Résolution des erreurs d'algorithmes de chiffrement AnyConnect avec FIPS activé

Contenu

Introduction

Ce document décrit pourquoi les utilisateurs ne peuvent pas se connecter à un appareil de sécurité adaptatif (ASA) avec l'utilisation d'un client FIPS (Federal Information Processing Standard), qui a une politique qui prend en charge les algorithmes de chiffrement FIPS.

Informations générales

Lors de la configuration d'une connexion Internet Key Exchange Version 2 (IKEv2), l'initiateur ne sait jamais quelles propositions sont acceptables par l'homologue. L'initiateur doit donc deviner quel groupe Diffie-Hellman (DH) utiliser lors de l'envoi du premier message IKE. Le groupe DH utilisé pour cette estimation est généralement le premier groupe DH de la liste des groupes DH configurés. L'initiateur calcule ensuite les données de clé pour les groupes devinés mais envoie également une liste complète de tous les groupes à l'homologue, ce qui permet à l'homologue de sélectionner un autre groupe DH si le groupe deviné est incorrect.

Dans le cas d'un client, il n'existe aucune liste de stratégies IKE configurée par l'utilisateur. Au lieu de cela, il existe une liste préconfigurée de stratégies prises en charge par le client. Pour cette raison, afin de réduire la charge de calcul sur le client lorsque vous calculez les données de clé pour le premier message avec un groupe qui est peut-être le mauvais, la liste des groupes DH a été ordonnée du plus faible au plus fort. Ainsi, le client choisit le groupe DH le moins gourmand en ressources informatiques et donc le groupe le moins gourmand en ressources pour l'estimation initiale, puis passe au groupe choisi par la tête de réseau dans les messages suivants.

> **Note**: Ce comportement est différent des clients AnyConnect version 3.0 qui ont ordonné aux groupes DH de passer du plus fort au plus faible.

Cependant, sur la tête de réseau, le premier groupe DH de la liste envoyée par le client qui correspond à un groupe DH configuré sur la passerelle est le groupe sélectionné. Par conséquent, si l'ASA a également des groupes DH plus faibles configurés, il utilise le groupe DH le plus faible qui est pris en charge par le client et configuré sur la tête de réseau malgré la disponibilité d'un groupe DH plus sécurisé aux deux extrémités.

Ce comportement a été corrigé sur le client via l'ID de bogue Cisco CSCub92935. Toutes les versions clientes avec la correction de ce bogue annulent l'ordre dans lequel les groupes DH sont listés lorsqu'ils sont envoyés à la tête de réseau. Cependant, afin d'éviter un problème de

rétrocompatibilité avec les passerelles non Suite B, le groupe DH le plus faible (un pour le mode non FIPS et deux pour le mode FIPS) reste en haut de la liste.

> **Note**: Après la première entrée de la liste (groupe 1 ou 2), les groupes sont classés par ordre de plus forte à plus faible. Ceci place les groupes de courbes elliptiques en premier (21, 20, 19), suivi des groupes MODP (Modular Exponential) (24, 14, 5, 2).

> **Astuce** : Si la passerelle est configurée avec plusieurs groupes DH dans la même stratégie et que le groupe 1 (ou 2 en mode FIPS) est inclus, l'ASA accepte le groupe le plus faible. La correction consiste à inclure uniquement le groupe DH 1 dans une stratégie configurée sur la passerelle. Lorsque plusieurs groupes sont configurés dans une stratégie, mais que le groupe 1 n'est pas inclus, le groupe le plus fort est sélectionné. Exemple :
>
> - Sur ASA version 9.0 (suite B) avec la stratégie IKEv2 définie sur 1 2 5 14 24 19 20 21, **le groupe 1 est sélectionné** comme prévu.
>
> - Sur ASA version 9.0 (suite B) avec la stratégie IKEv2 définie sur 2 5 14 24 19 20 21, **le groupe 21 est sélectionné** comme prévu.
>
> - Avec le client en mode FIPS sur ASA version 9.0 (suite B) avec la stratégie IKEv2 définie sur 1 2 5 14 24 19 20 21, **le groupe 2 est sélectionné** comme prévu.
>
> - Avec le client testé en mode FIPS sur ASA version 9.0 (suite B) avec la stratégie IKEv2 définie sur 5 14 24 19 20 21, **le groupe 21 est sélectionné** comme prévu.
>
> - Sur ASA version 8.4.4 (non-suite B) avec la stratégie IKEv2 définie sur 1 2 5 14, **le groupe 1 est sélectionné** comme prévu.
>
> - Sur ASA version 8.4.4 (non-suite B) avec la stratégie IKEv2 définie sur 2 5 14, **le groupe 14 est sélectionné** comme prévu.

Problème

L'ASA est configuré avec les stratégies IKEv2 suivantes :

```
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
```

Dans cette configuration, la stratégie 1 est clairement configurée afin de prendre en charge tous les algorithmes cryptographiques compatibles FIPS. Cependant, lorsqu'un utilisateur tente de se connecter à partir d'un client FIPS, la connexion échoue avec le message d'erreur :

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

Cependant, si l'administrateur modifie policy1 de sorte qu'il utilise le groupe DH 2 au lieu de 20, la connexion fonctionne.

Solution

En fonction des symptômes, la première conclusion serait que le client ne prend en charge que le groupe DH 2 lorsque le FIPS est activé et qu'aucun des autres ne fonctionne. C'est en fait incorrect. Si vous activez ce débogage sur l'ASA, vous pouvez voir les propositions envoyées par le client :

debug crypto ikev2 proto 127

Lors d'une tentative de connexion, le premier message de débogage est :

```
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
```

Par conséquent, malgré le fait que le client ait envoyé les groupes 2,21,20,19,24,14 et 5 (ces groupes compatibles FIPS), la tête de réseau ne connecte toujours que le groupe 2 activé dans la stratégie 1 dans la configuration précédente. Ce problème apparaît plus bas dans les débogages :

```
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
```

La connexion échoue en raison d'une combinaison de facteurs :

1. Lorsque FIPS est activé, le client envoie uniquement des stratégies spécifiques et celles-ci doivent correspondre. Parmi ces politiques, elle propose uniquement le chiffrement AES (Advanced Encryption Standard) avec une taille de clé supérieure ou égale à 256.

2. L'ASA est configuré avec plusieurs stratégies IKEv2, dont deux ont le groupe 2 activé. Comme décrit précédemment, dans ce scénario, la stratégie dont le groupe 2 est activé est utilisée pour la connexion. Cependant, l'algorithme de chiffrement de ces deux stratégies utilise une taille de clé de 192, ce qui est trop faible pour un client FIPS.

Par conséquent, dans ce cas, l'ASA et le client se comportent conformément à la configuration. Il existe trois façons de résoudre ce problème pour les clients FIPS :

1. Configurez une seule stratégie avec les propositions exactes souhaitées.

2. Si plusieurs propositions sont nécessaires, ne configurez pas une avec le groupe 2 ; sinon, celle-ci est toujours sélectionnée.

3. Si le groupe 2 doit être activé, assurez-vous qu'il a l'algorithme de chiffrement approprié configuré (Aes-256 ou aes-gcm-256).