当FIP启用时，AnyConnect客户端抱怨不支持的加密算法

目录

[简介](#)
[背景信息](#)
[问题](#)
[解决方案](#)

简介

本文描述用户为什么也许不能连接使用联邦信息处理标准(FIP) -已启用客户端到可适应安全工具(ASA)，有该一项的策略支持FIPS启用的crypto算法。

背景信息

在互联网密钥交换版本2 (IKEv2)连接建立期间，发起者从未知道什么建议由对等体是可接受，因此发起者必须猜测使用的哪Diffie-Hellman (DH)组，当第一个IKE信息发送时。用于此猜测的DH组通常是DH组列表的第一DH组配置。发起者然后计算被猜测的组的关键数据，而且发送所有组完整列表给对等体，允许对等体选择一不同的DH组，如果被猜测的组错误。

在客户端的情况下，没有IKE策略用户配置的列表。反而，有客户端支持策略的一预先配置的列表。因此，为了减少在客户端的计算负载，当您计算第一条消息的关键数据与可能是错误一个的组时，DH组列表从最弱指令到最强。另一方面因此，客户端选择最少计算性强的DH并且最少资源加强组最初的猜测的，但是转换到头端选择的组在随后的消息。

> **注意**：此行为是与AnyConnect定购从最强的DH组到最弱的版本3.0客户端不同。

然而，在头端，配比的客户端发送的列表的第一DH组在网关配置的DH组是选择的组。所以，如果ASA也有更加弱的DH组配置，它使用客户端在尽管一更加安全的DH组可用性的头端支持并且配置两端的最弱的DH组。

此行为在客户端修复通过Cisco Bug ID CSCub92935。所有客户端版本以从此bug的修正倒转DH组是列出的命令，当他们发送对头端时。然而，为了避免向后兼容性问题用非套件B网关，最弱的DH组(一非FIPS模式的和两FIP模式的)依然是在列表顶部。

> **注意**：在列表后的首先进入(group1或2)，组是列出的按照最强的顺序对最弱。这放置首先椭圆曲线组(21， 20， 19)，跟随由模块化指数(MODP)组(24， 14， 5， 2)。

> **提示**：如果网关配置与同一项策略的广泛DH组，并且group1 (或2在FIP模式)包括，则ASA接

受更加弱的组。修正是只包括单独DH group1在网关配置的策略。当多个组在一项策略时配置，但是group1没有包括，然后最强选择。例如：

-在ASA版本9.0 (套件B) IKEv2策略设置到1 2 5 14 24 19 20 21， **group1选择**正如所料。

-在ASA版本9.0 (套件B) IKEv2策略设置到2 5 14 24 19 20 21，**组21选择**正如所料。

-与FIP模式的客户端在ASA版本9.0 (套件B) IKEv2策略设置到1 2 5 14 24 19 20 21，**第2组选择**正如所料。

-与FIP模式的测试客户端在ASA版本9.0 (套件B) IKEv2策略设置到5 14 24 19 20 21，**组21选择**正如所料。

-在ASA版本8.4.4 (非套件B) IKEv2策略设置到1 2 5 14， **group1选择**正如所料。

-在ASA版本8.4.4 (非套件B) IKEv2策略设置到2 5 14，**组14选择**正如所料。

问题

ASA配置与这些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， policy1清楚地配置为了支持所有FIPS启用的加密算法。然而，当用户设法从一个FIPS启用的客户端时连接，连接失效与错误消息：

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

然而，如果admin更改policy1，以便使用DH组2而不是20，连接工作。

解决方案

凭症状，第一个结论是客户端只支持DH组2，当FIP启用时，并且其他都不工作。这实际上不正确。如果启用在ASA的此调试，您能看到客户端发送的建议：

debug crypto ikev2 proto 127

在连接尝试期间，第一个调试消息是：

```
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
```

所以，竟管客户端派了组2,21,20,19,24,14和5 (这些FIPS兼容组)，头端在先前配置里只仍然联络在policy1 2启用的仅组。此问题变为在调试的明显的进一步下来：

```
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
```

连接失效由于要素的组合：

1. 使用启用的FIP，客户端发送特定仅策略和那些必须配比。在那些策略中，它只报价与密钥大小的高级加密标准(AES)加密大于或等于256。

2. ASA配置与多项IKEv2策略，两有启用的第2组。如描述前，在此方案有启用的第2组的策略使用连接。然而，在两个的加密算法那些策略使用密钥大小192，为一个FIPS启用的客户端是太低。

所以，在这种情况下， ASA和客户端根据配置正常运行。有三种方式对应急方案FIPS启用的客户端的此问题：

1. 只配置与希望的确切的建议的一项策略。

2. 如果多个建议要求，请勿配置一与第2组;否则该一个永远将选择。

3. 如果必须启用第2组，则请保证安排正确的加密算法配置(Aes-256或aes-gcm-256)。