Когда FIPS Включен, клиент AnyConnect Жалуется На Неподдерживаемые Криптографические алгоритмы

Содержание

Введение

Этот документ описывает, почему пользователи не могли бы быть в состоянии подключить с использованием Федерального стандарта обработки информации (FIPS) (FIPS) поддерживающего клиента к Устройству адаптивной защиты (ASA), которое имеет политику, которая поддерживает поддерживающие FIPS алгоритмы шифрования.

Общие сведения

Во время установленного соединения второй версии протокола Internet Key Exchange (IKEv2) инициатор никогда не знает о том, какие предложения приемлемы узлом, таким образом, инициатор должен предположить , какую группу Diffie-Hellman (DH) использовать, когда передается первое сообщение IKE. Группа DH, используемая для этого предположения, обычно является первой группой DH в списке настроенных групп DH. Инициатор тогда вычисляет ключевые данные для предполагаемых групп, но также и передает полный список всех групп к узлу, который позволяет узлу выбирать другую группу DH, если предполагаемая группа неправа.

В случае клиента нет никакого настраиваемого списка Наборов правил IKE. Вместо этого существует предварительно сконфигурированный список политики что поддержки клиентов. Из-за этого, для сокращения вычислительной загрузки на клиенте при вычислении ключевых данных для первого сообщения с группой, которая является возможно неправильной, список групп DH был упорядочен от самого слабого до самого сильного. Таким образом клиент выбирает наименее в вычислительном отношении интенсивный DH и поэтому наименьшее количество группы загруженности ресурсов для исходного предположения, но тогда переключается группе, выбранной головным узлом в последующих сообщениях.

> **Примечание:** Это поведение является другим от клиентов Версии 3.0 AnyConnect, которые упорядочили группы DH от самого сильного до самого слабого.

Однако на головном узле, первая группа DH в списке, передаваемом клиентом, который совпадает с группой DH, настроенной на шлюзе, является группой, которая выбрана. Поэтому, если ASA также настроили более слабые группы DH, он использует самую слабую группу DH, которая поддерживается клиентом и настроенный на головном узле несмотря на доступность более безопасной группы DH на обоих концах.

Это поведение было закреплено на клиенте через идентификатор ошибки Cisco CSCub92935. Все версии клиентской части с исправлением от этого дефекта инвертируют заказ, в котором перечислены группы DH, когда они передаются головному узлу. Однако во избежание назад-проблемы-совместимости с некомплектом B шлюзы, самая слабая группа DH (один для режима не-FIPS и два для режима FIPS) остается наверху списка.

> **Примечание:** После первой записи в списке (группа 1 или 2), группы перечислены в порядке самого сильного к самому слабому. Это помещает группы эллиптической кривой сначала (21, 20, 19), придерживавшийся Модульным Экспоненциалом (MODP) группы (24, 14, 5, 2).

> **Совет:** Если шлюз настроен со множественными группами DH в той же политике, и группа 1 (или 2 в режиме FIPS) включена, то ASA принимает более слабую группу. Исправление должно только включать группу DH 1 один в политику, настроенную на шлюзе. Когда множественные группы настроены в одной политике, но группа 1 не включена, тогда самое сильное выбрано. Пример:
>
> - На Версии ASA 9.0 (комплект B) с набором политики IKEv2 к 1 2 5 14 24 19 20 21, **группа 1 выбрана** как ожидалось.
>
> - На Версии ASA 9.0 (комплект B) с набором политики IKEv2 к 2 5 14 24 19 20 21, **группа 21 выбрана** как ожидалось.
>
> - С клиентом в режиме FIPS на Версии ASA 9.0 (комплект B) с набором политики IKEv2 к 1 2 5 14 24 19 20 21, **группа 2 выбрана** как ожидалось.
>
> - С протестированным клиентом в режиме FIPS на Версии ASA 9.0 (комплект B) с набором политики IKEv2 к 5 14 24 19 20 21, **группа 21 выбрана** как ожидалось.
>
> - На Версии ASA 8.4.4 (некомплект B) с набором политики IKEv2 к 1 2 5 14, **группа 1 выбрана** как ожидалось.
>
> - На Версии ASA 8.4.4 (некомплект B) с набором политики IKEv2 к 2 5 14, **группа 14 выбрана** как ожидалось.

Проблема

ASA настроен с этой политикой IKEv2:

```
crypto ikev2 policy 1
encryption aes-gcm-256
integrity null
group 20
```

```
prf sha384 sha
lifetime seconds 86400
crypto ikev2 policy 10
encryption aes-192
integrity sha
group 5 2
prf sha
lifetime seconds 86400
crypto ikev2 policy 20
encryption aes
integrity sha
group 5 2
prf sha
lifetime seconds 86400
```

В этой конфигурации политика 1 ясно настроена для поддержки всех поддерживающих FIPS криптографических алгоритмов. Однако, когда пользователь пытается соединиться от поддерживающего FIPS клиента, сбоев соединения с сообщением об ошибках:

```
The cryptographic algorithms required by the secure gateway do not match those
supported by AnyConnect. Please contact your network administrator.
```

Однако, если admin изменяет policy1 так, чтобы это использовало DH group 2 вместо 20, соединение работает.

Решение

На основе признаков первое заключение состояло бы в том, что клиент только поддерживает DH group 2, когда FIPS включен, и ни один из других не работает. Это фактически неправильно. При включении этой отладки на ASA вы видите предложения, передаваемые клиентом:

`debug crypto ikev2 proto 127`

Во время попытки подключения первое сообщение отладки:

```
IKEv2-PROTO-2: Received Packet [From 192.168.30.5:51896/To 192.168.30.2:500/
VRF i0:f0]
Initiator SPI : 74572B8D1BEC5873 - Responder SPI : 0000000000000000 Message id: 0
IKEv2 IKE_SA_INIT Exchange REQUESTIKEv2-PROTO-3: Next payload: SA, version:
2.0 Exchange type: IKE_SA_INIT, flags: INITIATOR Message id: 0, length: 747
Payload contents:
SA Next payload: KE, reserved: 0x0, length: 316
last proposal: 0x2, reserved: 0x0, length: 140
Proposal: 1, Protocol id: IKE, SPI size: 0, #trans: 15 last transform: 0x3,
reserved: 0x0: length: 12
type: 1, reserved: 0x0, id: AES-GCM
last transform: 0x3, reserved: 0x0: length: 12
type: 1, reserved: 0x0, id: AES-GCM
last transform: 0x3, reserved: 0x0: length: 12
type: 1, reserved: 0x0, id: AES-GCM
last transform: 0x3, reserved: 0x0: length: 8
type: 2, reserved: 0x0, id: SHA512
last transform: 0x3, reserved: 0x0: length: 8
type: 2, reserved: 0x0, id: SHA384
last transform: 0x3, reserved: 0x0: length: 8
type: 2, reserved: 0x0, id: SHA256
last transform: 0x3, reserved: 0x0: length: 8
type: 2, reserved: 0x0, id: SHA1
last transform: 0x3, reserved: 0x0: length: 8
```

```
type: 3, reserved: 0x0, id: None
last transform: 0x3, reserved: 0x0: length: 8
type: 4, reserved: 0x0, id: DH_GROUP_1024_MODP/Group 2
last transform: 0x3, reserved: 0x0: length: 8
type: 4, reserved: 0x0, id: DH_GROUP_521_ECP/Group 21
last transform: 0x3, reserved: 0x0: length: 8
type: 4, reserved: 0x0, id: DH_GROUP_384_ECP/Group 20
last transform: 0x3, reserved: 0x0: length: 8
type: 4, reserved: 0x0, id: DH_GROUP_256_ECP/Group 19
last transform: 0x3, reserved: 0x0: length: 8
type: 4, reserved: 0x0, id: DH_GROUP_2048_MODP_256_PRIME/Group 24
last transform: 0x3, reserved: 0x0: length: 8
type: 4, reserved: 0x0, id: DH_GROUP_2048_MODP/Group 14
last transform: 0x0, reserved: 0x0: length: 8
type: 4, reserved: 0x0, id: DH_GROUP_1536_MODP/Group 5
last proposal: 0x0, reserved: 0x0, length: 172
Proposal: 2, Protocol id: IKE, SPI size: 0, #trans: 19 last transform: 0x3,
reserved: 0x0: length: 12
type: 1, reserved: 0x0, id: AES-CBC
last transform: 0x3, reserved: 0x0: length: 12
type: 1, reserved: 0x0, id: AES-CBC
last transform: 0x3, reserved: 0x0: length: 12
type: 1, reserved: 0x0, id: AES-CBC
last transform: 0x3, reserved: 0x0: length: 8
type: 1, reserved: 0x0, id: 3DES
last transform: 0x3, reserved: 0x0: length: 8
type: 2, reserved: 0x0, id: SHA512
last transform: 0x3, reserved: 0x0: length: 8
type: 2, reserved: 0x0, id: SHA384
last transform: 0x3, reserved: 0x0: length: 8
type: 2, reserved: 0x0, id: SHA256
last transform: 0x3, reserved: 0x0: length: 8
type: 2, reserved: 0x0, id: SHA1
last transform: 0x3, reserved: 0x0: length: 8
type: 3, reserved: 0x0, id: SHA512
last transform: 0x3, reserved: 0x0: length: 8
type: 3, reserved: 0x0, id: SHA384
last transform: 0x3, reserved: 0x0: length: 8
type: 3, reserved: 0x0, id: SHA256
last transform: 0x3, reserved: 0x0: length: 8
type: 3, reserved: 0x0, id: SHA96
last transform: 0x3, reserved: 0x0: length: 8
type: 4, reserved: 0x0, id: DH_GROUP_1024_MODP/Group 2
last transform: 0x3, reserved: 0x0: length: 8
type: 4, reserved: 0x0, id: DH_GROUP_521_ECP/Group 21
last transform: 0x3, reserved: 0x0: length: 8
type: 4, reserved: 0x0, id: DH_GROUP_384_ECP/Group 20
last transform: 0x3, reserved: 0x0: length: 8
type: 4, reserved: 0x0, id: DH_GROUP_256_ECP/Group 19
last transform: 0x3, reserved: 0x0: length: 8
type: 4, reserved: 0x0, id: DH_GROUP_2048_MODP_256_PRIME/Group 24
last transform: 0x3, reserved: 0x0: length: 8
type: 4, reserved: 0x0, id: DH_GROUP_2048_MODP/Group 14
last transform: 0x0, reserved: 0x0: length: 8
type: 4, reserved: 0x0, id: DH_GROUP_1536_MODP/Group 5
KE Next payload: N, reserved: 0x0, length: 136
DH group: 2, Reserved: 0x0

fc c9 90 2b 15 35 31 34 0e 75 88 c0 f9 2a 1e 0a
a5 6b e3 8e e1 73 b9 d1 56 1e 60 9f 82 71 6c 4e
5c 1c a4 bd b5 23 a2 bc 82 f2 11 17 61 28 33 3f
02 c9 e7 cb f7 84 a6 22 4a 64 eb fa d7 84 a1 d9
ad c7 5d 77 cd 2a 65 79 95 9a d4 5c 22 8c 62 ae
0e fc c8 fd bd c8 4d 66 0d c3 69 d3 c4 cb e8 33
```

```
72 1a f1 cc 31 5f 08 75 65 6b 77 3b 23 c3 b8 74
02 fa 15 6e e4 7a b2 73 17 8f 08 02 20 7e b8 d7
N Next payload: VID, reserved: 0x0, length: 24

87 4d 63 76 cc 10 30 0e 4c 95 40 24 d3 b3 3b f3
44 be 0f e5
```

Поэтому несмотря на то, что клиент передал группы 2,21,20,19,24,14 и 5 (эти совместимые FIPS группы), головной узел все еще только подключает только группу, поддерживающую 2 в политике 1 в предыдущей конфигурации. Эта проблема становится очевидной далее вниз в отладках:

```
IKEv2 received all requested SPIs from CTM to respond to a tunnel request.
IKEv2-PROTO-5: (64): SM Trace-> SA: I_SPI=74572B8D1BEC5873 R_SPI=E4160C492A824B5F
(R) MsgID = 00000006 CurState: R_VERIFY_AUTH Event: EV_OK_RECD_IPSEC_RESP
IKEv2-PROTO-2: (64): Processing IKE_AUTH message
IKEv2-PROTO-1: Tunnel Rejected: Selected IKEv2 encryption algorithm (AES-CBC-192)
is not strong enough to secure proposed IPsec encryption algorithm (AES-GCM-256).
IKEv2-PROTO-1: (64): Failed to find a matching policy
IKEv2-PROTO-1: (64): Received Policies:
ESP: Proposal 1: AES-GCM-256 AES-GCM-192 AES-GCM-128 None Don't use ESN

ESP: Proposal 2: AES-CBC-256 AES-CBC-192 AES-CBC-128 3DES SHA512 SHA384 SHA256 SHA96
Don't use ESN

IKEv2-PROTO-1: (64): Failed to find a matching policy
IKEv2-PROTO-1: (64): Expected Policies:
ESP: Proposal 0: AES-GCM-256 SHA384 Don't use ESN

IKEv2-PROTO-5: (64): Failed to verify the proposed policies
IKEv2-PROTO-1: (64): Failed to find a matching policy
```

Связь прерывается из-за комбинации факторов:

1. С включенным FIPS клиент только передает определенную политику, и те должны совпасть. Среди той политики это только предлагает шифрование Расширенного стандарта шифрования (AES) с размером ключа, больше, чем или равный 256.

2. ASA настроен со множественной политикой IKEv2, две из которой имеет группу 2, включил. Как описано ранее, в этом сценарии, который включила политика, которая имеет группу 2, используется для соединения. Однако алгоритм шифрования на обеих из той политики использует размер ключа 192, который слишком низок для поддерживающего FIPS клиента.

Поэтому в этом случае ASA и клиент ведут себя согласно конфигурации. Существует три способа обойти эту проблему для поддерживающих FIPS клиентов:

1. Настройте только одну политику с точными желаемыми предложениями.

2. Если множественные предложения требуются, не настраивайте один с группой 2; иначе тот будет всегда выбираться.

3. Если группе 2 нужно включить, затем гарантировать, что она имеет правильный настроенный алгоритм шифрования (Aes 256 или aes-gcm-256).