فهم تدفق اتصال AnyConnect SSL VPN

المحتويات

المقدمة

يركز هذا المستند على تدفق الأحداث التي تحدث بين AnyConnect والبوابة الآمنة أثناء اتصال SSLVPN.

معلومات أساسية

AnyConnect

AnyConnect هو عميل Cisco VPN المصمم لبروتوكولات SSL و IKEv2. وهو متوفر لمعظم أجهزة سطح المكتب والأنظمة الأساسية المتنقلة. ينشئ AnyConnect بشكل أساسي إتصالات آمنة مع FirePOWER Threat Defense (FTD) أو أجهزة الأمان المعدلة (ASA) أو موجهات Cisco IOS®/Cisco IOS® XE المشار إليها باسم بوابات الأمان.

البوابة الآمنة

في مصطلحات Cisco، تتم الإشارة إلى خادم SSL VPN كبوابة آمنة، بينما يعرف خادم IPSec (IKEv2) باسم عبارة VPN للوصول عن بعد. تدعم Cisco إنهاء نفق SSL VPN على هذه الأنظمة الأساسية:

- السلسلة ASA 5500 و 5500-X من Cisco
- برنامج FTD من Cisco (السلسل 2100 و 4100 و 9300)
- السلسلة ISR 4000 و ISR G2 من Cisco
- السلسلة Cisco CSR 1000 Series
- السلسلة Cisco Catalyst 8000 Series

تدفق اتصال AnyConnect SSL VPN

يقسم هذا المستند الأحداث التي تحدث بين AnyConnect و Secure Gateway أثناء إنشاء اتصال SSL VPN إلى ست مراحل:

1. مصافحة SSL

2. POST - تحديد المجموعة

3. POST - مصادقة المستخدم باسم المستخدم/كلمة المرور (إختياري)

4. أداة تنزيل VPN (إختيارية)

5. اتصال CSTP

6. اتصال DTLS (إختياري)

1. مصافحة SSL

يبدأ مصافحة SSL من قبل عميل AnyConnect بعد إكمال مصافحة TCP الثلاثية الإتجاه باستخدام رسالة "Client Hello". إن تدفق الأحداث والمقتنيات الرئيسية هي كما ذكر آنفا.

Client Hello

تبدأ جلسة عمل SSL مع قيام العميل بإرسال رسالة 'Client Hello'. في هذه الرسالة:

أ) تم تعيين معرف جلسة SSL إلى 0، مما يشير إلى بدء جلسة عمل جديدة.

ب) تتضمن الحمولة مجموعات التشفير المدعومة من قبل العميل ومجموعة عشوائية منشأة من قبل العميل.

Server Hello

يستجيب الخادم برسالة "Server Hello" التي تتضمن:

أ) مجموعة التشفير المحددة من القائمة التي يوفرها العميل.

ب) قام الخادم بإنشاء معرف جلسة عمل SSL، وقام الخادم بإنشاء رقم عشوائي مرة واحدة.

شهادة الخادم

بعد "Server Hello"، يرسل الخادم شهادة SSL الخاصة به، والتي تعمل كهوية له. تشمل النقاط الرئيسية التي يجب ملاحظتها ما يلي:

أ) في حالة فشل هذه الشهادة في التحقق من الصحة بشكل صارم، يقوم AnyConnect بشكل افتراضي بحظر الخادم.

ب) للمستخدم خيار تعطيل هذه الكتلة، ولكن تعرض الاتصالات التالية تحذيرا حتى يتم حل الأخطاء المبلغ عنها.

طلب شهادة العميل

يمكن للخادم أيضا طلب شهادة عميل، وإرسال قائمة تضم أسماء المواضيع لكافة شهادات CA المحملة على البوابة الآمنة. يخدم هذا الطلب غرضين:

أ) يساعد العميل (المستخدم) على إختيار شهادة الهوية الصحيحة إذا توفرت عدة شهادات هوية.

ب) يضمن أن الشهادة المرتجعة موثوق بها من قبل البوابة الآمنة، رغم أنه يجب إجراء مزيد من التحقق من صحة الشهادة.

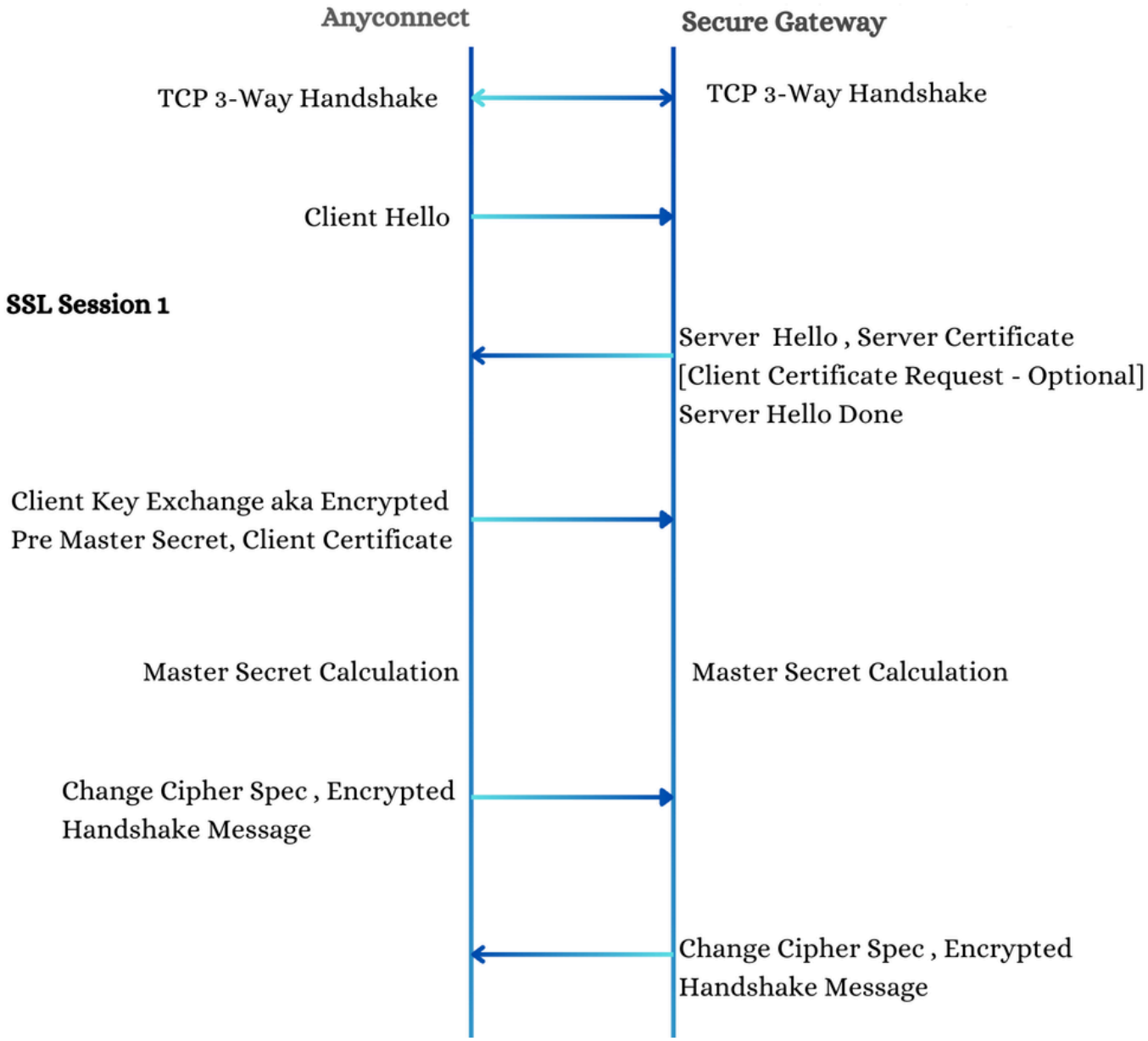
تبادل مفتاح العميل

يرسل العميل بعد ذلك رسالة "تبادل مفتاح العميل"، والتي تتضمن مفتاح سر أساسي مسبقا. يتم تشفير هذا المفتاح باستخدام:

أ) المفتاح العام للخادم من شهادة الخادم، إذا كانت مجموعة التشفير المختارة تستند إلى RSA (على سبيل المثال، TLS_RSA_WITH_AES_128_CBC_SHA).

ب) مفتاح DH العام للخادم المتوفر في رسالة "مرحبا على الخادم"، إذا كانت مجموعة التشفير المختارة تستند إلى DHE (على سبيل المثال، TLS_DHE_DSS_WITH_AES_256_CBC_SHA).

استنادا إلى السر الرئيسي المسبق، والشبكة العشوائية التي أنشأها العميل، والشبكة العشوائية التي أنشأها الخادم، يقوم كل من العميل والبوابة الآمنة بإنشاء سر رئيسي بشكل مستقل. ثم يتم إستخدام هذا السر الرئيسي الستخلاص مفاتيح الجلسة، مما يضمن الاتصال الآمن بين العميل والخادم.



SSL جلسة 1

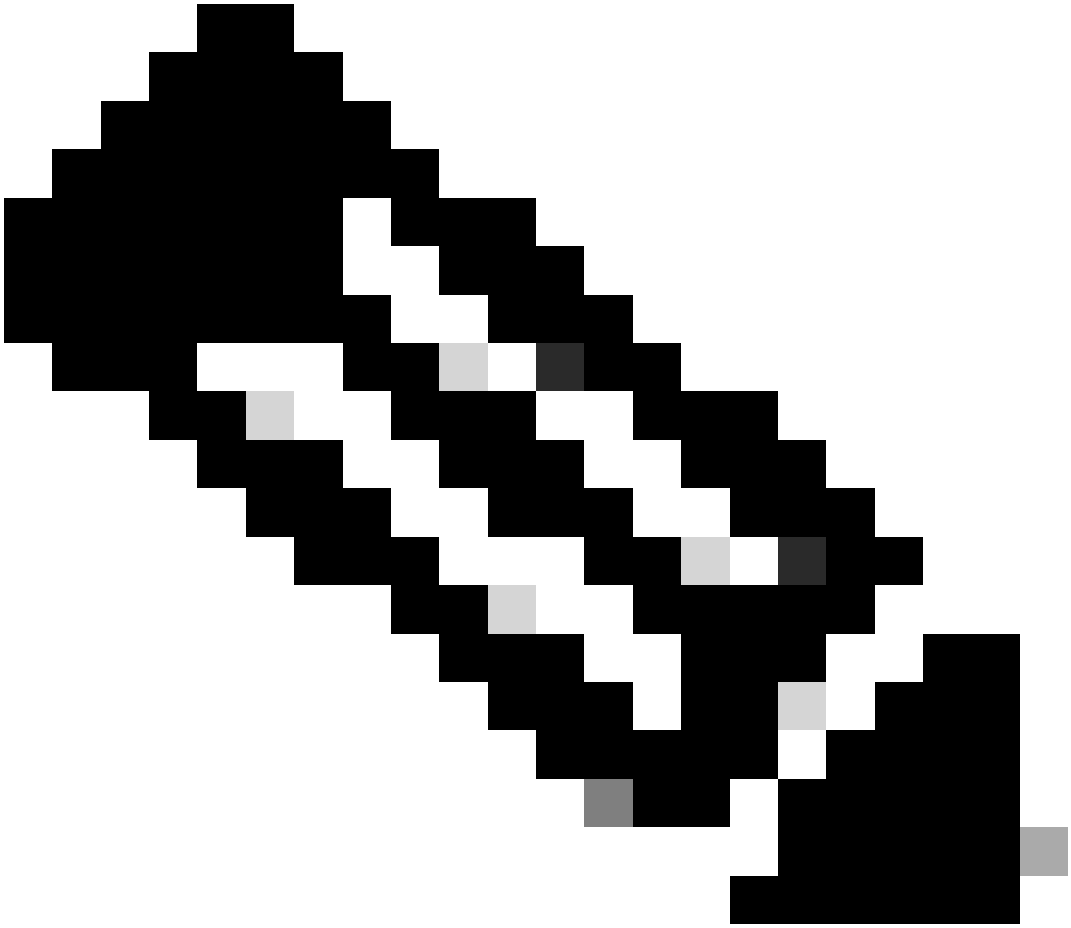
2. ترحيل - تحديد المجموعة

أثناء هذه العملية، ال يملك العميل معلومات حول ملف تعريف الاتصال ام لم يحددها المستخدم بشكل صريح. يتم توجيه محاولة الاتصال إلى URL البوابة الآمنة (asav.cisco.com)، كما هو موضح بواسطة العنصر "group-access" في الطلب. يشير العميل إلى دعمه للإصدار 2 من المصادقة التجميعية". يمثل هذا الإصدار تحسنا كبيرا عن الإصدار السابق، ال سيما من حيث معالجات XML الفعالة. يجب أن توافق كل من البوابة الآمنة والعميل على الإصدار الذي سيتم إستخدامه. في السيناريوهات التي ال تدعم فيها البوابة الآمنة الإصدار 2، يتم تشغيل عملية POST إضافية، مما يؤدي إلى تراجع العميل إلى الإصدار.

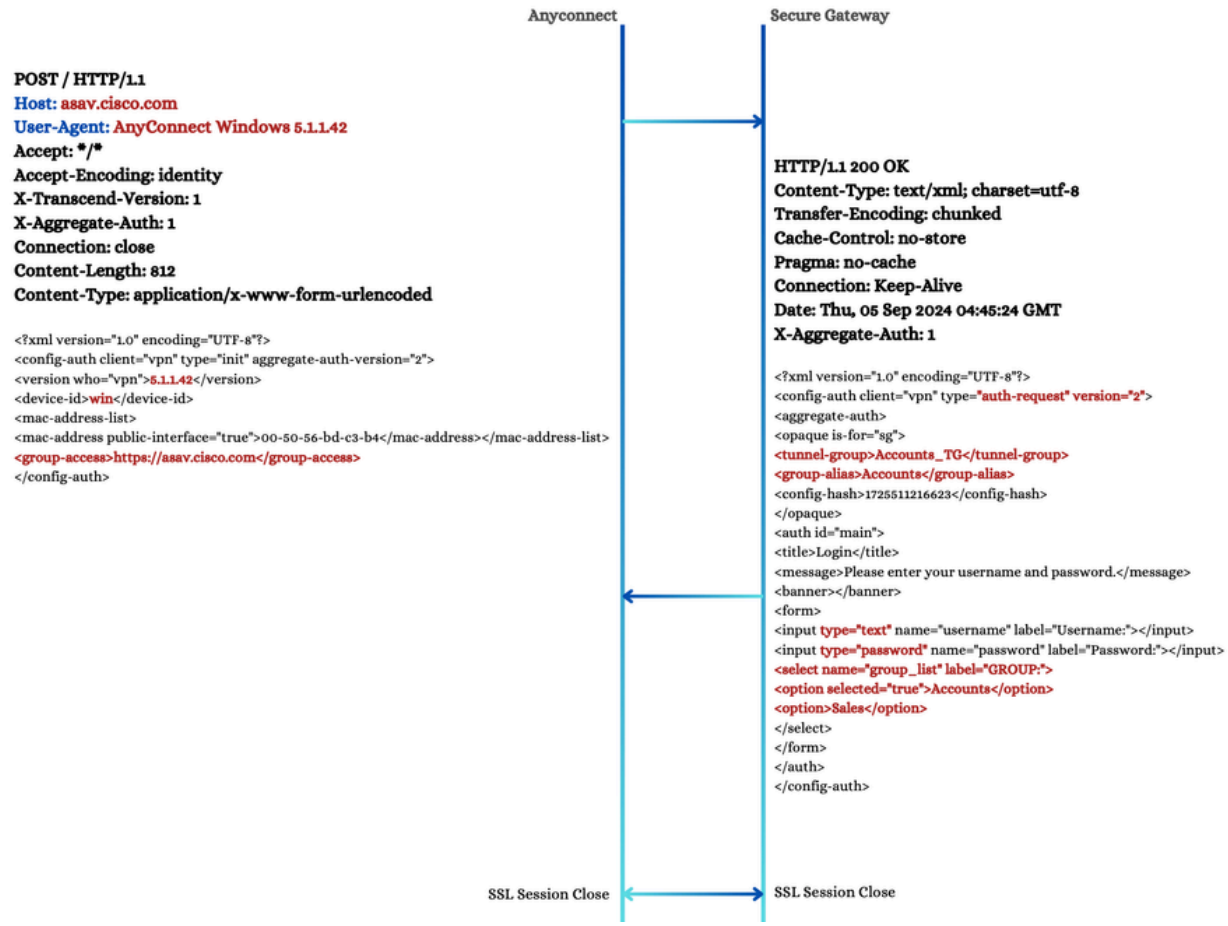
في إستجابة HTTP، تشير العبارة الآمنة إلى ما يلي:

1. إصدار المصادقة التجميعية التي تدعمها البوابة الآمنة.

2. قائمة مجموعة النفق ونموذج اسم المستخدم/كلمة المرور.

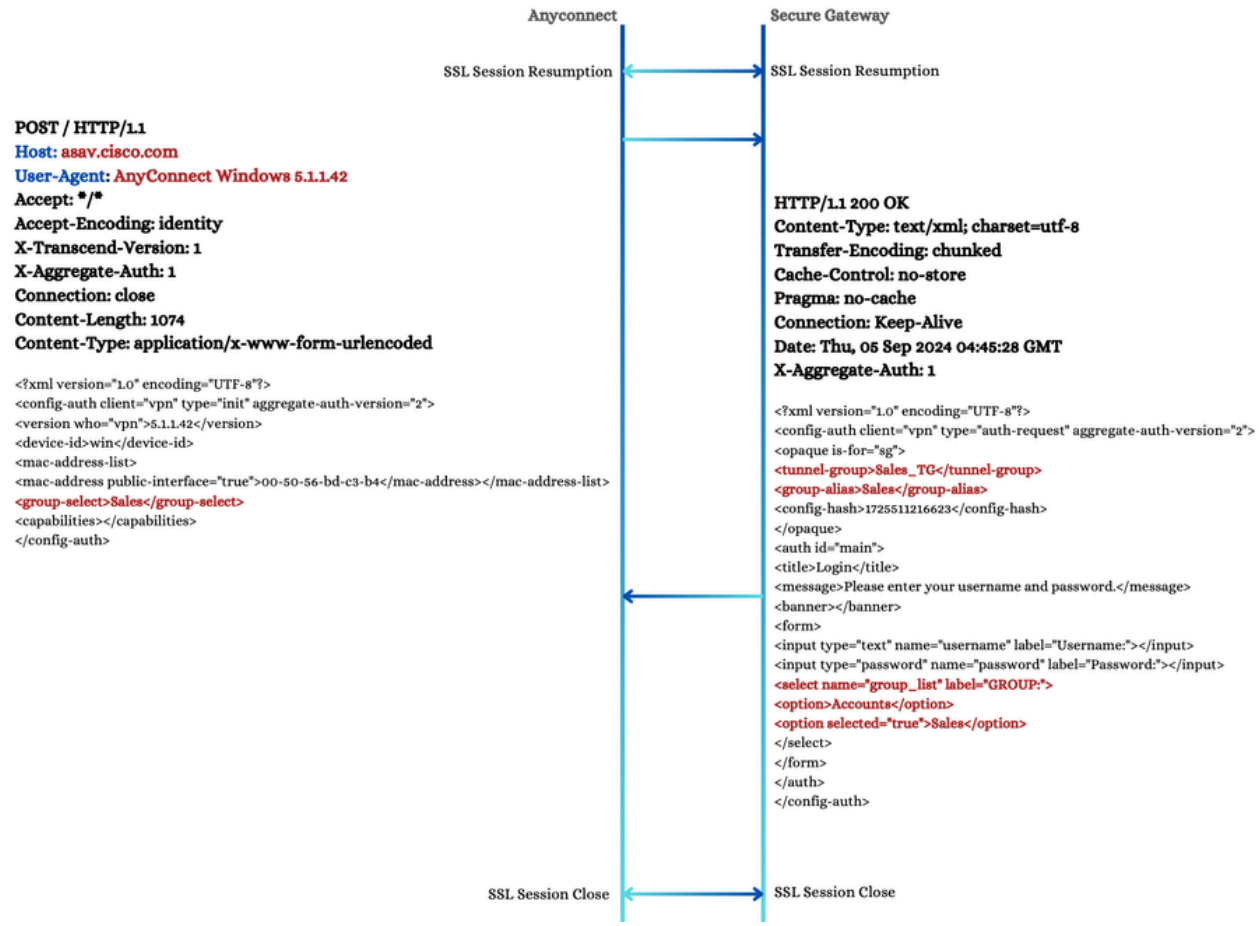


ملاحظة: يتضمن النموذج عنصر 'select'، الذي يسرد الأسماء المستعارة للمجموعة لكافة ملفات تعريف الاتصال التي تم تكوينها على البوابة الآمنة. بشكل افتراضي، يتم إبراز أحد أسماء المجموعات المستعارة هذه باستخدام السمة المنطقية المحددة = "true". تتوافق عناصر مجموعة النفق واسم المجموعة المستعار مع ملف تعريف الاتصال المختار هذا.



ترحيل - تحديد المجموعة 1

إذا اختار المستخدم ملف تعريف اتصال مختلفا من هذه القائمة، فستكون هناك عملية POST أخرى. في هذه الحالة، يرسل العميل طلب POST مع تحديث العنصر 'group-select' ليعكس ملف تعريف الاتصال المختار، كما هو موضح هنا.



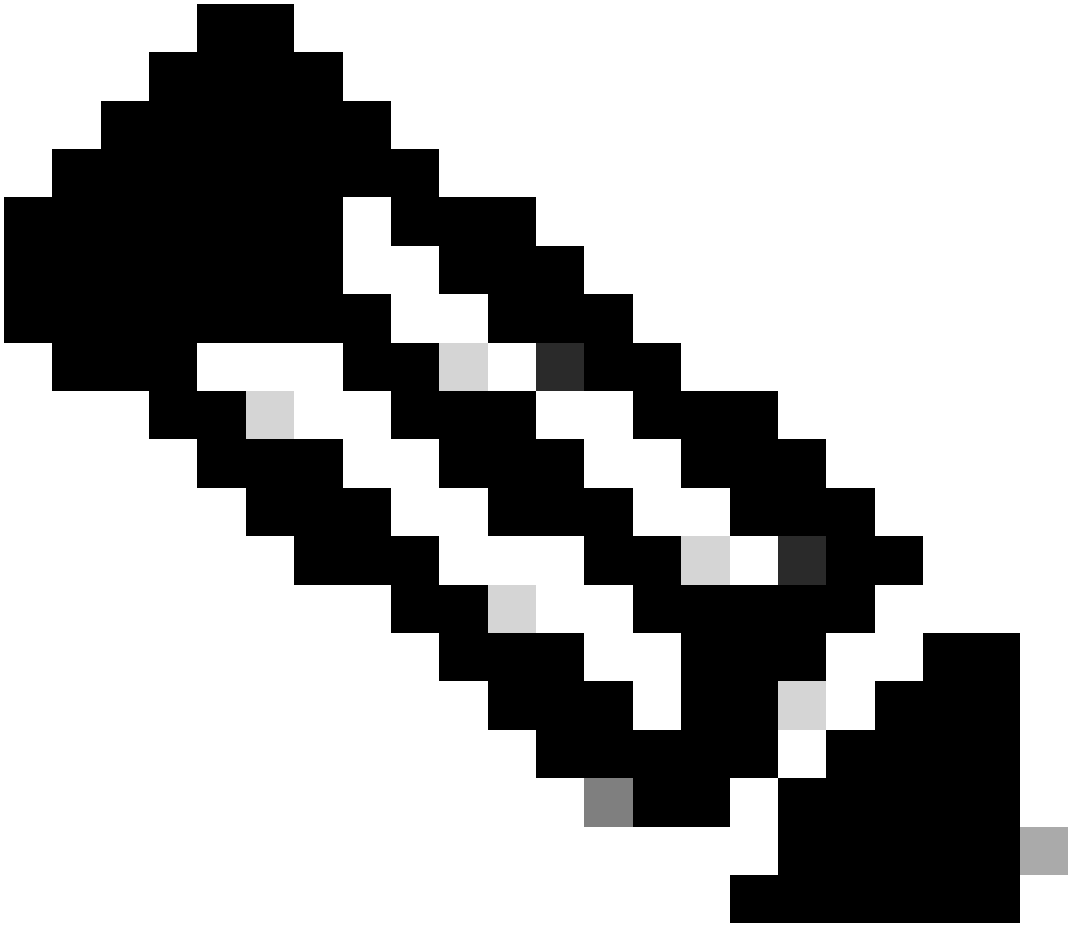
البريد - تحديد المجموعة 2

3. ترخيل - مصادقة المستخدم

في هذه العملية، التي تتبع تحديد ما بعد المجموعة، يرسل AnyConnect هذه المعلومات إلى البوابة الآمنة:

1. معلومات ملف تعريف الاتصال المختارة: تتضمن هذه المعلومات اسم مجموعة النفق والاسم المستعار للمجموعة كما هو مشار إليه بواسطة البوابة الآمنة في العملية السابقة.

2. اسم المستخدم وكلمة المرور: مسوغات المصادقة الخاصة بالمستخدم.



ملاحظة: نظرا لأن هذا التدفق خاص بمصادقة AAA، فقد يختلف عن طرق المصادقة الأخرى.

إستجابة لعملية POST، ترسل البوابة الآمنة ملف XML يحتوي على هذه المعلومات:

1. معرف جلسة العمل: هذا ليس هو نفس معرف جلسة SSL.

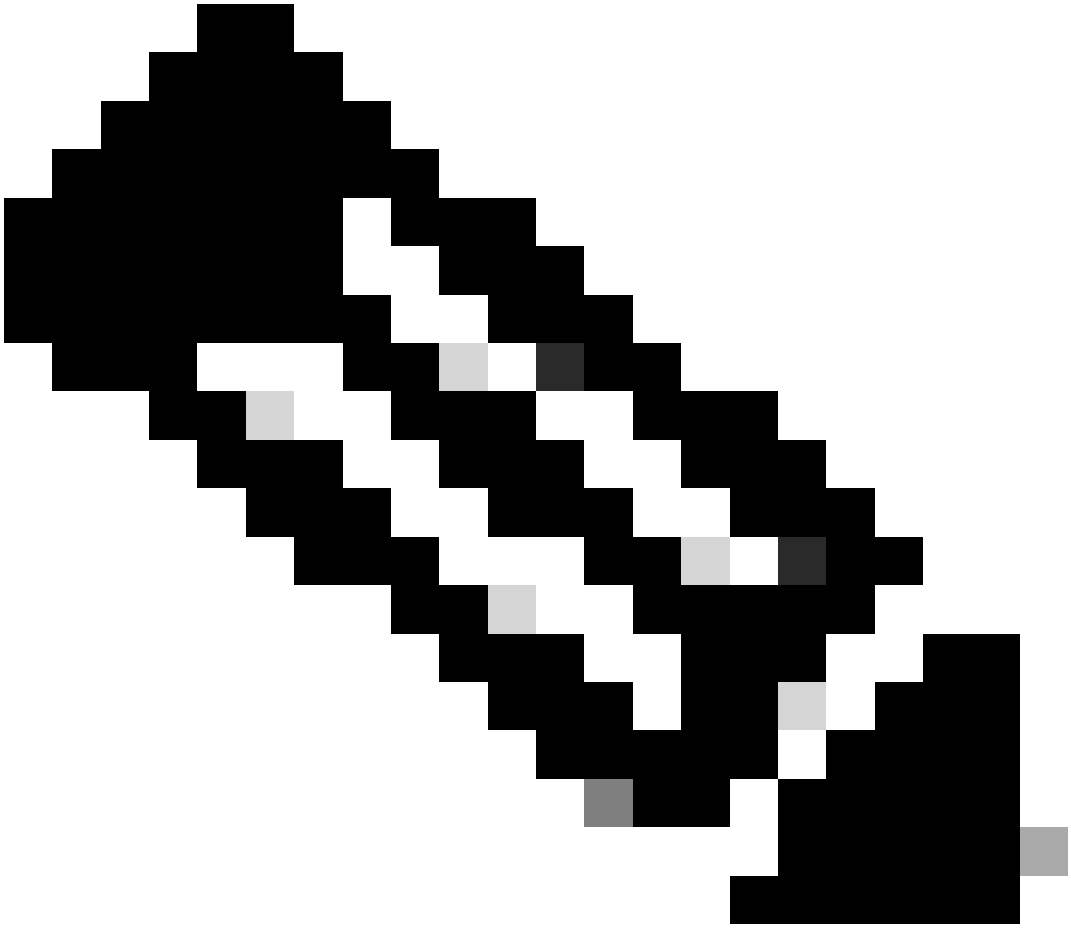
2. الرمز المميز لجلسة العمل: يتم إستخدام هذا الرمز المميز لاحقا من قبل العميل كملف تعريف إرتباط WebVPN.

3. حالة المصادقة: يشار إليها بواسطة عنصر مصادقة بمعرف = "نجاح".

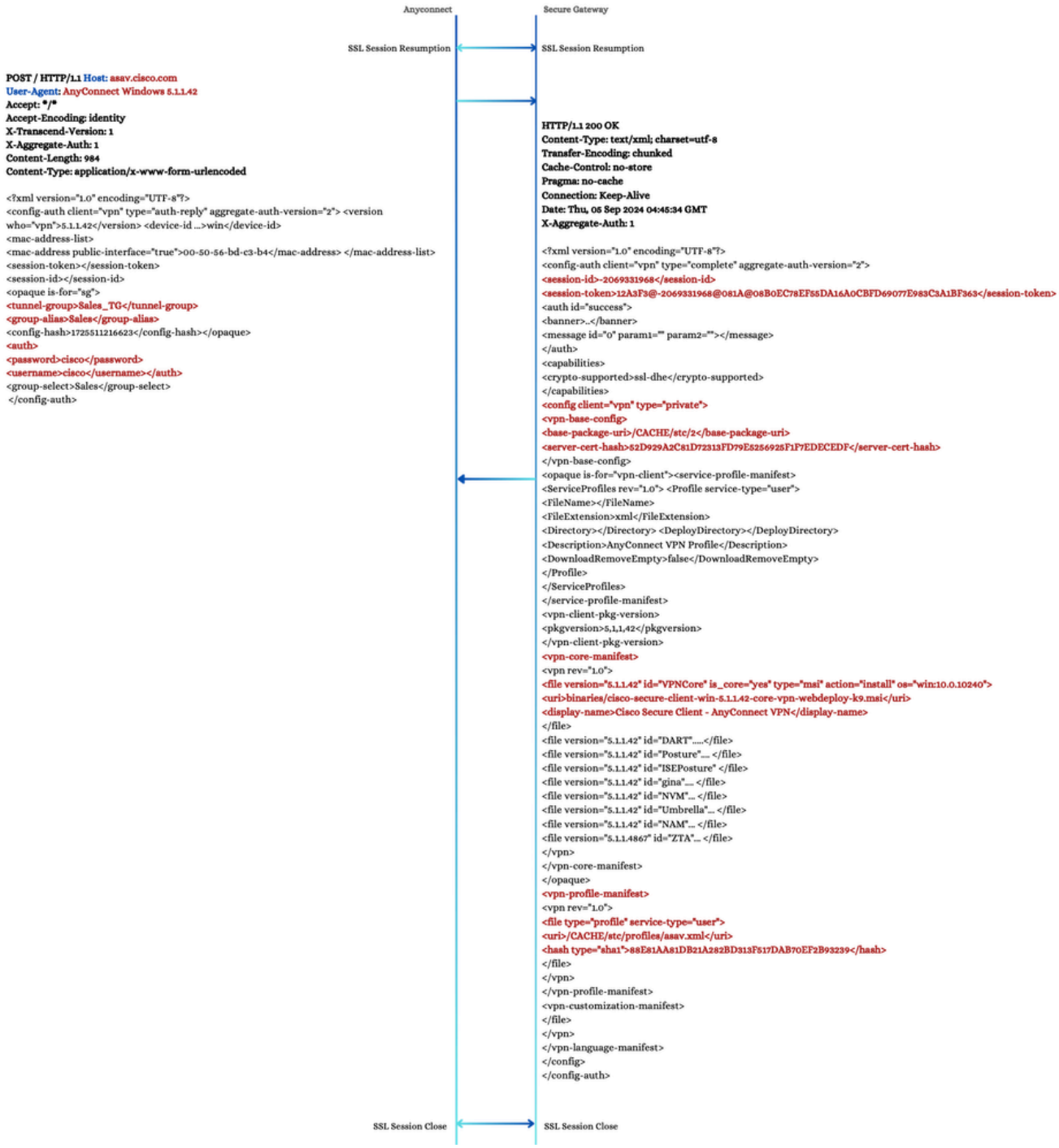
4. تجزئة شهادة الخادم: يتم تخزين هذه التجزئة مؤقتا في ملف preferences.xml.

5. VPN-core-manifest element: يشير هذا العنصر إلى مسار إصدار حزمة AnyConnect الأساسية، بالإضافة إلى مكونات أخرى مثل Dart و Posture و ISE Posture وما إلى ذلك. ويتم إستخدامه من قبل أداة تنزيل VPN في القسم التالي.

6. عنصر بيان ملف تعريف VPN: يشير هذا العنصر إلى المسار (اسم ملف التعريف) وتقسيم SHA-1 لملف التعريف.



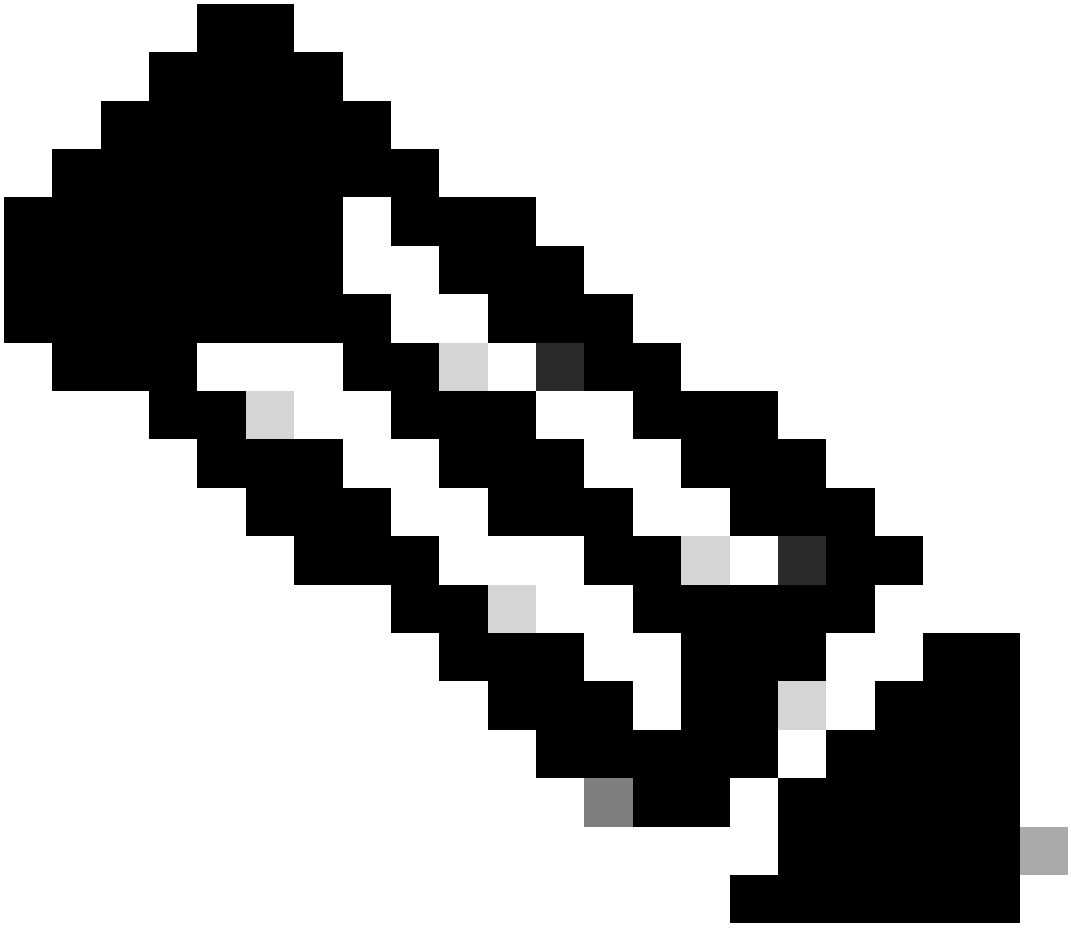
ملاحظة: إذا لم يكن لدى العميل ملف التعريف، يقوم جهاز تنزيل VPN في القسم التالي بتنزيله. إذا كان العميل لديه ملف التعريف بالفعل، فإنه يتم مقارنة تجزئة SHA-1 لملف تعريف العميل مع الموجود على الخادم. في حالة عدم تطابق، يقوم جهاز تنزيل VPN باستبدال ملف تعريف العميل بملف تعريف العميل الموجود على البوابة الآمنة. وهذا يضمن فرض التوصيف على البوابة الآمنة على العميل بعد المصادقة.



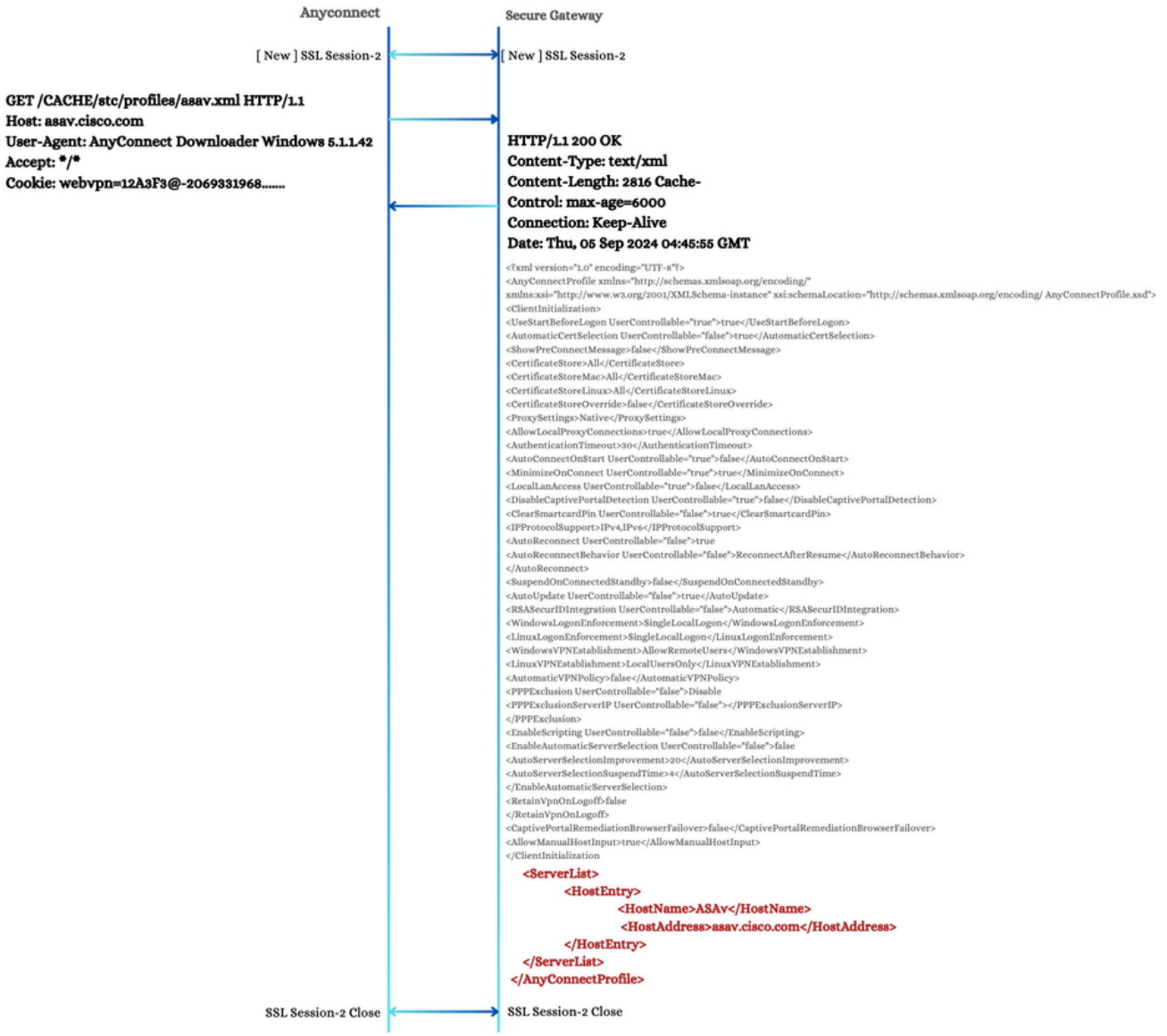
ترخيل - مصادقة المستخدم

4. أداة تنزيل AnyConnect

يقوم "جهاز تنزيل AnyConnect" دوما ببدء جلسة عمل SSL جديدة، وهذا هو السبب في أن المستخدمين يمكنهم مواجهة تحذير شهادة ثانية إذا كانت شهادة البوابة الآمنة غير موثوق بها. وأثناء هذه المرحلة، تقوم بتنفيذ عمليات GET منفصلة لكل عنصر يحتاج إلى التنزيل.



ملاحظة: إذا تم تحميل ملف تعريف العميل على عبارة آمنة، فهو إلزامي للتنزيل؛ وإلا، يتم إنهاء محاولة الاتصال بالكامل.

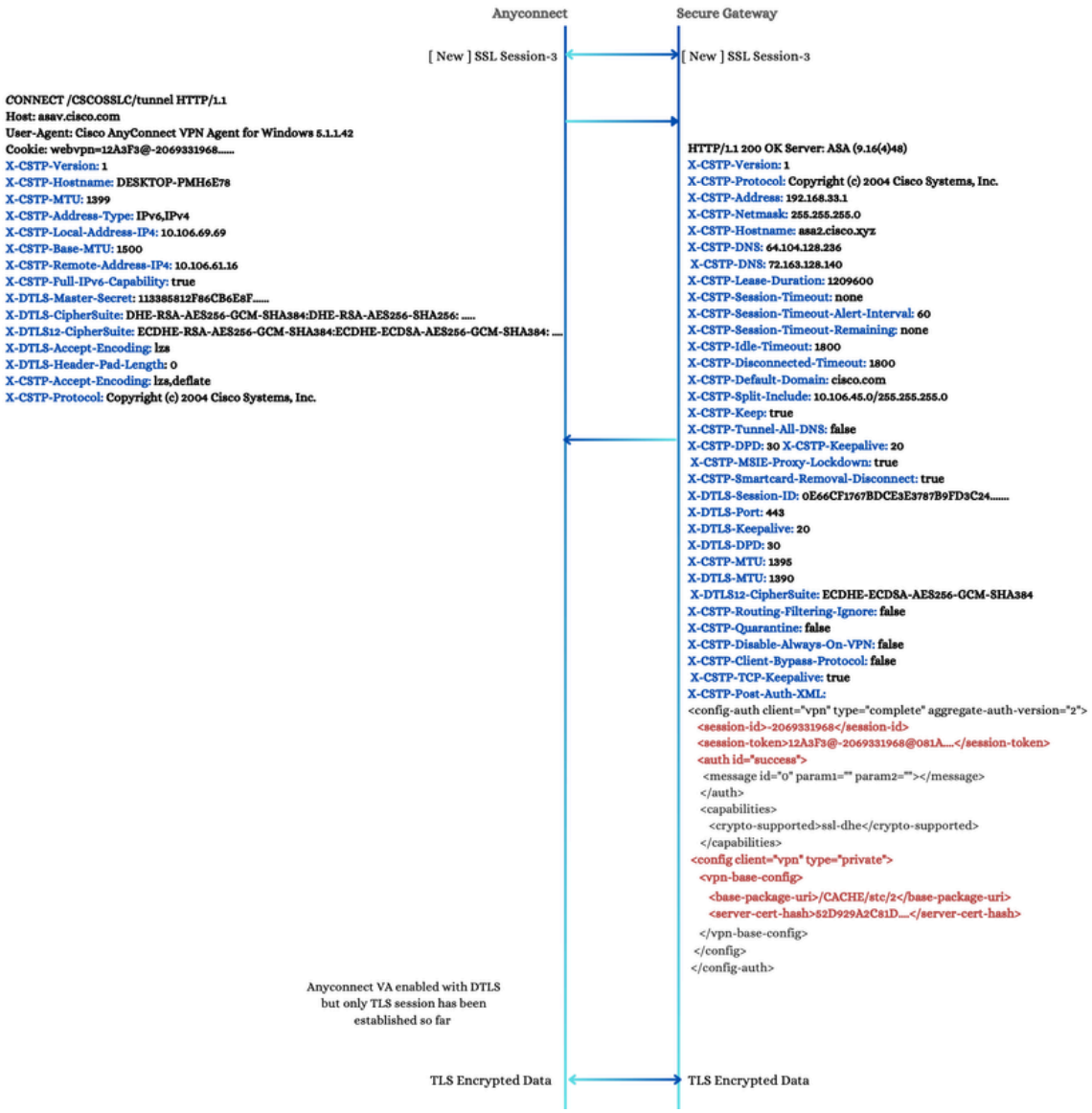


جهاز تنزيل VPN

5. اتصال CSTP

يجري AnyConnect عملية اتصال كخطوة نهائية في إنشاء قناة آمنة. أثناء عملية الاتصال، يرسل عميل AnyConnect سمات X-CSTP و X-DTLS مختلفة للعبارة الآمنة من أجل معالجتها. تستجيب البوابة الآمنة مع سمات X-CSTP و X-DTLS الإضافية التي يطبقها العميل على محاولة الاتصال الحالية. يتضمن هذا التبادل X-CSTP-Post-Auth-XML، مصحوبا بملف XML، والذي يشبه إلى حد كبير ذلك الموجود في خطوة مصادقة المستخدم - POST.

بعد تلقي إستجابة ناجحة، يقوم AnyConnect بتهيئة قناة بيانات TLS. في الوقت نفسه، يتم تنشيط واجهة المهائي الظاهري AnyConnect بقيمة MTU تساوي X-DTLS-MTU، على افتراض نجاح مصافحة DTLS التالية.



اتصال CSTP

6. مصافحة DTLS

تستمر المصافحة DTLS كما هو موضح هنا. هذا الإعداد سريع نسبيا نظرا للسمات المتبادلة بين العميل والخادم أثناء حدث الاتصال.

العميل

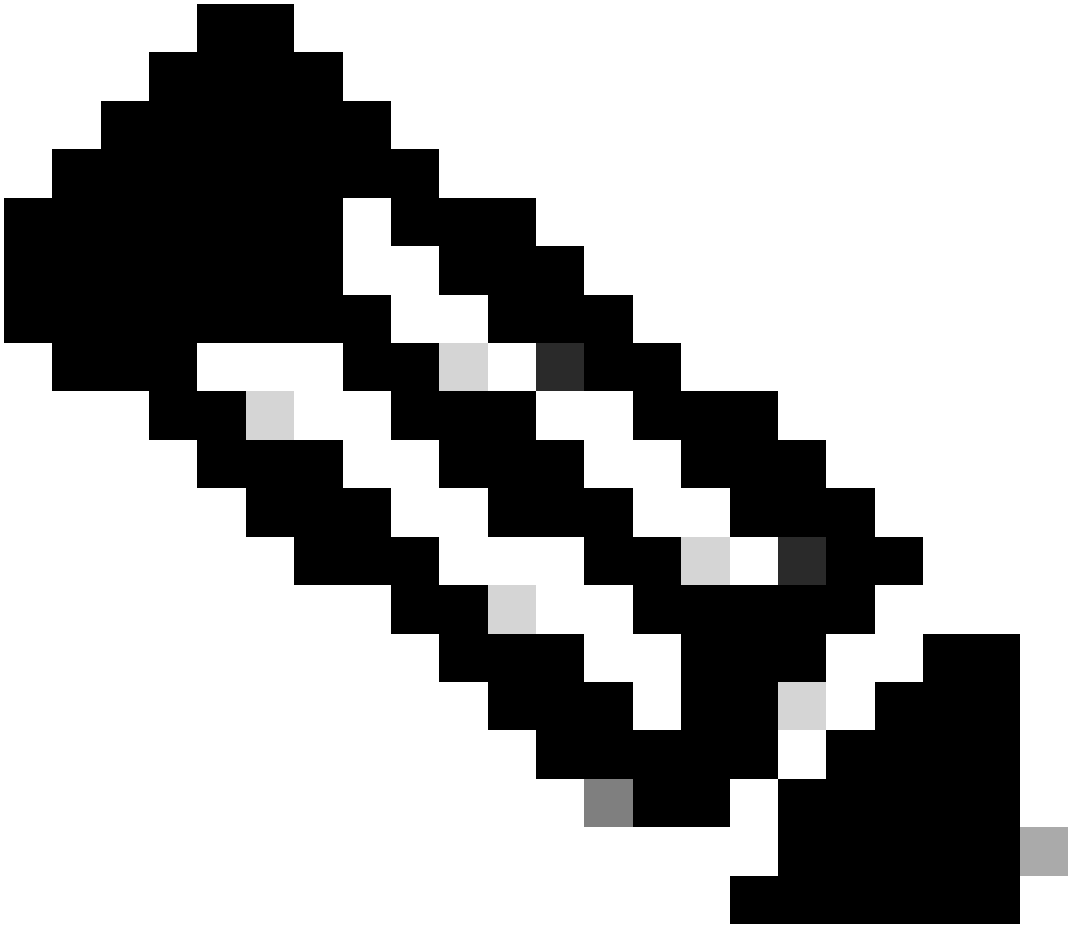
X-DTLS-Master-Secret: يتم إنشاء سر DTLS الرئيسي بواسطة العميل ومشاركته مع الخادم. هذا المفتاح ضروري لإنشاء جلسة DTLS آمنة.

X-DTLS-CipherSuite: قائمة مجموعات شفرة DTLS التي يدعمها العميل، تشير إلى إمكانات التشفير للعميل.

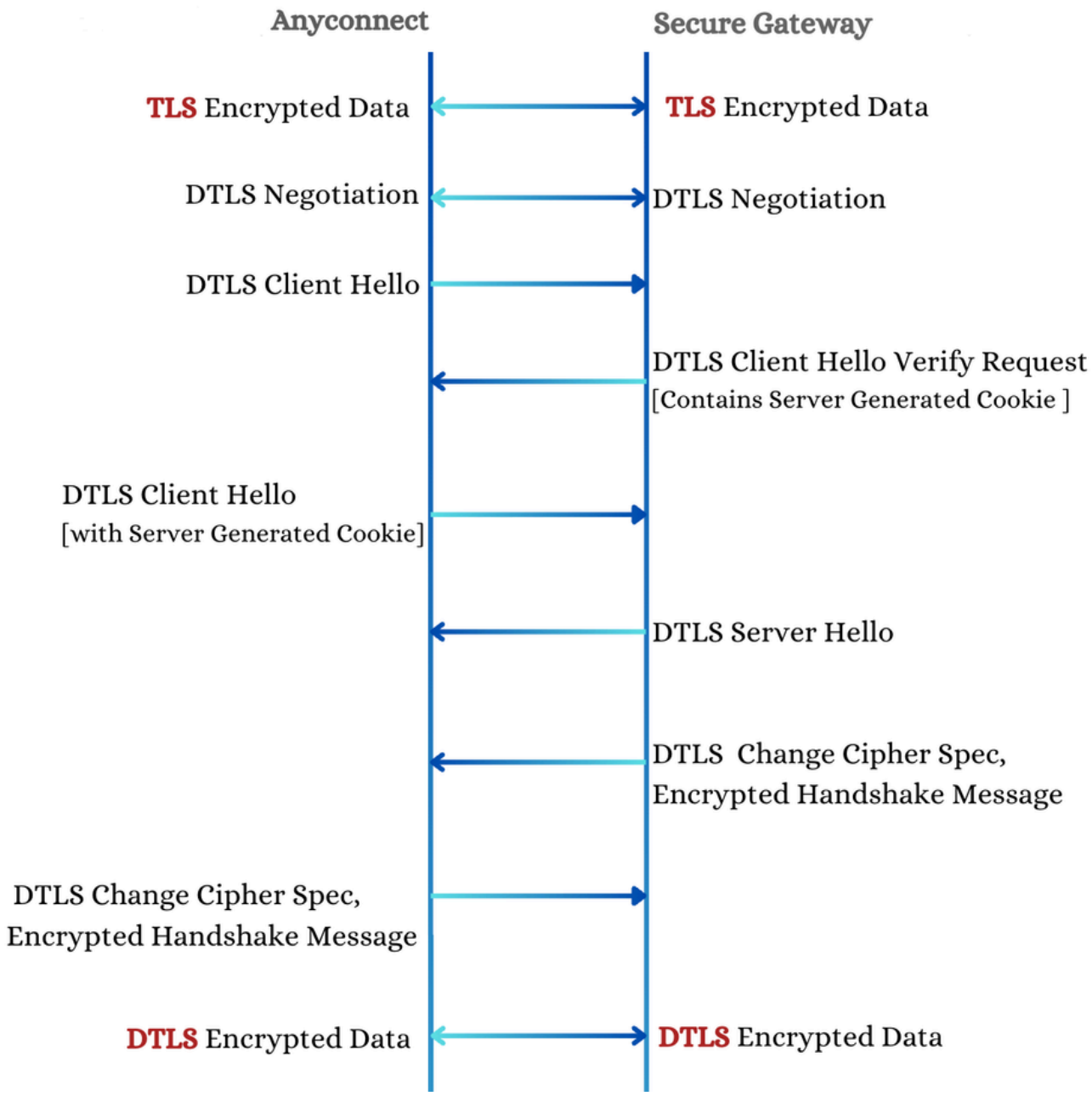
الخادم

X-DTLS-Session-ID: معرف جلسة عمل DTLS الذي تم تعيينه من قبل الخادم للعميل لاستخدامه، مما يضمن إستمرارية الجلسة.

X-DTLS-CipherSuite: مجموعة التشفير التي حددها الخادم من القائمة التي وفرها العميل، مما يضمن إستخدام كل الطرفين لطريقة تشفير متوافقة.



ملاحظة: بينما تكون مصافحة DTLS قيد التقدم، تستمر قناة بيانات TLS في العمل. وهذا يضمن أن ظل نقل البيانات متناسقا وآمنا أثناء عملية المصافحة. لا يحدث الانتقال بسلاسة إلى قناة تشفير بيانات DTLS إلا بعد اكتمال مصافحة DTLS.

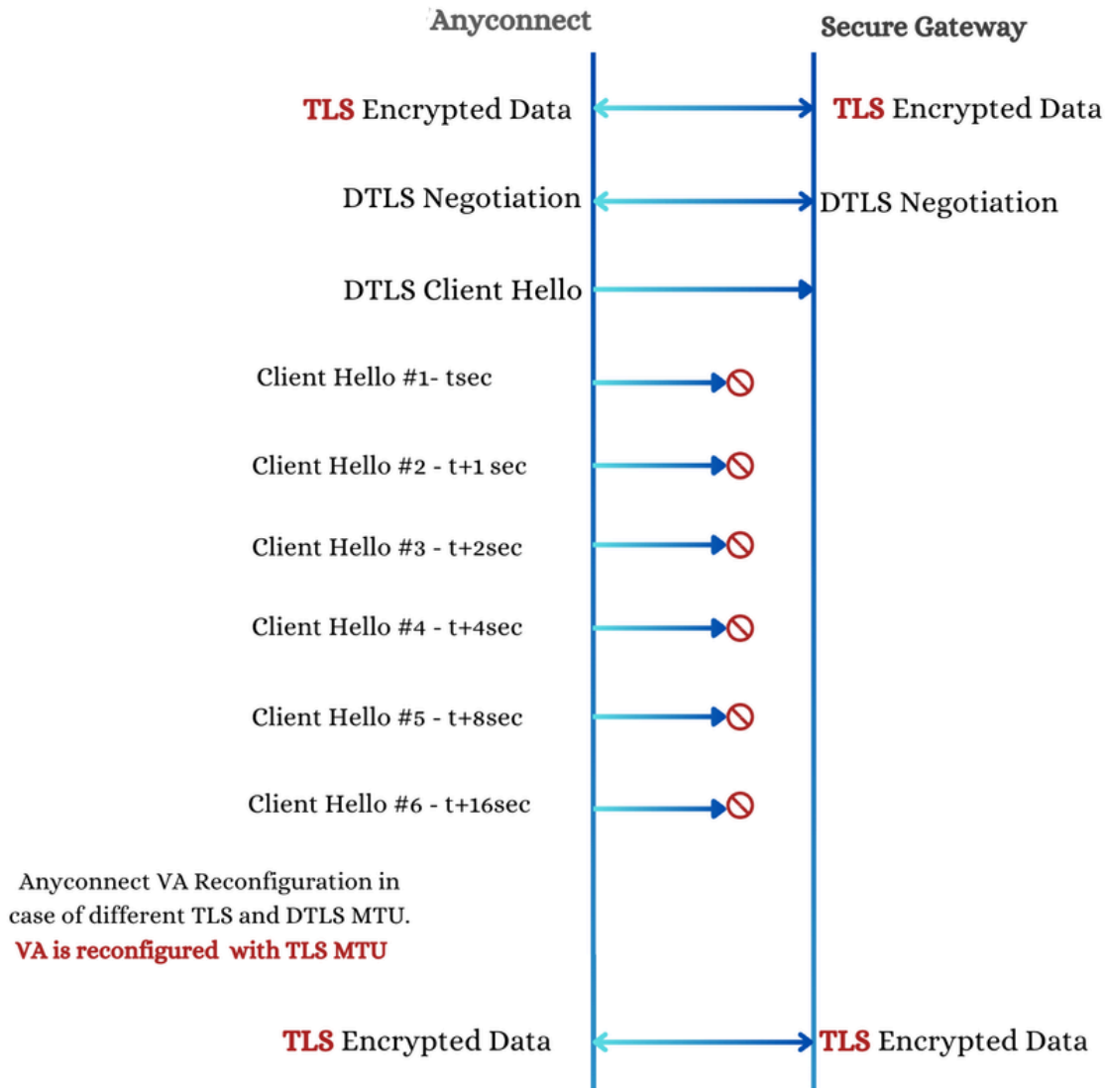


مصافحة DTLS

6.1. حظر منفذ DTLS

في حالة حظر منفذ DTLS أو فشل البوابة الآمنة في الاستجابة لحزم DTLS Client Hello، يقوم AnyConnect بتنفيذ تراجع أسي مع ما يصل إلى خمس محاولات، بدءا من التأخير لمدة ثانية واحدة والزيادة حتى 16 ثانية.

إذا لم تنجح هذه المحاولات، فسيقوم AnyConnect بتطبيق وحدة الحد الأقصى للنقل (MTU) الفعلية ل TLS، كما هو محدد بواسطة قيمة X-CSTP-MTU التي تم إرجاعها بواسطة البوابة الآمنة في المرحلة 5.، على المهايئ الظاهري AnyConnect. ونظرا لأن وحدة الحد الأقصى للنقل (MTU) هذه تختلف عن وحدة الحد الأقصى للنقل (MTU) المطبقة سابقا (X-DTLS-MTU)، فمن الضروري إعادة تكوين المهايئ الظاهري. تظهر إعادة التكوين هذه للمستخدم النهائي كمحاولة لإعادة الاتصال، رغم عدم حدوث مفاوضات جديدة أثناء هذه العملية. بمجرد إعادة تكوين المحول الظاهري، تستمر قناة بيانات TLS في العمل.



كتلة منفذ DTLS

معلومات ذات صلة

- مرجع وثائق تقنيات VPN من Cisco
- الدعم الفني والتنزيلات من Cisco

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).