FIPSを有効にした場合のAnyConnect暗号化アルゴリズムのエラーの修正

内容

概要

このドキュメントでは、ユーザが連邦情報処理標準(FIPS)対応クライアントを使用して、FIPS対応の暗号化アルゴリズムをサポートするポリシーを持つ適応型セキュリティアプライアンス(ASA)に接続できない場合がある理由について説明します。

背景説明

インターネット キー エクスチェンジ バージョン 2（IKEv2）接続のセットアップ時に、発信側はピアによって受け入れ可能なプロポーザルを認識していることはないため、発信側は最初の IKE メッセージが送信されたときに、使用する Diffie-Hellman（DH）グループを推測する必要があります。この推測に使用される DH グループは、通常、設定された DH グループのリストの最初の DH グループです。発信側では推測したグループのキー データを計算しますが、ピアにすべてのグループの完全なリストも送信します。これにより、ピアではその推測したグループが誤っている場合に、別の DH グループを選択できます。

クライアントの場合、ユーザ設定の IKE ポリシーのリストはありません。代わりに、クライアントでサポートされる事前設定されたポリシーのリストがあります。このため、誤っている可能性のあるグループが含まれた最初のメッセージのキー データを計算する際にクライアント側での計算の負荷を減らすため、DH グループのリストは最も弱いものから最も強いものの順に並べられています。したがって、クライアントでは最初の推測に計算負荷が最も低い DH と、最もリソースを消費しないグループを選択しますが、後続のメッセージではヘッドエンドによって選択されたグループに切り替えます。

> **注**：この動作は、 DH グループが最も強いものから最も弱いものの順に並べられる AnyConnect バージョン 3.0 クライアントとは異なります。

ただし、ヘッドエンド上では、ゲートウェイに設定された DH グループに一致する、クライアントによって送信されたリスト上の最初の DH グループが、選択されるグループです。このため、ASA により弱い DH グループも設定されている場合、両端のより安全性の高い DH グループを利用できるにもかかわらず、クライアントでサポートされ、ヘッドエンド上に設定されている最も弱い DH グループが ASA によって使用されます。

この動作は、Cisco Bug ID CSCub92935でクライアントで修正されています。このバグから修正されたクライアントバージョンでは、すべてヘッドエンドに送信されるDHグループのリスト順序が逆になっています。ただし、非 Suite B のゲートウェイとの後方互換性の問題を避けるために

、最も弱い DH グループ（非 FIPS モードの場合は 1 つ、FIPS モードの場合は 2 つ）がリストの先頭に残ります。

注：リストの最初のエントリ（グループ 1 またはグループ 2）の後に、他のグループが最も強いものから最も弱いものの順にリストされます。これにより、楕円曲線グループが最初に（21、20、19）配置され、その後に Modular Exponential（MODP）グループ（24、14、5、2）が続きます。

ヒント：ゲートウェイが同じポリシーで複数の DH グループで設定され、グループ 1（または FIPS モードの場合、グループ 2）が含まれている場合は、ASA ではより弱いグループを受け入れます。修正では、ゲートウェイに設定されているポリシーに DH グループ 1 だけを含めます。複数のグループを 1 つのポリシーに設定するが、グループ 1 を含めない場合、最も強いグループが選択されます。以下に、いくつかの例を示します。

- ASA バージョン 9.0（Suite B）上で IKEv2 ポリシーが 1 2 5 14 24 19 20 21 に設定されている場合、予期したとおりに**グループ 1 が選択されます。**

- ASA バージョン 9.0（Suite B）上で IKEv2 ポリシーが 2 5 14 24 19 20 21 に設定されている場合、予期したとおりに**グループ 21 が選択されます。**

- クライアントが FIPS モードで、ASA バージョン 9.0（Suite B）上で IKEv2 ポリシーが 1 2 5 14 24 19 20 21 に設定されている場合、予期したとおりに**グループ 2 が選択されます。**

- テストされるクライアントが FIPS モードで、ASA バージョン 9.0（Suite B）上で IKEv2 ポリシーが 5 14 24 19 20 21 に設定されている場合、予期したとおりに**グループ 21 が選択されます。**

- ASA バージョン 8.4.4（非 Suite B）上で IKEv2 ポリシーが 1 2 5 14 に設定されている場合、予期したとおりに**グループ 1 が選択されます。**

- ASA バージョン 8.4.4（非 Suite B）上で IKEv2 ポリシーが 2 5 14 に設定されている場合、予期したとおりに**グループ 14 が選択されます。**

問題

ASA が、以下の IKEv2 ポリシーで設定されています。

```
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
```
この設定では、すべての FIPS 対応暗号化アルゴリズムをサポートするために、ポリシー 1 が明確に設定されています。しかし、ユーザが FIPS 対応クライアントから接続しようとすると、次のエラー メッセージが表示されて接続が失敗します。

```
The cryptographic algorithms required by the secure gateway do not match those supported by
AnyConnect.
Please contact your network administrator.
```
一方、管理者がポリシー 1 で DH グループ 20 ではなく、DH グループ 2 を使用するように変更すると、この接続は機能します。

解決方法

症状に基づくと、最初の推論は、FIPS が有効になっていて他になにも動作していない場合はクライアントで DH グループ 2 しかサポートしていないということになります。これは、実際には正しくありません。ASA 上で次の debug を有効にすると、クライアントから送信されたプロポーザルを確認できます。

```
debug crypto ikev2 proto 127
```
接続の試行中、最初の debug のメッセージは次のとおりです。

```
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
```

したがって、クライアントがグループ 2、21、20、19、24、14 および 5 (これらの FIPS 準拠グ

ループ）を送信したという事実にもかかわらず、ヘッドエンドでは依然として以前の設定のポリシー 1 で有効なグループ 2 のみに接続しているだけです。この問題は、debug のメッセージをさらに確認していくと明らかになります。

```
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
```

この接続の失敗は、次の要素の組み合わせに起因します。

1. FIPS を有効にすると、クライアントでは特定のポリシーを送信するだけで、それらは一致する必要があります。それらのポリシーのうち、クライアントではキー サイズが 256 以上の Advanced Encryption Standard（AES）暗号化だけを提示します。

2. ASA は複数の IKEv2 ポリシーで設定され、その内の 2 つでグループ 2 が有効にされています。上述のように、このシナリオではグループ 2 が有効にされているポリシーが接続に使用されます。ただし、これらのポリシーのどちらの暗号化アルゴリズムでも、FIPS 対応クライアントには低すぎるキー サイズの 192 が使用されます。

したがって、この場合、ASA とクライアントはこの設定に従って動作します。FIPS 対応クライアントに対して、この問題を回避する方法は、次の 3 つがあります。

1. 必要なプロポーザルだけを保持する 1 つのポリシーのみを設定します。

2. 複数のプロポーザルが必要な場合は、グループ 2 を保持するポリシーを設定しません。それ以外の場合は、常に選択されます。

3. グループ 2 を有効にする必要がある場合は、そのグループに適切な暗号化アルゴリズム（AES-256 または AES-GCM-256）が設定されるようにしてください。