K9, C887VAG+7 K9, C887VAMG+7-K9, C888SRST-GN-A-K9, C888SRSTW-GN-E-K9, C888SRST-K9, C888ESRST-K9, C888ESRSTW-GNA-GNA K9, C888ESRSTW- GNE-K9, C888-CUBE-K9, C888E-CUBE-K9 et C888EG+7-K9.
Remarque 5 : La prise en charge du plan de contrôle NGE (ECDH et ECDSA) a été introduite avec la ver XE3.7 (15.2(4)S). La prise en charge initiale du plan de contrôle SHA-2 était uniquement pour IKEv2, ave prise en charge IKEv1 ajoutée dans la version XE3.10 (15.3(3)S). Les algorithmes de chiffrement AES-G 128 et AES-GCM-256 ont été pris en charge pour la protection du plan de contrôle IKEv2 depuis les versi XE3.12 (15.4(2)S) et 15.4(2)T. La prise en charge du plan de données NGE a été ajoutée dans la version XE3.8 (15.3(1)S) pour les plates-formes basées sur Octeon uniquement (ASR1006 ou ASR1013 avec un module ESP-100 ou ESP-200); La prise en charge du plan de données n'est pas disponible pour les autr plates-formes ASR1000.

Autres fonctionnalités NGE

Prise en charge GETVPN pour NGE

- La prise en charge du logiciel Cisco IOS sur les plates-formes ISR G2 commence avec la version 15.2(4)M.
- La prise en charge d'ASR commence avec le logiciel Cisco IOS-XE, version 3.10S (15.3(3)S).

Informations connexes

- Cryptographie de nouvelle génération
- Support et documentation techniques - Cisco Systems