# 啟用FIPS後修復AnyConnect加密演算法錯誤

## 目錄



## 簡介

本文檔說明使用者為什麼不能使用啟用聯邦資訊處理標準(FIPS)的客戶端連線到自適應安全裝置(ASA)，該裝置的策略支援啟用FIPS的加密演算法。

## 背景資訊

在Internet金鑰交換版本2(IKEv2)連線設定期間，發起方從來不知道對等方可以接受哪些提議，因此發起方必須猜測在傳送第一個IKE消息時要使用的Diffie-Hellman(DH)組。用於此猜測的DH組通常是所配置的DH組清單中的第一個DH組。然後，發起方會計算猜測組的關鍵資料，但也會向對等方傳送所有組的完整清單，這將允許對等方在猜測組出錯時選擇不同的DH組。

對於客戶端，沒有使用者配置的IKE策略清單。相反，客戶端支援預先配置的策略清單。因此，為了減少當您使用可能錯誤的組計算第一個消息的關鍵資料時客戶端的計算負載，DH組的清單從最弱到最強。因此，客戶端選擇計算密集度最低的DH並因此選擇資源密集度最低的組進行初始猜測，然後在後續消息中切換到頭端選擇的組。

> **附註**：此行為與將DH組從最強到最弱排序的AnyConnect 3.0版客戶端不同。

但是，在頭端，由客戶端傳送的與網關上配置的DH組匹配的清單上的第一個DH組是選定的組。因此，如果ASA還配置了較弱的DH組，則它使用客戶端支援的最弱的DH組，並且在前端進行配置，儘管兩端都有更安全的DH組。

此行為已通過Cisco錯誤ID CSCub92935在客戶端上修正。所有客戶端版本通過此錯誤的修正將顛倒DH組傳送到頭端時列出的順序。但是，為了避免與非Suite B網關發生向後相容問題，最弱的DH組（一個用於非FIPS模式，兩個用於FIPS模式）仍位於清單頂部。

> **附註**：在清單中的第一個條目（組1或組2）之後，組按從強到弱的順序列出。這把橢圓曲線群排在第一位(21,20,19)，然後是模數指數(MODP)群(24,14,5,2)。

> **提示：**如果網關配置了同一策略中的多個DH組，並且包含組1（或2的FIPS模式），則ASA接受較弱的組。此修複方案僅將DH組1包括在網關上配置的策略中。當在一個策略中配置了多個組，但不包括組1時，將選擇最強組。例如：
>
> — 在將IKEv2策略設定為1 2 5 14 24 19 20 21的ASA 9.0版（套件B）上，**組1按預期**選擇。
>
> — 在將IKEv2策略設定為2 5 14 24 19 20 21的ASA 9.0版（套件B）上，**組21按預期**選擇。

— 在IKEv2策略設定為1 2 5 14 24 19 20 21的ASA 9.0版（套件B）上，客戶端處於FIPS模式，按預期選擇組2。

— 在IKEv2策略設定為5 14 24 19 20 21的ASA 9.0版（套件B）上，測試客戶端處於FIPS模式，按預期選擇組21。

— 在IKEv2策略設定為1 2 5 14的ASA 8.4.4版（非套件B）上，**組1按預期選**擇了。

— 在IKEv2策略設定為2 5 14的ASA 8.4.4版（非套件B）上，**組14按預期選**擇了。

# 問題

ASA配置了以下IKEv2策略：

```
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
```

在此配置中，策略1已明確配置，以支援所有啟用FIPS的加密演算法。但是，當使用者嘗試從啟用了FIPS的客戶端進行連線時，連線將失敗，並顯示以下錯誤消息：

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

但是，如果管理員更改policy1，使其使用DH組2而不是20，則連線將正常工作。

# 解決方案

根據症狀，第一個結論將是當啟用FIPS時客戶端僅支援DH組2，其他任何組均無法工作。這實際上是不正確的。如果在ASA上啟用此調試，您可以看到客戶端傳送的建議：

```
debug crypto ikev2 proto 127
```

在連線嘗試期間，第一個調試消息是：

```
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
```

因此，儘管客戶端傳送了組2、21、20、19、24、14和5（這些與FIPS相容的組），但在以前的配置中，頭端仍然只連線策略1中啟用組2。這一問題在調試階段進一步顯現：

```
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
```

連線失敗的原因包括：

1. 啟用FIPS後，客戶端僅傳送特定策略，這些策略必須匹配。在這些策略中，它只推薦金鑰大小大於或等於256的高級加密標準(AES)加密。

2. ASA配置了多個IKEv2策略，其中兩個策略啟用了組2。如前所述，在此方案中，將啟用組2的策略用於連線。但是，這兩個策略上的加密演算法使用的金鑰大小為192，對於啟用FIPS的客戶端來說該大小太低。

因此，在這種情況下，ASA和客戶端按照配置運行。對於啟用FIPS的客戶端，有三種方法可解決此問題：

1. 僅配置一個具有所需建議書的策略。

2. 如果需要多個建議，不要使用組2配置一個；否則將始終選擇一個。

3. 如果必須啟用組2，請確保其配置了正確的加密演算法（Aes-256或aes-gcm-256）。