Le client d'AnyConnect se plaint au sujet des algorithmes de chiffrement sans support quand des PAP est activées

Contenu

Introduction

Ce document décrit pourquoi les utilisateurs ne pourraient pas pouvoir se connecter à l'utilisation d'une Norme fédérale pour le traitement de l'information (PAP) - client activé à une appliance de sécurité adaptable (ASA), qui a une stratégie qui prend en charge de cryptos algorithmes PAP-activés.

Informations générales

Pendant une configuration de connexion de la version 2 d'échange de clés Internet (IKE) (IKEv2), le demandeur ne se rend jamais compte de quelles propositions sont acceptables par le pair, ainsi le demandeur doit deviner qui groupe de Protocole DH (Diffie-Hellman) à l'utiliser quand le premier message d'IKE est envoyé. Le groupe CAD utilisé pour cette conjecture est habituellement le premier groupe CAD dans la liste de groupes CAD configurés. Le demandeur calcule alors les données principales pour les groupes devinés mais envoie également une liste complète de tous les groupes au pair, qui permet au pair pour sélectionner un groupe différent CAD si le groupe deviné a tort.

En cas de client, il n'y a aucune liste utilisateur-configurée de stratégies IKE. Au lieu de cela, il y a une liste préconfigurée de stratégies que le client prend en charge. Pour cette raison, afin de réduire le volume des calculs sur le client quand vous calculez les données principales pour le premier message avec un groupe qui est probablement le faux, la liste de groupes CAD a été commandée de plus faible à plus fort. Ainsi, le client choisit le moins CAD comportant de nombreux calculs et donc le moins groupe ressource-intensif pour la conjecture initiale, mais d'autre part s'oriente vers le groupe choisi par le headend dans les messages ultérieurs.

> Remarque: Ce comportement est différent des clients de version 3.0 d'AnyConnect qui ont commandé les groupes CAD de plus fort à plus faible.

Cependant, sur le headend, le premier groupe CAD sur la liste envoyée par le client qui est assorti

un groupe configuré CAD sur la passerelle est le groupe qui est sélectionné. Par conséquent, si l'ASA a également des groupes plus faibles CAD configurés, il utilise le groupe CAD le plus faible qui est pris en charge par le client et davantage configuré sur le headend en dépit de la Disponibilité d'un groupe CAD de sécuriser sur les deux extrémités.

Ce comportement a été réparé sur le client par l'ID de bogue Cisco CSCub92935. Toutes les versions du client avec la difficulté de cette bogue renversent la commande dans laquelle des groupes CAD sont répertoriés quand ils sont envoyés au headend. Cependant, afin d'éviter une question de vers l'arrière-compatibilité avec des passerelles de la non-suite B, le groupe CAD le plus faible (un pour mode non-PAP et deux pour le mode PAP) demeure en haut de la liste.

> Remarque: Après que la première entrée dans la liste (le groupe 1 ou 2), les groupes sont répertoriés par ordre plus fort à plus faible. Ceci met les groupes elliptiques de curve d'abord (21, 20, 19), suivi des groupes (MODP) exponentiels modulaires (24, 14, 5, 2).

> **Conseil** : Si la passerelle est configurée avec de plusieurs groupes CAD dans la même stratégie et le groupe 1 (ou 2 en mode PAP) est inclus, alors l'ASA reçoit le groupe plus faible. La difficulté est seul d'inclure seulement le groupe 1 CAD dans une stratégie configurée sur la passerelle. Quand de plusieurs groupes sont configurés dans une stratégie, mais le groupe 1 n'est pas inclus, alors le plus fort est sélectionné. Exemple :
>
> - Sur la version 9.0 ASA (la suite B) avec la stratégie IKEv2 réglée à 1 2 5 14 24 19 20 21, le **groupe 1 est sélectionnée** comme prévue.
>
> - Sur la version 9.0 ASA (la suite B) avec la stratégie IKEv2 réglée à 2 5 14 24 19 20 21, le **groupe 21 est sélectionnée** comme prévue.
>
> - Avec le client en mode PAP sur la version 9.0 ASA (la suite B) avec la stratégie IKEv2 réglée à 1 2 5 14 24 19 20 21, le **groupe 2 est sélectionnée** comme prévue.
>
> - Avec le client examiné en mode PAP sur la version 9.0 ASA (la suite B) avec la stratégie IKEv2 réglée à 5 14 24 19 20 21, le **groupe 21 est sélectionnée** comme prévue.
>
> - Sur la version 8.4.4 ASA (la non-suite B) avec la stratégie IKEv2 réglée à 1 2 5 14, le **groupe 1 est sélectionnée** comme prévue.
>
> - Sur la version 8.4.4 ASA (la non-suite B) avec la stratégie IKEv2 réglée à 2 5 14, le **groupe 14 est sélectionnée** comme prévue.

Problème

L'ASA est configurée avec ces stratégies IKEv2 :

```
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 de chiffrement PAP-activés. Cependant, quand les essais d'un utilisateur à connecter d'un client PAP-activé, 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'admin change policy1 de sorte qu'il utilise le groupe 2 CAD au lieu de 20, la connexion fonctionne.

Solution

Basé sur les symptômes, la première conclusion serait que le client prend en charge seulement le groupe 2 CAD quand des PAP est activées et aucune des autres ne fonctionne. C'est réellement incorrect. Si vous activez ceci mettez au point sur l'ASA, vous peut voir les propositions envoyées par le client :

debug crypto ikev2 proto 127

Pendant 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 envoyé les groupes 2,21,20,19,24,14 et 5 (ces groupes PAP-conformes), le headend connecte toujours seulement seulement le groupe 2-enabled dans la stratégie 1 dans la configuration précédente. Ce problème devient autre bas évident dans met au point :

```
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 des facteurs :

1. Les PAP étant activé, le client envoie seulement des stratégies spécifiques et ceux doivent s'assortir. Parmi ces stratégies, il propose seulement le cryptage de Norme AES (Advanced Encryption Standard) avec une taille de clé supérieur ou égal à 256.

2. L'ASA est configurée avec les plusieurs stratégies IKEv2, deux dont ayez le groupe 2 activé. Comme décrit plus tôt, dans ce scénario que la stratégie qui a le groupe 2 a activé est utilisé pour la connexion. Cependant, l'algorithme de chiffrement sur chacun des deux ces stratégies utilise une taille de clé de 192, qui est si basse pour un client PAP-activé.

Par conséquent, dans ce cas, l'ASA et le client se comportent selon la configuration. Il y a trois manières au contournement ce problème pour les clients PAP-activés :

1. Configurez seulement une stratégie avec les propositions précises désirées.

2. Si de plusieurs propositions sont exigées, ne configurez pas un avec le groupe 2 ; autrement celui-là sera toujours sélectionné.

3. Si le groupe 2 doit être activé, alors assurez-vous qu'il fait configurer le bon algorithme de chiffrement (Aes-256 ou aes-gcm-256).