Contenu

Introduction

Ce document décrit le support du cryptage de nouvelle génération (NGE) sur le Cisco IOS® et les Plateformes IOS-XE.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

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

- Cisco IOS, plusieurs versions comme observé dans la table
- Cisco IOS XE, plusieurs versions comme observé dans la table
- Plusieurs Plateformes de Cisco comme observé dans la table

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Algorithmes NGE

Les algorithmes qui composent NGE sont le résultat de plus de 30 ans d'avances globales et évolution dans le chiffrement. Chaque composant de NGE a son propre historique, qui dépeint l'historique divers des algorithmes NGE et de leur examen de longue date d'universitaire et de

communauté. NGE comporte globalement créé, globalement passé en revue, et publiquement - les algorithmes disponibles.

Des algorithmes NGE sont intégrés dans l'Internet Engineering Task Force (IETF), l'IEEE, et d'autres normes internationales. En conséquence, des algorithmes NGE ont été appliqués aux protocoles les plus récents et haut-les plus sécurisés qui protègent des données d'utilisateur, telles que la version 2 (IKEv2) d'échange de clés Internet (IKE).

Les types d'algorithmes de chiffrement incluent :

- Norme AES (Advanced Encryption Standard) -128-bit ou 256-bit de cryptage symétrique dans GCM (mode de Galois/compteur)
- Informations parasites - Secure Hash Algorithm (SHA)-2 (SHA-256, SHA-384, et SHA-512)
- Signatures numériques - Algorithme elliptique de signature numérique de curve (ECDSA)
- Accord principal - Curve elliptique Diffie-Hellman (ECDH)

Support NGE sur des Plateformes IOS et IOS-XE

Cette table récapitule le support NGE sur les Plateformes basées sur IOS et basées sur IOS de Cisco.

Plateformes	Type de moteur de chiffrement	Pris en charge par NGE	Première version de IOS/IOS-XE pour pre en charge NGE
Toutes les Plateformes qui exécutent le classique IOS	Moteur de chiffrement de logiciel IOS	Oui	15.1(2)T
7200	VAM/VAM2/VSA	Non	S/O
ISR G1	Tous	Non	S/O
ISR G2 2951, 3925, 3945	Àbord de	Oui	15.1(3)T
ISR G2 (exclut 3925E/3945E)	VPN-ISM	Oui	15.2(1)T1
ISR G2 1900, 2901, 2911, 2921, 2951, 3925, 3945, 3925E, 3945E	Àbord de	Oui	15.2(4)M
ISR G2 CISCO87x	Logiciel/matériel	Non	S/O
ISR G2 CISCO86x/C86x	Logiciel	Oui	15.1(2)T
ISR G2 C812/C819	Logiciel/matériel	Oui	Jour 1
ISR G2 CISCO88x/CISCO89x	Logiciel/matériel	Oui	15.1(2)T
ISR G2 C88x	Logiciel/matériel	Oui	Jour 1
6500/7600	VPN-SPA	Non	S/O
ASR 1000	Àbord	Oui	Note
ISR 4451-X	Àbord	Oui	IOS-XE 3.9 (15.3(2)S
ISR 4321, 4331, 4351, 4431	Àbord	Oui	IOS-XE 3.13 (15.4(3)
CSR 1000v	Logiciel	Oui	IOS-XE 3.12 (15.4(2)

Note 1 : Sur la plate-forme d'ISR G2, si ECDH/ECDSA est configuré, ces exécutions cryptographiques se exécutées en logiciel indépendamment de l'engine cryptographique.

Note 2 : L'ISR G2 CISCO86x/C86x n'a pas le support NGE dans le moteur de chiffrement de matériel.
Note 3 : L'ISR G2 CISCO88x/CISCO89x a le support matériel pour SHA-256 SEULEMENT avec la versio
15.2(4)M3 ou ultérieures.
Note 4 : Ces C88x UGS n'ont aucun support matériel pour 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-
C881G+7-K9, C881G+7-A-K9, C886SRST-K9, C886SRSTW-GN-E-K9, C886VA-CUBE-K9, C886VAG+7
C887SRST-K9, C887SRSTW-GN-A-K9, C887SRSTW-GN-E-K9, C887VSRST-K9, C887VSRSTW-GNA-
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, C888ESRSTW-GNA-K9, C888ESRSTW-GNE-K9, C888-CUBE-K9, C888E-CUBE-K9,
C888EG+7-K9.
Note 5 : Le soutien de l'avion de contrôle NGE (ECDH et ECDSA) a été introduit avec la version XE3.7
(15.2(4)S). Le support SHA-2 plat de contrôle est pour IKEv2 seulement, avec le support IKEv1 ajouté da
version XE3.10 (15.3(3)S). Le support de Dataplane est ajouté dans la version XE3.8 (15.3(1)S) pour Oct
basé des Plateformes seulement (ASR1001-X, ASR1002-X, ESP-100, et ESP-200) ; le support de datapl
n'est pas disponible pour d'autres Plateformes ASR.

L'autre prise en charge de fonctionnalité NGE

Soutien GETVPN de NGE

- Support logiciel de Cisco IOS sur des débuts de Plateformes d'ISR G2 avec la version 15.2(4)M.
- Débuts de support ASR avec le Logiciel Cisco IOS XE version 2, version 3.10S (15.3(3)S).