El cliente de AnyConnect se queja por los algoritmos criptográficos sin apoyo cuando se habilitan los FIP

Contenido

Introducción

Este documento describe porqué los usuarios no pudieron poder conectar con el uso de un Estándar de procesamiento de la información federal (FIP) - cliente habilitado a un dispositivo de seguridad adaptante (ASA), que tiene una directiva que soporte los algoritmos de cifrado FIP-habilitados.

Antecedentes

Durante una configuración de conexión del intercambio de claves de Internet versión 2 (IKEv2), el iniciador nunca es consciente de qué ofertas son aceptables por el par, así que el iniciador debe conjeturar qué grupo del Diffie-Hellman (DH) a utilizar cuando se envía el primer mensaje IKE. El grupo DH usado para esta conjetura es generalmente el primer grupo DH en la lista de grupos DH configurados. El iniciador entonces computa los datos clave para los grupos conjeturados pero también envía una lista completa de todos los grupos al par, que permite que el par seleccione a un diverso grupo DH si el grupo conjeturado es incorrecto.

En caso de un cliente, no hay lista del usuario configurado de políticas IKE. En lugar, hay una lista preconfigurada de directivas que los soportes de cliente. Debido a esto, para reducir la carga de cómputo en el cliente cuando usted calcula los datos clave para el primer mensaje con un grupo que sea posiblemente el incorrecto, la lista de grupos DH fue pedida de la más débil a la más fuerte. Así, el cliente elige el menos DH de cómputo-intensivo y por lo tanto el menos grupo del uso intensivo de recurso para la conjetura inicial, pero por otra parte el Switches encima al grupo elegido por el headend en los mensajes subsiguientes.

> Nota: Este comportamiento es diferente de los clientes de la versión 3.0 de AnyConnect que pidieron a los grupos DH de la más fuerte a la más débil.

Sin embargo, en el headend, el primer grupo DH en la lista enviada por el cliente que hace juego un grupo DH configurado en el gateway es el grupo se selecciona que. Por lo tanto, si el ASA

también tiene grupos más débiles DH configurados, utiliza al grupo más débil DH que es soportado por el cliente y configurado en el headend a pesar de la Disponibilidad de un grupo más seguro DH en los ambos extremos.

Este comportamiento fue reparado en el cliente con el Id. de bug Cisco CSCub92935. Todas las versiones de cliente con el arreglo de este bug invierten la orden en la cual los grupos DH son mencionados cuando les envían al headend. Sin embargo, para evitar un problema de la al revés-compatibilidad con los gatewayes de la NON-habitación B, sigue habiendo el grupo más débil DH (uno para el modo NON-FIP y dos para el modo FIP) en la cima de la lista.

> Nota: Después de la primera entrada en la lista (el group1 o 2), los grupos es mencionado en orden de la más fuerte a la más débil. Esto pone los grupos elípticos de la curva primero (21, 20, 19), seguido por los grupos exponenciales modulares (MODP) (24, 14, 5, 2).

> Consejo: Si el gateway se configura con los grupos múltiples DH en la misma directiva y el group1 (o 2 en el modo FIP) es incluidos, después el ASA valida al grupo más débil. El arreglo es incluir solamente el group1 DH solamente en una directiva configurada en el gateway. Cuando configuran a los múltiples grupos en una directiva, pero el group1 no es incluido, después se selecciona el más fuerte. Por ejemplo:
>
> - En la Versión de ASA 9.0 (la habitación B) con la directiva IKEv2 fijada a 1 2 5 14 24 19 20 21, **group1 se selecciona** como se esperaba.
>
> - En la Versión de ASA 9.0 (la habitación B) con la directiva IKEv2 fijada a 2 5 14 24 19 20 21, el **grupo 21 se selecciona** como se esperaba.
>
> - Con el cliente en el modo FIP en la Versión de ASA 9.0 (la habitación B) con la directiva IKEv2 fijada a 1 2 5 14 24 19 20 21, **group2 se selecciona** como se esperaba.
>
> - Con el cliente probado en el modo FIP en la Versión de ASA 9.0 (la habitación B) con la directiva IKEv2 fijada a 5 14 24 19 20 21, el **grupo 21 se selecciona** como se esperaba.
>
> - En la Versión de ASA 8.4.4 (la NON-habitación B) con la directiva IKEv2 fijada a 1 2 5 14, **group1 se selecciona** como se esperaba.
>
> - En la Versión de ASA 8.4.4 (la NON-habitación B) con la directiva IKEv2 fijada a 2 5 14, el **grupo 14 se selecciona** como se esperaba.

Problema

El ASA se configura con estas directivas 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
```

En esta configuración, la directiva 1 se configura claramente para soportar todos los algoritmos criptográficos FIP-habilitados. Sin embargo, cuando un usuario intenta conectar de un cliente FIP-habilitado, la conexión falla con el mensaje de error:

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

Sin embargo, si el admin cambia policy1 de modo que utilice grupo 2 DH en vez de 20, la conexión trabaja.

Solución

De acuerdo con los síntomas, la primera conclusión sería que los soportes del cliente solamente grupo 2 DH cuando se habilitan los FIP y ningunos de los otros trabajan. Esto es realmente incorrecto. Si usted habilita este debug en el ASA, usted puede ver las ofertas enviadas por el cliente:

debug crypto ikev2 proto 127

Durante un intento de conexión, el primer mensaje del debug es:

```
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
```

Por lo tanto, a pesar de que el cliente enviado los grupos 2,21,20,19,24,14 y 5 (estos grupos FIP-obedientes), el headend todavía conecta solamente solamente el grupo 2-enabled en la directiva 1 en la configuración previa. Este problema se convierte en plumón posterior evidente en los debugs:

```
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 conexión falla debido a una combinación de factores:

1. Con los FIP habilitados, el cliente envía solamente las directivas específicas y ésas deben hacer juego. Entre esas directivas, propone solamente el cifrado del Advanced Encryption Standard (AES) con un tamaño de clave mayor o igual un 256.

2. El ASA se configura con las directivas múltiples IKEv2, dos cuyo tenga group2 habilitado. Según lo descrito anterior, en este escenario que la directiva que tiene group2 habilitado está utilizada para la conexión. Sin embargo, el algoritmo de encripción en ambas directivas utiliza un tamaño de clave de 192, que es demasiado bajo para un cliente FIP-habilitado.

Por lo tanto, en este caso, el ASA y el cliente se comportan según la configuración. Hay tres maneras a la solución alternativa este problema para los clientes FIP-habilitados:

1. Configure solamente una directiva con las ofertas exactas deseadas.

2. Si se requieren las ofertas múltiples, no configure uno con el group2; si no aquél será seleccionado siempre.

3. Si el group2 debe ser habilitado, después asegúrese de que haga el algoritmo de encripción correcto configurar (Aes-256 o aes-gcm-256).