Fehler bei kryptografischen AnyConnect-Algorithmen mit aktivierter FIPS-Funktion beheben

Inhalt

Einleitung

In diesem Dokument wird erläutert, warum Benutzer möglicherweise nicht mit einem FIPS-fähigen Client (Federal Information Processing Standard) eine Verbindung zu einer Adaptive Security Appliance (ASA) herstellen können, die über eine Richtlinie verfügt, die FIPS-fähige Verschlüsselungsalgorithmen unterstützt.

Hintergrundinformationen

Bei der Einrichtung einer IKEv2-Verbindung (Internet Key Exchange Version 2) ist dem Initiator nie bekannt, welche Vorschläge vom Peer akzeptiert werden. Der Initiator muss daher erraten, welche Diffie-Hellman (DH)-Gruppe beim Versenden der ersten IKE-Nachricht verwendet werden soll. Die für diese Schätzung verwendete DH-Gruppe ist in der Regel die erste DH-Gruppe in der Liste der konfigurierten DH-Gruppen. Der Initiator berechnet dann Schlüsseldaten für die erraten Gruppen, sendet aber auch eine vollständige Liste aller Gruppen an den Peer, sodass der Peer eine andere DH-Gruppe auswählen kann, wenn die erratene Gruppe falsch ist.

Bei einem Client gibt es keine vom Benutzer konfigurierte Liste von IKE-Richtlinien. Stattdessen gibt es eine vorkonfigurierte Liste von Richtlinien, die der Client unterstützt. Aus diesem Grund wurde die Liste der DH-Gruppen von schwächsten bis stärksten geordnet, um die Rechenlast auf dem Client zu reduzieren, wenn Sie die Schlüsseldaten für die erste Nachricht mit einer möglicherweise falschen Gruppe berechnen. Der Client wählt daher die am wenigsten rechenintensive DH und damit die am wenigsten ressourcenintensive Gruppe für die anfängliche Schätzung aus, schaltet dann aber in nachfolgenden Nachrichten auf die vom Headend ausgewählte Gruppe um.

> **Anmerkung:** Dieses Verhalten unterscheidet sich von den AnyConnect Version 3.0-Clients, die die DH-Gruppen vom stärksten bis zum schwächsten sorgten.

Am Headend ist jedoch die erste DH-Gruppe in der vom Client gesendeten Liste, die mit einer auf dem Gateway konfigurierten DH-Gruppe übereinstimmt, die ausgewählte Gruppe. Wenn die ASA außerdem schwächere DH-Gruppen konfiguriert hat, verwendet sie daher die schwächste DH-Gruppe, die vom Client unterstützt und auf dem Headend konfiguriert wird, trotz der Verfügbarkeit einer sichereren DH-Gruppe an beiden Enden.

Dieses Verhalten wurde auf dem Client mithilfe der Cisco Bug-ID CSCub92935 behoben. Alle Clientversionen mit der Behebung dieses Fehlers kehren die Reihenfolge um, in der DH-Gruppen aufgelistet werden, wenn sie an das Headend gesendet werden. Um jedoch ein Problem mit der Abwärtskompatibilität mit Gateways von anderen als der Suite B zu vermeiden, steht die schwächste DH-Gruppe (eine für den Nicht-FIPS-Modus und zwei für den FIPS-Modus) weiterhin ganz oben auf der Liste.

> **Anmerkung:** Nach dem ersten Eintrag in der Liste (Gruppe 1 oder 2) werden die Gruppen in der Reihenfolge am stärksten bis am schwächsten aufgelistet. Dabei werden zunächst die elliptischen Kurve-Gruppen (21, 20, 19) und anschließend die Modular Exponential (MODP)-Gruppen (24, 14, 5, 2) aufgeführt.

> **Tipp:** Wenn das Gateway mit mehreren DH-Gruppen in derselben Richtlinie konfiguriert ist und Gruppe 1 (oder 2 im FIPS-Modus) enthalten ist, akzeptiert die ASA die schwächere Gruppe. Die Korrektur besteht darin, dass nur die DH-Gruppe 1 in eine auf dem Gateway konfigurierte Richtlinie aufgenommen wird. Wenn mehrere Gruppen in einer Richtlinie konfiguriert sind, Gruppe 1 jedoch nicht enthalten ist, wird die stärkste Gruppe ausgewählt. Beispiele:
>
> - Auf ASA Version 9.0 (Suite B) mit IKEv2-Richtlinien, die auf 1 2 5 14 24 19 20 21 festgelegt sind, **wird Gruppe 1** wie erwartet **ausgewählt**.
>
> - Auf ASA Version 9.0 (Suite B) mit IKEv2-Richtlinien, die auf 2 5 14 24 19 20 21 festgelegt sind, **wird Gruppe 21** wie erwartet **ausgewählt**.
>
> - Wenn sich der Client auf ASA Version 9.0 (Suite B) im FIPS-Modus befindet und die IKEv2-Richtlinie auf 1 2 5 14 24 19 20 21 festgelegt ist, **wird Gruppe 2** wie erwartet **ausgewählt**.
>
> - Wenn der getestete Client auf ASA Version 9.0 (Suite B) im FIPS-Modus betrieben wird und die IKEv2-Richtlinie auf 5 14 24 19 20 21 festgelegt ist, **wird Gruppe 21** wie erwartet **ausgewählt**.
>
> - Auf ASA Version 8.4.4 (außer Suite B) mit IKEv2-Richtlinien auf 1 2 5 14 **wird Gruppe 1** wie erwartet **ausgewählt**.
>
> - Auf ASA Version 8.4.4 (außer Suite B) mit IKEv2-Richtlinien auf 2 5 14 **wird Gruppe 14** wie erwartet **ausgewählt**.

Problem

Die ASA wird mit den folgenden IKEv2-Richtlinien konfiguriert:

```
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 dieser Konfiguration ist Richtlinie 1 eindeutig konfiguriert, um alle FIPS-fähigen Verschlüsselungsalgorithmen zu unterstützen. Wenn ein Benutzer jedoch versucht, eine Verbindung über einen FIPS-fähigen Client herzustellen, schlägt die Verbindung mit der Fehlermeldung fehl:

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

Wenn der Administrator jedoch Policy1 so ändert, dass er statt 20 die DH-Gruppe 2 verwendet, funktioniert die Verbindung.

Lösung

Auf der Grundlage der Symptome besteht die erste Schlussfolgerung darin, dass der Client die DH-Gruppe 2 nur unterstützt, wenn FIPS aktiviert ist und keine der anderen funktioniert. Das ist eigentlich falsch. Wenn Sie dieses Debuggen auf der ASA aktivieren, werden die vom Client gesendeten Vorschläge angezeigt:

```
debug crypto ikev2 proto 127
```

Während eines Verbindungsversuchs lautet die erste Debugmeldung:

```
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
```

Obwohl der Client die Gruppen 2, 21, 20, 19, 24, 14 und 5 (diese FIPS-konformen Gruppen) gesendet hat, stellt das Headend daher immer noch nur eine Verbindung für Gruppe 2 her, die in Richtlinie 1 der vorherigen Konfiguration aktiviert ist. Dieses Problem wird weiter unten im Debugger deutlich:

```
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
```

Die Verbindung schlägt aufgrund einer Kombination von Faktoren fehl:

1. Wenn FIPS aktiviert ist, sendet der Client nur bestimmte Richtlinien, die übereinstimmen müssen. Unter diesen Richtlinien wird nur die AES-Verschlüsselung (Advanced Encryption Standard) mit einer Schlüssellänge größer/gleich 256 vorgeschlagen.

2. Die ASA wird mit mehreren IKEv2-Richtlinien konfiguriert, von denen zwei für Gruppe 2 aktiviert sind. Wie bereits beschrieben, wird in diesem Szenario die Richtlinie, die Gruppe 2 aktiviert hat, für die Verbindung verwendet. Der Verschlüsselungsalgorithmus beider Richtlinien verwendet jedoch eine Schlüsselgröße von 192, was für einen FIPS-fähigen Client zu niedrig ist.

Daher verhalten sich in diesem Fall ASA und Client wie in der Konfiguration. Es gibt drei Möglichkeiten, dieses Problem für FIPS-fähige Clients zu umgehen:

1. Konfigurieren Sie nur eine Richtlinie mit den gewünschten Vorschlägen.

2. Wenn mehrere Vorschläge erforderlich sind, sollten Sie keine mit Gruppe 2 konfigurieren. andernfalls wird immer eine ausgewählt.

3. Wenn Gruppe 2 aktiviert sein muss, stellen Sie sicher, dass der richtige Verschlüsselungsalgorithmus konfiguriert ist (Aes-256 oder aes-gcm-256).