O cliente de AnyConnect queixa-se sobre algoritmos criptográficos Unsupported quando os FIP são permitidos

Índice

Introdução

Este documento descreve porque os usuários não puderam poder conectar com o uso de um padrão de processamento de informação federal (FIP) - cliente permitido a uma ferramenta de segurança adaptável (ASA), que tenha uma política que apoie algoritmos de criptografia FIP-permitidos.

Informações de Apoio

Durante uma instalação de conexão da versão 2 do intercâmbio de chave de Internet (IKEv2), o iniciador está nunca ciente de que propostas são aceitáveis pelo par, assim que o iniciador deve supor que grupo do Diffie-Hellman (DH) a se usar quando o primeiro mensagem IKE é enviado. O grupo DH usado para esta suposição é geralmente o primeiro grupo DH na lista de grupos DH configurados. O iniciador computa então dados-chave para os grupos supostos mas igualmente envia uma lista completa de todos os grupos ao par, que permite que o par selecione um grupo diferente DH se o grupo suposto é errado.

Em caso de um cliente, não há nenhuma lista do configurado pelo usuário de políticas de IKE. Em lugar de, há uma lista preconfigured de políticas que os suportes ao cliente. Devido a isto, a fim reduzir a carga computacional no cliente quando você calcula os dados-chave para a primeira mensagem com um grupo que fosse possivelmente errado, a lista de grupos DH foi pedida de mais fraco a mais forte. Assim, o cliente escolhe menos DH computacional-intensivo e consequentemente menos grupo dos recursos intensivos para a suposição inicial, mas por outro lado comuta-os sobre ao grupo escolhido pelo final do cabeçalho nos mensagens subsequente.

> Nota: Este comportamento é diferente dos clientes da versão 3.0 de AnyConnect que pediram os grupos DH de mais forte a mais fraco.

Contudo, no final do cabeçalho, o primeiro grupo DH na lista enviou pelo cliente que combina um grupo DH configurado no gateway é o grupo que é selecionado. Consequentemente, se o ASA

igualmente tem uns grupos mais fracos DH configurados, usa o grupo o mais fraco DH que é apoiado pelo cliente e configurado no final do cabeçalho apesar da Disponibilidade de um grupo mais seguro DH no ambas as extremidades.

Este comportamento foi fixado no cliente com a identificação de bug Cisco CSCub92935. Todas as versões de cliente com o reparo deste erro invertem a ordem em que os grupos DH estão listados quando são enviados ao final do cabeçalho. Contudo, a fim evitar uma para trás-compatibilidade emita com os gateways da NON-série B, as sobras as mais fracas do grupo DH (um para o modo NON-FIP e dois para o modo FIP) na parte superior da lista.

> Nota: Após a primeira entrada na lista (grupo1 ou 2), os grupos estão listados por ordem de mais forte a mais fraco. Isto põe os grupos elípticos da curva primeiramente (21, 20, 19), seguido (MODP) pelos grupos exponenciais modulares (24, 14, 5, 2).

> Dica: Se o gateway está configurado com grupos múltiplos DH na mesma política e o grupo1 (ou 2 no modo FIP) são incluído, a seguir o ASA aceita o grupo mais fraco. O reparo é incluir somente o grupo1 DH apenas em uma política configurada no gateway. Quando os grupos múltiplos estão configurados em uma política, mas o grupo1 não é incluído, a seguir o mais forte está selecionado. Por exemplo:
>
> - Na versão ASA 9.0 (a série B) com a política IKEv2 ajustada a 1 2 5 14 24 19 20 21, **grupo1 é selecionada** como esperado.
>
> - Na versão ASA 9.0 (a série B) com a política IKEv2 ajustada a 2 5 14 24 19 20 21, o **grupo 21 é selecionada** como esperado.
>
> - Com o cliente no modo FIP na versão ASA 9.0 (a série B) com a política IKEv2 ajustada a 1 2 5 14 24 19 20 21, **grupo2 é selecionada** como esperado.
>
> - Com o cliente testado no modo FIP na versão ASA 9.0 (a série B) com a política IKEv2 ajustada a 5 14 24 19 20 21, o **grupo 21 é selecionada** como esperado.
>
> - Na versão ASA 8.4.4 (a NON-série B) com a política IKEv2 ajustada a 1 2 5 14, **grupo1 é selecionada** como esperado.
>
> - Na versão ASA 8.4.4 (a NON-série B) com a política IKEv2 ajustada a 2 5 14, o **grupo 14 é selecionada** como esperado.

Problema

O ASA é configurado com 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
```

Nesta configuração, a política 1 é configurada claramente a fim apoiar todos os algoritmos criptográficos FIP-permitidos. Contudo, quando um usuário tenta conectar de um cliente FIP-permitido, a conexão falha com o Mensagem de Erro:

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

Contudo, se o admin muda policy1 de modo que use o grupo 2 DH em vez de 20, a conexão trabalha.

Solução

Baseado nos sintomas, a primeira conclusão seria que o cliente apoia somente o grupo 2 DH quando os FIP são permitidos e nenhuma do outro trabalha. Isto está realmente incorreto. Se você permite este debugar no ASA, você pode ver as propostas enviadas pelo cliente:

debug crypto ikev2 proto 127

Durante uma tentativa de conexão, o primeiros debugam a mensagem são:

```
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
```

Consequentemente, apesar do fato de que o cliente enviado os grupos 2,21,20,19,24,14 e 5 (estes grupos FIP-complacentes), o final do cabeçalho ainda conecta somente somente o grupo 2-enabled na política 1 na configuração precedente. Este problema transforma-se pena mais adicional evidente no debuga:

```
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
```

A conexão falha devido a uma combinação de fatores:

1. Com os FIP permitidos, o cliente envia somente políticas específicas e aquelas devem combinar. Entre aquelas políticas, propõe somente a criptografia do Advanced Encryption Standard (AES) com um tamanho chave superior ou igual a um 256.

2. O ASA é configurado com políticas IKEv2 múltiplas, dois de que tenha o grupo2 permitido. Como descrito mais cedo, nesta encenação que a política que tem grupo2 permitido é usada para a conexão. Contudo, o algoritmo de criptografia em ambas aquelas políticas usa um tamanho chave de 192, que seja demasiado baixo para um cliente FIP-permitido.

Consequentemente, neste caso, o ASA e o cliente comportam-se conforme a configuração. Há três maneiras à ação alternativa este problema para clientes FIP-permitidos:

1. Configurar somente uma política com as propostas exatas desejadas.

2. Se as propostas múltiplas são exigidas, não configurar um com grupo2; se não esse será selecionado sempre.

3. Se o grupo2 deve ser permitido, a seguir assegure-se de que tenha o algoritmo de criptografia direito configurado (Aes-256 ou aes-gcm-256).