Содержание

Введение

Этот документ описывает поддержку Шифрования следующего поколения (NGE) на платформах XE IOS и Cisco IOS®.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Cisco IOS, несколька версий, как обращено внимание в таблице
- Cisco IOS XE, несколька версий
- Множественные Платформы cisco, как обращено внимание в таблице

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Алгоритмы NGE

Алгоритмы, которые составляют NGE, являются результатом больше чем 30 лет глобальных усовершенствований и развития в криптографии. Каждый компонент NGE имеет свою собственную историю, которая изображает разнообразную историю алгоритмов NGE и

их долгосрочного академика и анализа сообщества. NGE включает глобально созданный, глобально рассмотренные, и общедоступные алгоритмы.

Алгоритмы NGE интегрированы в инженерную группу по развитию Интернета (IETF), IEEE и другие международные стандарты. В результате алгоритмы NGE были применены к новым и высоко-защищенным-протоколам, которые защищают пользовательские данные, такие как вторая версия протокола Internet Key Exchange (IKEv2).

Типы криптографических алгоритмов включают:

- Симметричное шифрование - 128-разрядный или 256-разрядный Расширенный стандарт шифрования (AES) в GCM (Режим Галуа/Счетчика)
- Хэш - защищенные алгоритмы хэширования (SHA)-2 (SHA 256, SHA 384 и SHA 512)
- Цифровые подписи - Алгоритм цифровой подписи эллиптической кривой (ECDSA)
- Согласование ключей - Диффи-Хеллман эллиптической кривой (ECDH)

Поддержка NGE на IOS и платформах XE IOS

Эта таблица суммирует поддержку NGE на Cisco на основе IOS и ОСНОВАННЫХ НА IOS-XE платформах.

Платформы	Тип ядра шифрования	Поддерживаемый NGE	Первая Версия Cisco IOS/IOS-XE для Поддержки NGE
Все платформы, которые выполняют классику IOS	Механизм программного шифрования IOS	Да	15.1 (2) T
7200	VAM/VAM2/VSA	Нет	Н/Д
ISR G1	Все	Нет	Н/Д
ISR G2 2951, 3925, 3945		Да	15.1 (3) T
ISR G2 (исключает 3925E/3945E),		Да	15.2 (1) T1
ISR G2 1900, 2901, 2911, 2921, 2951, 3925, 3945, 3925E, 3945E		Да	15.2 (4) M
ISR G2 CISCO87x	Программное обеспечение / Аппаратные средства	Нет	Н/Д
ISR G2 CISCO86x/C86x		Да	15.1 (2) T
ISR G2 C812/C819	Программное обеспечение / Аппаратные средства	Да	День 1
ISR G2 CISCO88x/CISCO89x	Программное обеспечение /	Да	15.1 (2) T

ISR G2 C88x	Программное обеспечение /	Да	День 1
6500/7600	SPA VPN	Нет	Н/Д
ASR 1000	На борту	Да	Note5
4451-X ISR	На борту	Да	XE IOS 3.9 (15.3 (2) S)
ISR 4321, 4331, 4351, 4431	На борту	Да	XE IOS 3.13 (15.4 (3) S)
CSR 1000v	Программное обеспечение	Да	XE IOS 3.12 (15.4 (2) S)

Примечание 1: На платформе ISR G2, если ECDH/ECDSA настроен, эти криптографические операции будут выполнены в программном обеспечении независимо от криптографического механизма.
Примечание 2: ISR G2 CISCO86x/C86x не имеет поддержки NGE в аппаратном ядре шифрования.
Примечание 3: ISR G2 CISCO88x/CISCO89x имеет аппаратную поддержку для SHA 256 ONLY с Версией 15.2 (4) M3 или позже.
Обратите внимание 4: Они C88x SKUs не имеют никакой аппаратной поддержки для 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, 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, C888ESRSTW-GNA-K9, C888ESRSTW-GNE-K9, C888-CUBE-K9, C888E-CUBE-K9, и C888EG+7-K9.
Обратите внимание 5: Поддержка уровня управления NGE (ECDH и ECDSA) была начата с Версии XE3.7 (15.2 (4) S). Поддержка уровня управления SHA 2 для IKEv2 только с поддержкой IKEv1, добавленной в Версии XE3.10 (15.3 (3) S). Поддержка Dataplane добавлена в Версии XE3.8 (15.3 (1), S) для Octeon базировал платформы только (ASR1001-X, ASR1002-X, ESP 100 и ESP 200); поддержка dataplane не доступна для других платформ ASR.

Другая поддержка характеристик NGE

Поддержка GETVPN NGE

- Поддержка Программного обеспечения Cisco IOS на платформах ISR G2 запускается с Версии 15.2 (4) M.
- Поддержка ASR запускается с программного обеспечения Cisco IOS XE, Версия 3.10S (15.3 (3) S).