# Fix AnyConnect cryptografische algoritmes fout met FIPS-enabled

## Inhoud



## Inleiding

Dit document beschrijft waarom gebruikers misschien niet in staat zijn om verbinding te maken met het gebruik van een FIPS (Federal Information Processing Standards)-enabled client voor een adaptieve security applicatie (ASA), die een beleid heeft dat FIPS-enabled crypto algoritmen ondersteunt.

## Achtergrondinformatie

Tijdens een verbinding van Internet Key Exchange, versie 2 (IKEv2), is de initiator zich nooit bewust van welke voorstellen door de peer worden geaccepteerd, dus moet de initiator raden welke Diffie-Hellman (DH) groep moet worden gebruikt wanneer het eerste IKE-bericht wordt verstuurd. De DH-groep die voor deze schatting wordt gebruikt, is doorgaans de eerste DH-groep in de lijst met geconfigureerde DH-groepen. De initiatiefnemer berekent dan de sleutelgegevens voor de gezochte groepen maar stuurt ook een volledige lijst van alle groepen naar de peer, wat de peer in staat stelt om een andere DH groep te selecteren als de gegoten groep verkeerd is.

In het geval van een client is er geen door de gebruiker ingestelde lijst met IKE-beleid. In plaats daarvan is er een vooraf ingestelde lijst met beleid dat de client ondersteunt. Om de computationele belasting van de klant te verminderen wanneer je de belangrijkste gegevens voor het eerste bericht berekent met een groep die mogelijk het verkeerde is, werd de lijst van DH groepen van zwakste naar sterkste gerangschikt. De klant kiest dus voor de minst computationeel-intensieve DH en dus voor de eerste gok de minst bron-intensieve groep, maar dan switches naar de groep die door het hoofd van de bank in de volgende berichten wordt gekozen.

> **Opmerking:** Dit gedrag is anders dan de AnyConnect versie 3.0-clients die de DH-groepen van de sterkste tot de zwakste groepen bestelden.

Echter, op het head-end, is de eerste DH groep op de lijst die door de client wordt verstuurd die een DH groep aanpast die op de poort is ingesteld de groep die geselecteerd is. Daarom, als de ASA ook zwakkere DH-groepen heeft geconfigureerd, gebruikt zij de zwakste DH-groep die door de client wordt ondersteund en op het head-end is ingesteld, ondanks de beschikbaarheid van een meer beveiligde DH-groep aan beide uiteinden.

Dit gedrag is op de client vastgelegd via Cisco bug-ID CSCub92935. Alle clientversies met de oplossing van deze bug draaien de volgorde om waarin DH-groepen worden opgesomd wanneer

ze naar het head-end worden verzonden. Om echter een probleem van achterwaartse compatibiliteit met niet-Suite B-gateways te voorkomen, blijft de zwakste DH-groep (één voor niet-FIPS-modus en twee voor FIPS-modus) bovenaan de lijst staan.

> **Opmerking:** Na de eerste vermelding in de lijst (groep 1 of 2) worden de groepen gerangschikt in volgorde van sterkste tot zwakste. Hiermee worden de elliptische kromme groepen eerst geplaatst (21, 20, 19), gevolgd door de modulaire (MODP) groepen (24, 14, 5, 2).

> **Tip**: Als de poort is ingesteld met meerdere DH-groepen in hetzelfde beleid en groep 1 (of 2 in FIPS-modus) is opgenomen, dan accepteert de ASA de zwakkere groep. Het probleem is alleen DH groep 1 in een op de poort ingesteld beleid te integreren. Wanneer meerdere groepen in één beleid zijn geconfigureerd, maar groep 1 niet is opgenomen, is het sterkste geselecteerd. Voorbeeld:
>
> - Op ASA versie 9.0 (reeks B) met IKEv2-beleid ingesteld op 1 2 5 14 24 19 20 21 **wordt groep 1 geselecteerd** zoals verwacht.
>
> - Op ASA versie 9.0 (reeks B) met IKEv2-beleid ingesteld op 2 5 14 24 19 20 21 **wordt groep 21 geselecteerd** zoals verwacht.
>
> - Met de client in FIPS-modus op ASA versie 9.0 (reeks B) met IKEv2-beleid ingesteld op 1 2 5 14 24 19 20 21, **wordt groep 2 geselecteerd** zoals verwacht.
>
> - Wanneer de geteste client in FIPS-modus op ASA versie 9.0 (reeks B) is uitgevoerd met IKEv2-beleid ingesteld op 5 14 24 19 20 21, **wordt groep 21 geselecteerd** zoals verwacht.
>
> - Op ASA versie 8.4.4 (niet-suite B) met IKEv2-beleid ingesteld op 1 2 5 14, **wordt groep 1 geselecteerd** zoals verwacht.
>
> - Op ASA versie 8.4.4 (niet-suite B) met IKEv2-beleid ingesteld op 2 5 14, **wordt groep 14 geselecteerd** zoals verwacht.

# Probleem

ASA is ingesteld met dit IKEv2-beleid:

```
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
```

In deze configuratie is beleid 1 duidelijk geconfigureerd om alle FIPS-enabled cryptografische algoritmen te ondersteunen. Wanneer een gebruiker echter probeert verbinding te maken met een FIPS-enabled-client, valt de verbinding niet met de foutmelding:

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

Als de beheerder echter beleid 1 wijzigt zodat hij DH groep 2 in plaats van 20 gebruikt, werkt de verbinding.

# Oplossing

Op basis van de symptomen zou de eerste conclusie zijn dat de cliënt alleen DH groep 2 ondersteunt wanneer FIPS is ingeschakeld en geen van de andere werkt. Dit klopt gewoon niet. Als u dit debug op de ASA toelaat, kunt u de voorstellen zien die door de klant worden verstuurd:

```
debug crypto ikev2 proto 127
```

Tijdens een verbindingspoging is de eerste debug-bericht:

```
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
```

Ondanks het feit dat de klant de groepen 2,21,20,19,24,14 en 5 heeft verstuurd (deze FIPS-conforme groepen), sluit het head-end in de vorige configuratie nog steeds alleen groep 2-enabled

aan. Dit probleem wordt nog verder verergerd in de uitwerpselen:

```
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
```

De verbinding mislukt vanwege een combinatie van factoren:

1. Als FIPS is ingeschakeld, stuurt de client alleen specifiek beleid en moeten deze overeenkomen. Onder dat beleid wordt alleen Advanced Encryption Standard (AES)-encryptie voorgesteld met een belangrijke grootte groter dan of gelijk aan 256.

2. De ASA is ingesteld met meerdere IKEv2-beleidslijnen, waarvan er twee groep 2 hebben ingeschakeld. Zoals eerder beschreven, wordt in dit scenario dat beleid dat groep 2 heeft ingeschakeld, gebruikt voor de verbinding. Echter, het encryptie algoritme op beide beleid gebruikt een zeer belangrijke grootte van 192, die voor een FIPS-enabled client te laag is.

Daarom gedragen de ASA en de klant zich in dit geval volgens de configuratie. Er zijn drie manieren om dit probleem aan te pakken voor FIPS-enabled klanten:

1. Het instellen van één beleid met de exacte gewenste voorstellen.

2. Indien meerdere voorstellen vereist zijn, moet u deze niet configureren met groep 2; anders wordt deze altijd geselecteerd .

3. Als groep 2 moet worden geactiveerd, zorg er dan voor dat het het juiste encryptie-algoritme is geconfigureerd (AES-256 of aes-gcm-256).