修复启用FIPS的AnyConnect加密算法错误

目录

简介

本文档介绍用户无法使用启用联邦信息处理标准(FIPS)的客户端连接到自适应安全设备(ASA)的原因，该设备具有支持启用FIPS的加密算法的策略。

背景信息

在Internet密钥交换版本2(IKEv2)连接设置期间，发起方从不知道对等体可以接受哪些提议，因此发起方必须猜测发送第一条IKE消息时要使用的Diffie-Hellman(DH)组。用于此猜测的DH组通常是配置的DH组列表中的第一个DH组。然后，发起方会计算被猜到组的密钥数据，同时还会向对等体发送所有组的完整列表，这允许对等体在被猜到组错误时选择不同的DH组。

对于客户端，没有用户配置的IKE策略列表。相反，客户端支持预配置的策略列表。因此，为了减少在计算第一个消息的密钥数据时客户端的计算负载，将DH组列表从最弱到最强排序。因此，客户端选择计算密集度最低的DH，并因此选择资源密集度最低的组进行初始猜测，但随后在后续消息中切换到头端选择的组。

> **注意：**此行为与将DH组从最强到最弱排序的AnyConnect 3.0版客户端不同。

但是，在头端上，客户端发送的列表中与网关上配置的DH组匹配的第一个DH组是所选组。因此，如果ASA也配置了较弱的DH组，则它使用客户端支持并在头端上配置的最弱的DH组，尽管两端都有更安全的DH组。

此行为已通过Cisco Bug ID CSCub92935在客户端上修复。所有包含此Bug修复的客户端版本都会改变DH组发送到头端时列出的顺序。但是，为避免非Suite B网关出现向后兼容问题，最弱的DH组（一个用于非FIPS模式，两个用于FIPS模式）仍位于列表顶部。

> **注意：**在列表（组1或组2）中的第一个条目后，按最强到最弱的顺序列出组。这将椭圆曲线组放在第一(21,20,19)位，后跟模指数(MODP)组(24,14,5,2)。

> **提示：**如果网关在同一策略中配置了多个DH组，并且组1（或2在FIPS模式下）包含，则ASA接受弱组。修复是仅将DH组1包含在网关上配置的策略中。当在一个策略中配置多个组，但不包括组1时，将选择最强的组。例如：
>
> — 在ASA 9.0版（套件B）中，IKEv2策略设置为1 2 5 14 24 19 20 21，组**1按预期选**择。
>
> — 在ASA 9.0版（套件B）中，IKEv2策略设置为2 5 14 24 19 20 21，组**21按预期**选择。

— 在ASA 9.0版（套件B）上，客户端处于FIPS模式，IKEv2策略设置为1 2 5 14 24 19 20 21时，组**2将按预期**选择。

— 在ASA 9.0版（套件B）上以FIPS模式测试的客户端，IKEv2策略设置为5 14 24 19 20 21时，组**21将按预期**选择。

— 在ASA 8.4.4版（非套件B）中，IKEv2策略设置为1 2 5 14,**组1按预期**选择。

— 在ASA 8.4.4版（非套件B）中，IKEv2策略设置为2 5 14，组**14按预期**选择。

问题

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已经过清楚配置，以支持所有启用FIPS的加密算法。但是，当用户尝试从启用FIPS的客户端连接时，连接失败并显示错误消息：

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

但是，如果管理员更改策略1，使其使用DH组2而不是20，则连接会正常。

解决方案

根据症状，第一个结论是，当启用FIPS时，客户端仅支持DH组2，而其他组均不工作。这其实不正确。如果在ASA上启用此调试，您可以看到客户端发送的建议：

```
debug crypto ikev2 proto 127
```

在尝试连接期间，第一条调试消息为：

```
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，尽管客户端发送了组2,21,20,19,24,14和5（这些符合FIPS的组），但头端仍然只连接在先前配置中策略1中启用的组2。此问题在调试中进一步明显：

```
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
```

由于以下因素的组合，连接失败：

1. 启用FIPS后，客户端仅发送特定策略，且这些策略必须匹配。在这些策略中，它仅建议密钥大小大于或等于256的高级加密标准(AES)加密。

2. ASA配置了多个IKEv2策略，其中两个已启用组2。如前所述，在此场景中，启用了组2的策略用于连接。但是，这两个策略上的加密算法都使用密钥大小192，对于启用FIPS的客户端而言，该值太低。

因此，在本例中，ASA和客户端的行为与配置相同。对于启用FIPS的客户端，有三种方法可解决此问题：

1. 仅使用所需的确切建议配置一个策略。

2. 如果需要多个建议，请勿使用组2配置一个建议；否则，始终选择一个。

3. 如果必须启用组2，请确保它已配置正确的加密算法（Aes-256或aes-gcm-256）。