Error al corregir los algoritmos criptográficos de AnyConnect con FIPS habilitado

Contenido

Introducción

Este documento describe por qué los usuarios no pueden conectarse con un cliente habilitado para Federal Information Processing Standard (FIPS) a un dispositivo de seguridad adaptable (ASA), que tiene una política que admite algoritmos de cifrado habilitados para FIPS.

Antecedentes

Durante una conexión de Intercambio de claves de Internet versión 2 (IKEv2) configurada, el iniciador nunca sabe qué propuestas son aceptables para el par, por lo que el iniciador debe adivinar qué grupo Diffie-Hellman (DH) utilizar cuando se envía el primer mensaje IKE. El grupo DH utilizado para esta suposición suele ser el primer grupo DH de la lista de grupos DH configurados. A continuación, el iniciador calcula los datos clave de los grupos adivinados, pero también envía una lista completa de todos los grupos al par, lo que permite al par seleccionar un grupo DH diferente si el grupo adivinado es incorrecto.

En el caso de un cliente, no hay una lista configurada por el usuario de las políticas IKE. En su lugar, hay una lista preconfigurada de políticas que admite el cliente. Debido a esto, para reducir la carga computacional en el cliente cuando calcula los datos clave para el primer mensaje con un grupo que posiblemente sea el incorrecto, la lista de grupos DH se ordenó de lo más débil a lo más fuerte. Por lo tanto, el cliente elige el DH con menor densidad computacional y, por lo tanto, el grupo con menor densidad de recursos para la estimación inicial, pero luego pasa al grupo elegido por el encabezado en los mensajes posteriores.

> **Nota:** Este comportamiento es diferente al de los clientes de AnyConnect versión 3.0 que ordenaron a los grupos DH de los más fuertes a los más débiles.

Sin embargo, en la cabecera, el primer grupo DH de la lista enviado por el cliente que coincide con un grupo DH configurado en la gateway es el grupo seleccionado. Por lo tanto, si el ASA también tiene grupos DH más débiles configurados, utiliza el grupo DH más débil que es soportado por el cliente y configurado en la cabecera a pesar de la disponibilidad de un grupo DH más seguro en ambos extremos.

Este comportamiento se corrigió en el cliente a través del ID de bug de Cisco CSCub92935. Todas las versiones de cliente con la corrección de este error invierten el orden en que se enumeran los grupos DH cuando se envían a la cabecera. Sin embargo, para evitar un problema

de compatibilidad con versiones anteriores con gateways no Suite B, el grupo DH más débil (uno para el modo no FIPS y dos para el modo FIPS) permanece en la parte superior de la lista.

Nota: Después de la primera entrada de la lista (grupo 1 ó 2), los grupos se enumeran en orden de mayor a menor. Esto coloca los grupos de curva elíptica primero (21, 20, 19), seguido por los grupos Exponenciales Modulares (MODP) (24, 14, 5, 2).

Consejo: Si la puerta de enlace está configurada con varios grupos DH en la misma política y se incluye el grupo 1 (o 2 en el modo FIPS), el ASA acepta el grupo más débil. La solución es incluir sólo el grupo DH 1 en una política configurada en el gateway. Cuando se configuran varios grupos en una política, pero no se incluye el grupo 1, se selecciona la más fuerte. Por ejemplo:

- En ASA versión 9.0 (suite B) con la política IKEv2 establecida en 1 2 5 14 24 19 20 21, el **grupo 1 se selecciona** como se espera.

- En ASA versión 9.0 (suite B) con la política IKEv2 establecida en 2 5 14 24 19 20 21, el **grupo 21 se selecciona** como se espera.

- Con el cliente en modo FIPS en ASA versión 9.0 (suite B) con la política IKEv2 establecida en 1 2 5 14 24 19 20 21, el **grupo 2 se selecciona** como se espera.

- Con el cliente probado en modo FIPS en ASA versión 9.0 (suite B) con la política IKEv2 establecida en 5 14 24 19 20 21, el **grupo 21 se selecciona** como se espera.

- En ASA versión 8.4.4 (no suite B) con la política IKEv2 establecida en 1 2 5 14, el **grupo 1 se selecciona** como se espera.

- En ASA versión 8.4.4 (no suite B) con la política IKEv2 establecida en 2 5 14, el **grupo 14 se selecciona** como se esperaba.

Problema

El ASA se configura con estas políticas 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 política 1 está claramente configurada para soportar todos los algoritmos criptográficos habilitados para FIPS. Sin embargo, cuando un usuario intenta conectarse desde un cliente habilitado para FIPS, 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 administrador cambia policy1 para que utilice el grupo DH 2 en lugar de 20, la conexión funciona.

Solución

En base a los síntomas, la primera conclusión sería que el cliente sólo admite el grupo DH 2 cuando FIPS está habilitado y ninguno de los otros funcionan. Esto es realmente incorrecto. Si habilita este debug en el ASA, puede ver las propuestas enviadas por el cliente:

```
debug crypto ikev2 proto 127
```

Durante un intento de conexión, el primer mensaje de depuración 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 del hecho de que el cliente envió a los grupos 2,21,20,19,24,14 y 5 (estos grupos compatibles con FIPS), la cabecera todavía conecta solamente el grupo 2 habilitado en la política 1 de la configuración anterior. Este problema se hace evidente más abajo en las depuraciones:

```
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 FIPS habilitado, el cliente sólo envía políticas específicas y éstas deben coincidir. Entre estas políticas, solo propone cifrado de estándar de cifrado avanzado (AES) con un tamaño de clave superior o igual a 256.

2. El ASA se configura con varias políticas IKEv2, dos de las cuales tienen habilitado el grupo 2. Como se ha descrito anteriormente, en este escenario se utiliza para la conexión la política que tiene activado el grupo 2. Sin embargo, el algoritmo de cifrado de ambas políticas utiliza un tamaño de clave de 192, que es demasiado bajo para un cliente habilitado para FIPS.

Por lo tanto, en este caso, el ASA y el cliente se comportan según la configuración. Existen tres formas de solucionar este problema para los clientes habilitados para FIPS:

1. Configure sólo una política con las propuestas exactas deseadas.

2. Si se requieren varias propuestas, no configure una con el grupo 2; de lo contrario, siempre se seleccionará uno.

3. Si se debe habilitar el grupo 2, asegúrese de que tiene el algoritmo de cifrado correcto configurado (Aes-256 o aes-gcm-256).