AnyConnect: تكوين Basic SSL VPN لواجهة سطر الأوامر من Cisco IOS

المقدمة

المحتويات

المقدمة
المتطلبات الأساسية
المتطلبات
المكونات المستخدمة
معلومات أساسية
معلومات الترخيص إلصدارات IOS المختلفة
تحسينات البرامج المهمة
التكوين
الخطوة 1. تم تمكين تأكيد الترخيص
الخطوة 2. تحميل حزمة AnyConnect Secure Mobility Client وتثبيتها على الموجه
الخطوة 3. إنشاء زوج مفاتيح RSA وشهادة موقعة ذاتيا
الخطوة 4. تكوين حسابات مستخدمي VPN المحلية
الخطوة 5. تحديد قائمة الوصول إلى تجمع العناوين وتقسيم النفق المراد استخدامها من قبل العملاء
الخطوة 6. تكوين واجهة القالب الظاهري (VTI)
الخطوة 7. تكوين بوابة WebVPN
الخطوة 8. تكوين سياق WebVPN ونهج المجموعة
الخطوة 9 (اختياري) قم بتكوين ملف تعريف عميل
التحقق من الصحة
استكشاف الأخطاء وإصلاحها
معلومات ذات صلة

يصف هذا المستند التكوين الأساسي لموجه Cisco IOS® على أنه وحدة الاستقبال والبث الخاصة بطبقة مآخذ التوصيل الآمنة AnyConnect VPN (SSL VPN).

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- Cisco من IOS
- AnyConnect Secure Mobility Client
- عملية SSL العامة

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- الموجه Cisco 892W الذي يشغل 15.3(3)M5
- AnyConnect Secure Mobility Client 3.1.08009

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهم للتأثير المحتمل لأي أمر.

معلومات أساسية

معلومات الترخيص لإصدارات IOS المختلفة

- يلزم توفر مجموعة ميزات securityK9 لاستخدام ميزات SSL VPN، بغض النظر عن إصدار Cisco IOS الذي يتم إستخدامه.
- Cisco IOS 12.x - يتم دمج ميزة SSL VPN في جميع الصور 12.x التي تبدأ ب 12.4(6)T التي تحتوي على ترخيص أمان على الأقل (على سبيل المثال، Advsecurityk9 و Adventerprisek9 وما إلى ذلك).
- Cisco IOS 15.0 - تتطلب الإصدارات الأقدم تثبيت ملف LIC على الموجه مما يسمح ب 10 أو 25 أو 100 اتصال مستخدم. تطبيق ترخيص الاستخدام* في الإصدار 15.0(1)M4
- Cisco IOS 15.1 - تتطلب الإصدارات الأقدم تثبيت ملف LIC على الموجه مما يسمح ب 10 أو 25 أو 100 اتصال مستخدم. تم تنفيذ تراخيص الاستخدام* في 15.1(1)T2 و 15.1(2)T2 و 15.1(3)T و 15.1(4)M1
- Cisco IOS 15.2 - توفر جميع الإصدارات 15.2 تراخيص الاستخدام* ل SSLVPN
- برنامج Cisco IOS 15.3 وما بعده - توفر الإصدارات الأقدم الحق في الاستخدام*. بدءا من الطراز 15.3(3)M، تتوفر ميزة SSLVPN بعد التمهيد في حزمة تقنية SecurityTYK9

للحصول على ترخيص RTU، يتم تمكين ترخيص التقييم عند تكوين ميزة WebVPN لأول مرة (أي عبارة webVPN1) وقبول إتفاقية ترخيص المستخدم النهائي (EULA). وبعد 60 يوما، يصبح ترخيص التقييم هذا ترخيصا دائما. وتستند هذه التراخيص إلى الشرف وتتطلب شراء ترخيص ورقي لاستخدام الميزة. بالإضافة إلى ذلك، وبدلا من القيود على عدد معين من الاستخدامات، تسمح وحدة الحد الأقصى من الاتصالات المتزامنة التي يمكن للنظام الأساسي للموجه دعمها في نفس الوقت.

تحسينات البرامج المهمة

نتج عن معرفات الأخطاء هذه ميزات أو إصلاحات مهمة ل AnyConnect:

- CSCti89976: دعم إضافي ل AnyConnect 3.x إلى IOS
- CSCtx38806: إصلاح للقابلية للتعرض ل BEAST، Microsoft KB2585542

التكوين

الخطوة 1. تم تمكين تأكيد الترخيص

تتمثل الخطوة الأولى عند تكوين AnyConnect على وحدة الاستقبال والبث لموجه IOS في التأكد من تثبيت الترخيص بشكل صحيح (إذا كان ذلك ممكنا) وتمكينه. ارجع إلى معلومات

الترخيص في القسم السابق للحصول على تفاصيل الترخيص حول الإصدارات المختلفة. يعتمد على إصدار الرمز والنظام الأساسي سواء كان عرض الترخيص يسرد ترخيص SSL_VPN أو securityTyk9. وبغض النظر عن الإصدار والترخيص، سيلزم قبول EULA وسيظهر الترخيص كنشاط.

الخطوة 2. تحميل حزمة AnyConnect Secure Mobility Client وتثبيتها على الموجه

لتحميل صورة AnyConnect إلى شبكة VPN، تخدم وحدة الاستقبال والبث غرضين. أولا، سيسمح فقط لأنظمة التشغيل التي تحتوي على صور AnyConnect موجودة على وحدة الاستقبال والبث ل AnyConnect بالاتصال. على سبيل المثال، تتطلب عملاء Windows تثبيت حزمة Windows على وحدة الاستقبال والبث، ويتطلب عملاء Linux إصدار 64 بت حزمة Linux إصدار 64 بت، وهكذا. ثانيا، سيتم دفع صورة AnyConnect المثبتة على وحدة الاستقبال والبث تلقائيا إلى جهاز العميل عند الاتصال. سيتمكن المستخدمون الذين يتصلون للمرة الأولى من تنزيل العميل من بوابة الويب وسيتمكن المستخدمون الذين يرجعون من الترقية، شريطة أن تكون حزمة AnyConnect الموجودة على وحدة الاستقبال والبث أحدث من تلك المثبتة على جهاز العميل لديهم.

يمكن الحصول على حزم AnyConnect من خلال قسم AnyConnect Secure Mobility Client من [موقع Cisco على الويب تنزيلات برامج]. في حين أن هناك العديد من الخيارات المتوفرة، سيتم وسم الحزم التي سيتم تثبيتها على وحدة الاستقبال والبث بنظام التشغيل وعملية النشر على الرأس (PKG). تتوفر حزم AnyConnect لأنظمة التشغيل هذه: Windows و Mac OS X و Linux (32 بت) و Linux 64 بت. لاحظ أنه بالنسبة للينكس، هناك حاجة لكل من حزم 32 و 64 بت. يتطلب كل نظام تشغيل تركيب الحزمة المناسبة على وحدة الاستقبال والبث للسماح بالاتصالات.

لتنزيل حزمة AnyConnect، يمكن تحميلها إلى ذاكرة Flash (الذاكرة المؤقتة) للموجه بدرج الأمر **copy** عبر TFTP أو FTP أو SCP أو عدد قليل من الخيارات الأخرى. فيما يلي مثال:

```
copy tftp: flash:/webvpn/

Address or name of remote host []? 192.168.100.100
Source filename []? anyconnect-win-3.1.08009-k9.pkg
Destination filename [/webvpn/anyconnect-win-3.1.08009-k9.pkg]?
Accessing tftp://192.168.100.100/anyconnect-win-3.1.08009-k9.pkg...
Loading anyconnect-win-3.1.08009-k9.pkg from 192.168.100.100 (via GigabitEthernet0):
!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 37997096 bytes]

37997096 bytes copied in 117.644 secs (322984 bytes/sec)
```

بعد نسخ صورة AnyConnect إلى ذاكرة Flash (الذاكرة المؤقتة) الخاصة بالموجه، يجب تثبيتها عبر سطر الأوامر. يمكن تثبيت حزم AnyConnect المتعددة عند تحديد رقم تسلسل في أمر التثبيت، مما يسمح للموجه بالعمل كجهاز توجيه للأنظمة تشغيل متعددة. عند تثبيت حزمة AnyConnect، فإنها تستقل أيضا بنقلها بموقت إلى **الذاكرة المؤقتة:/webVPN/ directory** إذا لم يتم نسخه هناك في البداية.

```
crypto vpn anyconnect flash:/webvpn/anyconnect-win-3.1.08009-k9.pkg sequence 1
```

```
SSLVPN Package SSL-VPN-Client (seq:1): installed successfully
```

في إصدارات التعليمات البرمجية التي تم إصدارها قبل 15.2(1)T، يختلف الأمر الخاص بتركيب PKG قليلا.

```
webvpn install svc flash:/webvpn/anyconnect-win-3.1.08009-k9.pkg sequence 1
```

الخطوة 3. إنشاء زوج مفاتيح RSA وشهادة موقعة ذاتيا

عندما تقوم بتكوين SSL أو أي ميزة تقوم بتنفيذ البنية الأساسية للمفاتيح العام (PKI) والشهادات الرقمية، يلزم وجود زوج مفاتيح Rivest-Shamir-Adleman (RSA) لتوقيع الشهادة. سيقوم هذا الأمر بإنشاء زوج مفاتيح RSA الذي سيتم إستخدامه بعد ذلك عند إنشاء شهادة PKI الموقعة ذاتيا. تمتع باستخدام معدل وحدات بت يبلغ 2048، وهو ليس متطلبا ولكن يوصى باستخدام أكبر وحدات وحدات بت متوفرة لتحسين الأمان والتوافق مع أجهزة عميل AnyConnect. كما يوصى باستخدام تسمية مفاتيح وصفية سيتم تعيينها مع إدارة المفاتيح. يمكن تأكيد إنشاء المفاتيح باستخدام الأمر **show crypto key mypubkey rsa**.

> **ملاحظة**: نظرا لوجود العديد من مخاطر الأمان المرتبطة بجعل مفاتيح RSA قابلة للتصدير، فإن الممارسة الموصى بها هي التأكد من تكوين المفاتيح لتكون غير قابلة للتصدير، وهو الإعداد الافتراضي. تتم مناقشة المخاطر التي تنطوي عليها عند قيامك بجعل مفاتيح RSA قابلة للتصدير في هذا المستند: نشر مفاتيح RSA داخل PKI.

```
crypto key generate rsa label SSLVPN_KEYPAIR modulus 2048

The name for the keys will be: SSLVPN_KEYPAIR

% The key modulus size is 2048 bits
% Generating 2048 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 3 seconds)

show crypto key mypubkey rsa SSLVPN_KEYPAIR

% Key pair was generated at: 14:01:34 EDT May 21 2015
Key name: SSLVPN_KEYPAIR
Key type: RSA KEYS
Storage Device: not specified
Usage: General Purpose Key
Key is not exportable.
Key Data:
30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101
00C4C7D6 F9533CD3 A5489D5A 4DC3BAE7 6831E832 7326E322 CBECC41C 8395A5F7
4613AF70 827F581E 57F72074 FD803EEA 693EBACC 0EE5CA65 5D1875C2 2F19A432
84188F61 4E282EC3 D30AE4C9 1F2766EF 48269FE2 0C1AECAA 81511386 1BA6709C
7C5A2A40 2FBB3035 04E3770B 01155368 C4A5B488 D38F425C 23E430ED 80A8E2BD
E713860E F654695B C1780ED6 398096BC 55D410DB ECC0E2D9 2621E1AB A418986D
39F241FE 798EF862 9D5EAEEB 5B06D73B E769F613 0FCE2585 E5E6DFF3 2E48D007
3443AD87 0E66C2B1 4E0CB6E9 81569DF2 DB0FE9F1 1A9E737F 617DC68B 42B78A8B
952CD997 78B96CE6 CB623328 C2C5FFD6 18C5DA2C 2EAFA936 5C866DE8 5184D2D3
6D020301 0001
```

بمجرد إنشاء زوج مفاتيح RSA بنجاح، يجب تكوين نقطة اتصال PKI باستخدام معلومات الموجه وزوج مفاتيح RSA الخاص بنا. يجب تكوين السم الشائع (CN) في اسم الموضوع باستخدام عنوان IP أو اسم المجال المؤهل بالكامل (FQDN) الذي يستخدمه المستخدمون

للاتصال بوابة AnyConnect؛ في هذا المثال، يستخدم العميل FQDN الخاص ب fdenofa-SSLVPN.cisco.com عند محاولة الاتصال. على الرغم من أنه غير إجباري، عندما تدخل ال CN بشكل صحيح، فإنه يساعد على تقليل عدد أخطاء الشهادة التي تتم مطالبتك بها عند تسجيل الدخول.

> **ملاحظة**: بدل من إستخدام شهادة موقعة ذاتيا تم إنشاؤها بواسطة الموجه، من الممكن إستخدام شهادة صادرة عن مرجع مصدق من جهة خارجية. يمكن أن يتم ذلك من خلال عدة طرق مختلفة كما هو موضح في هذا المستند: تكوين تسجيل الشهادة ل PKI.

```
crypto pki trustpoint SSLVPN_CERT
 enrollment selfsigned
 subject-name CN=fdenofa-SSLVPN.cisco.com
 rsakeypair SSLVPN_KEYPAIR
```

بعد تحديد TrustPoint بشكل صحيح، يجب أن يقوم الموجه بإنشاء الشهادة باستخدام الأمر **crypto pki enroll**. مع هذه العملية، من الممكن تحديد بضعة معلمات أخرى مثل الرقم التسلسلي وعنوان IP. غير أن هذه غير مطلوب. يمكن تأكيد إنشاء الشهادة باستخدام أمر **show crypto pki certificates**.

```
crypto pki enroll SSLVPN_CERT

% Include the router serial number in the subject name? [yes/no]: no
% Include an IP address in the subject name? [no]: no
Generate Self Signed Router Certificate? [yes/no]: yes

Router Self Signed Certificate successfully created

show crypto pki certificates SSLVPN_CERT

Router Self-Signed Certificate
  Status: Available
  Certificate Serial Number (hex): 01
  Certificate Usage: General Purpose
  Issuer:
    hostname=fdenofa-892.fdenofa.lab
    cn=fdenofa-SSLVPN.cisco.com
  Subject:
    Name: fdenofa-892.fdenofa.lab
    hostname=fdenofa-892.fdenofa.lab
    cn=fdenofa-SSLVPN.cisco.com
  Validity Date:
    start date: 18:54:04 EDT Mar 30 2015
    end   date: 20:00:00 EDT Dec 31 2019
  Associated Trustpoints: SSLVPN_CERT
```

الخطوة 4. تكوين حسابات مستخدمي VPN المحلية

بينما من الممكن إستخدام خادم المصادقة والتفويض والمحاسبة (AAA) الخارجي، يتم إستخدام المصادقة المحلية على سبيل المثال. ستقوم هذه الأوامر بإنشاء مستخدم vpnUser وأيضا إنشاء قائمة مصادقة AAA باسم SSLVPN_AAA.

```
aaa new-model
aaa authentication login SSLVPN_AAA local
username VPNUSER password TACO
```

الخطوة 5. تحديد قائمة الوصول إلى تجمع العناوين وتقسيم النفق المرار إستخدامها من قبل العملاء

يجب إنشاء تجمع عناوين IP محلي للحصول على عنوان IP لمهائيات عميل AnyConnect. تأكد من تكوين تجمع كبير بدرجة كافية لدعم الحد الأقصى من إتصالات عملاء AnyConnect المتزامنة.

بشكل افتراضي، سيعمل AnyConnect في وضع النفق الكامل مما يعني أن أي حركة مرور يتم إنشاؤها بواسطة جهاز العميل سيتم إرسالها عبر النفق. وحيث أن هذا الأمر غير مرغوب فيه عادة، فمن الممكن تكوين قائمة تحكم في الوصول (ACL) التي تحدد بعد ذلك حركة المرور التي يجب أو لا يجب إرسالها عبر النفق. كما هو الحال مع عمليات تنفيذ قوائم التحكم في الوصول الأخرى، يعمل الرفض الضمني في النهاية على إزالة الحاجة إلى رفض صريح، وبالتالي، فمن الضروري فقط تكوين عبارات السماح لحركة المرور التي يجب إنشاء قنوات لها.

```
ip local pool SSLVPN_POOL 192.168.10.1 192.168.10.10
access-list 1 permit 192.168.0.0 0.0.255.255
```

الخطوة 6. تكوين واجهة القالب الظاهري (VTI)

شبكات VTI الديناميكية توفير واجهة وصول افتراضي منفصلة حسب الطلب لكل جلسة من جلسات شبكة VPN تسمح باتصال آمن وقابل للتوطير بدرجة كبيرة لشبكات VPN للوصول عن بعد. تحل تقنية DVTI محل الخارئط المشفرة الديناميكية وطريقة المحاور الأكثر تعقيدا لأنها تدعم مثل أي مزيج DVTI من بروتوكولات التوجيه الديناميكية التي تساعد على إنشاء أنفاق. ونظرا لأن أجهزة DVTI تعمل كوجهة حقيقية أخرى، فإنها تسمح بنشر الوصول عن بعد أكثر تعقيدا لأنها تدعم وجهة الخدمة وجدار الحماية وسمات كل مستخدم وخدمات الأمان الأخرى بمجرد أن يصبح النفق نشطا.

```
interface Loopback0
 ip address 172.16.1.1 255.255.255.255
!
interface Virtual-Template 1
 ip unnumbered Loopback0
```

الخطوة 7. تكوين بوابة WebVPN

عبارة WebVPN هي التي تحدد عنوان IP والمنفذ (المنافذ) الذي سيتم إستخدامه من قبل وحدة الاستقبال والبث من AnyConnect، بالإضافة إلى خوارزمية تشفير SSL وشهادة PKI التي سيتم تقديمها إلى العملاء. بشكل افتراضي، ستدعم البوابة جميع خوارزميات التشفير المحتملة، والتي تختلف اعتمادا على إصدار Cisco IOS على الموجه.

```
webvpn gateway SSLVPN_GATEWAY
 ip address 209.165.201.1 port 443
 http-redirect port 80
 ssl trustpoint SSLVPN_CERT
 inservice
```

الخطوة 8. تكوين سياق WebVPN ونهج المجموعة

يحدد سياق WebVPN ونهج المجموعة بعض المعلمات الإضافية التي سيتم إستخدامها لاتصال عميل AnyConnect. بالنسبة لتكوين AnyConnect أساسي، يعمل السياق بسياسة "نهج المجموعة" الافتراضي الذي سيتم إستخدامه ل

AnyConnect. وهو ذلك، يمكن إستخدام السياق لتخصيص صفحة بداية WebVPN وعملية WebVPN SSLVPN_AAA قائمة تكوين تتم، المحددة النهج المجموعة في. إضافي لشكل WebVPN ب. الأمر **functions svc enabled** وهو جزء من قائمة مصادقة AAA التي يكون المستخدمون عضوا فيها. درجة من الدخول إلى AnyConnect SSL VPN لعميل AnyConnect الذي يسمح للمستخدمين بالاتصال عبر التكوين. أخيرا، تحدد أوامر SVC الإضافية المعلمات ذات الصلة بقفل تصفح WebVPN من الخلال. باتصالات SVC: يعلم **SVC address-pool** البوابة إلى عنوان الوثيقة في SSLVPN_POOL للعملاء، **SVC مع انقسام تضمين** تعريف سياسة النفق المقسم لكل قائمة تحكم في الوصول (ACL) معرفة أعلاه، ويقوم **svc dns-server** بتعريف خادم DNS الذي سيتم إستخدامه لحل إسم المجال. مع هذا التكوين، سيتم إرسال كافة إستعلامات DNS إلى خادم DNS المحدد. سيفرض العنوان الذي يتم إستلامه في إستجابة الاستعلام ما إذا تم إرسال حركة مرور البيانات عبر النفق أم ال.

```
webvpn context SSLVPN_CONTEXT
virtual-template 1
 aaa authentication list SSLVPN_AAA
gateway SSLVPN_GATEWAY inservice
policy group SSLVPN_POLICY functions svc-enabled svc address-pool "SSLVPN_POOL" netmask
255.255.255.0 svc split include acl 1 svc dns-server primary 8.8.8.8
default-group-policy SSLVPN_POLICY
```

الخطوة 9 (إختياري) قم بتكوين ملف تعريف عميل

بخلاف ASAs، الذي يحتوي Cisco IOS على واجهة GUI مدمجة يمكنها مساعدة المسؤولين في إنشاء ملف تعريف العميل. يلزم إنشاء/تحرير ملف تعريف عميل AnyConnect بشكل منفصل باستخدام محرر ملف التعريف المستقل.

> **تلميح**: ابحث عن AnyConnect-profileeditor-win-3.1.03103-k9.exe.

اتبع هذه الخطوات لجعل الموجه ينشر التوصيف:

- قم بتحميله إلى ذاكرة IOS Flash باستخدام FTP/TFTP.
- أستخدم هذا الأمر لتعريف التوصيف الذي تم تحميله للتو:

```
crypto vpn annyconnect profile SSLVPN_PROFILE flash:test-profile.xml
```

> **تلميح**: في إصدارات Cisco IOS الأقدم من 15.2(1)T، يلزم إستخدام هذا الأمر: **إستيراد ملف تعريف WebVPN <profile_name> flash:<profile.xml>**

3. تحت السياق، أستخدم هذا الأمر لربط ملف التعريف بذلك السياق:

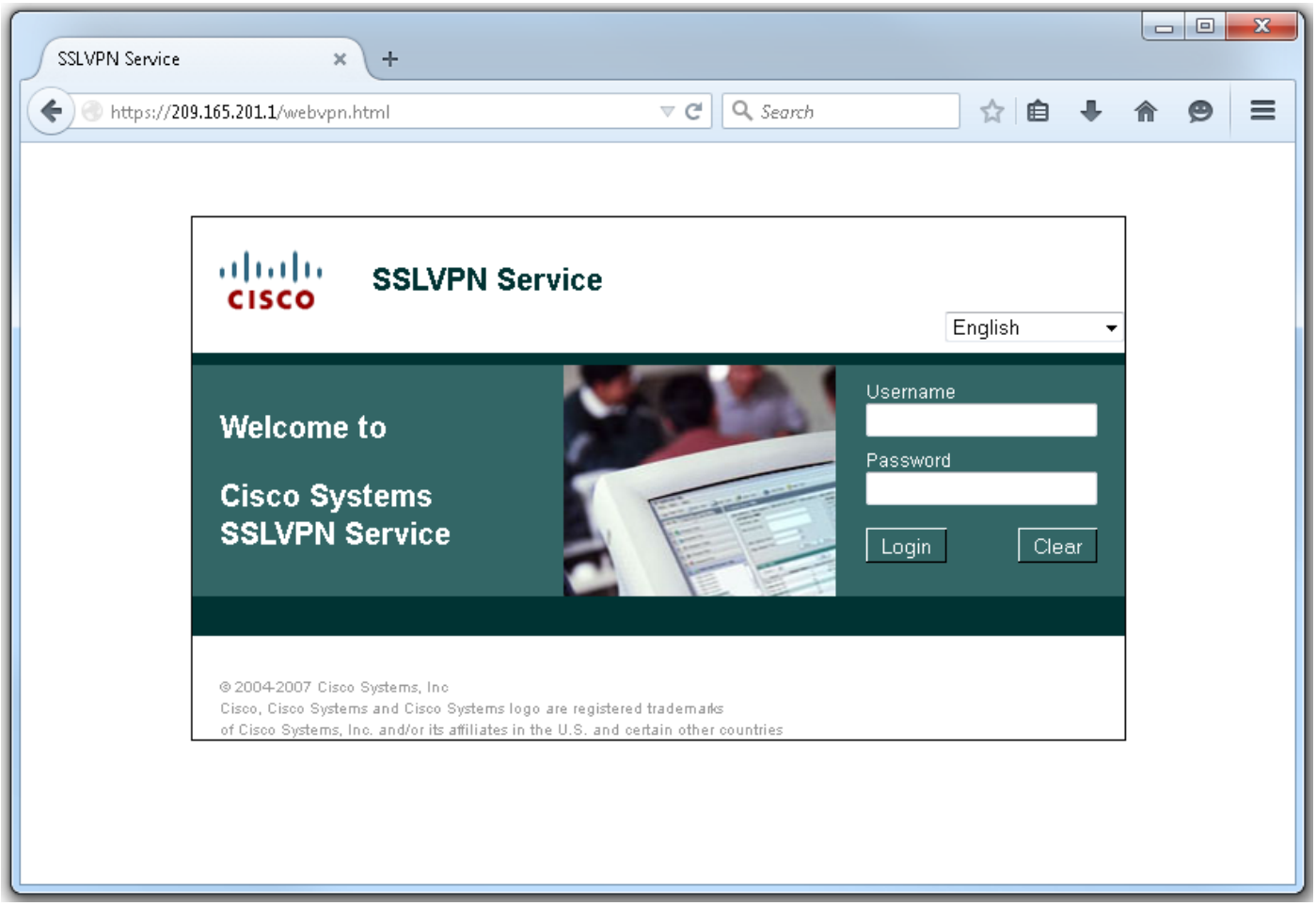
```
webvpn context SSLVPN_CONTEXT
 policy group SSLVPN_POLICY
 svc profile SSLVPN_PROFILE
```

> **ملاحظة**: أستخدم أداة بحث الأوامر (للعملاء المسجلين فقط) للحصول على مزيد من المعلومات حول الأوامر المستخدمة في هذا القسم.

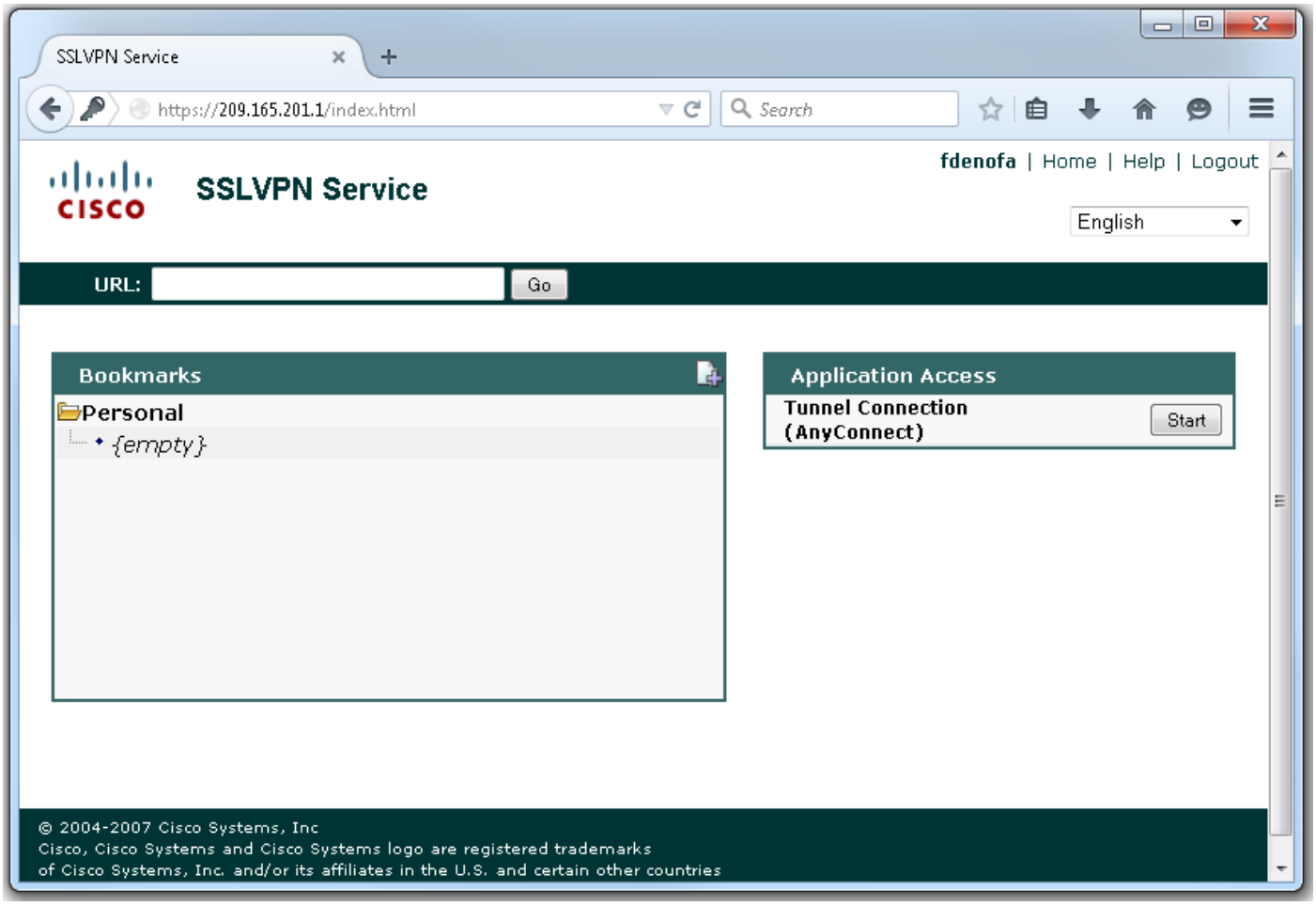
التحقق من الصحة

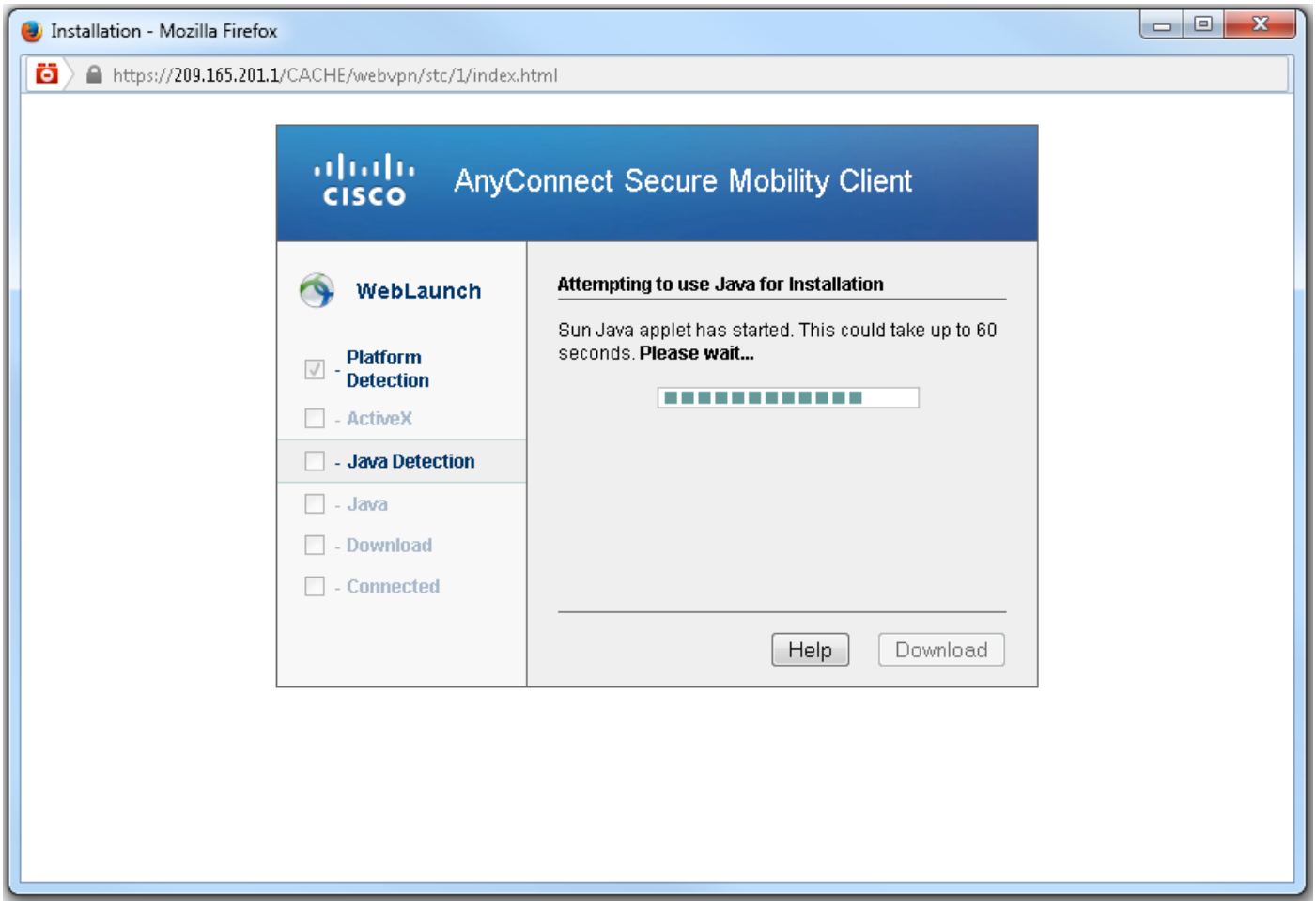
استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

بمجرد اكتمال التكوين، فعند الوصول إلى عنوان البوابة ومنفذها عبر المستعرض، سوف يعود إلى صفحة ترحيل WebVPN.



بعد تسجيل الدخول، يتم عرض الصفحة الرئيسية ل WebVPN. من هنا، انقر على **اتصال النفق (AnyConnect).** عند إستخدام Internet Explorer، يتم إستخدام ActiveX لخفض عميل AnyConnect وتثبيته. في حالة عدم اكتشافه، سيتم إستخدام Java بدلا من ذلك. تستخدم كافة المستعرضات الأخرى Java على الفور.

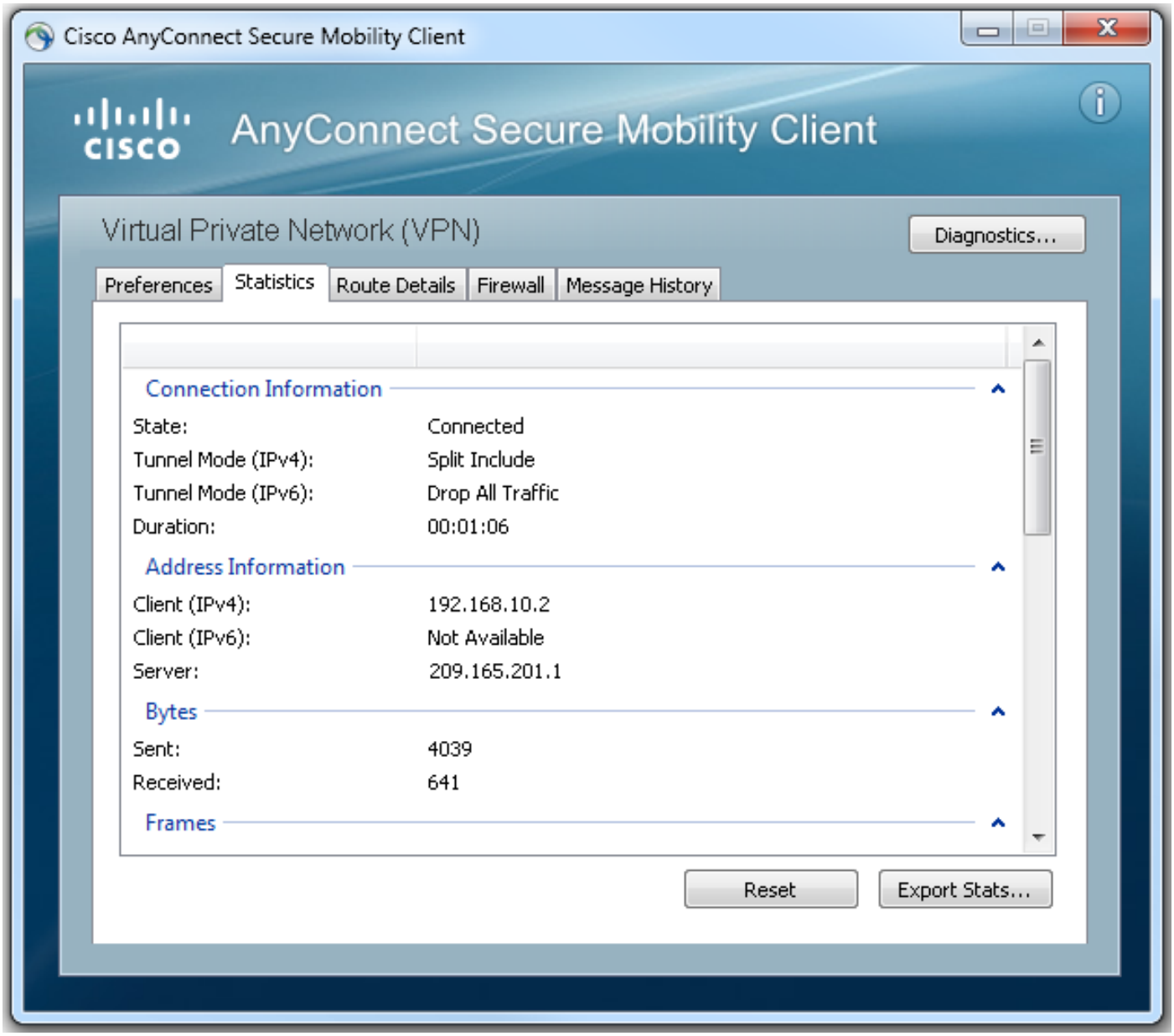


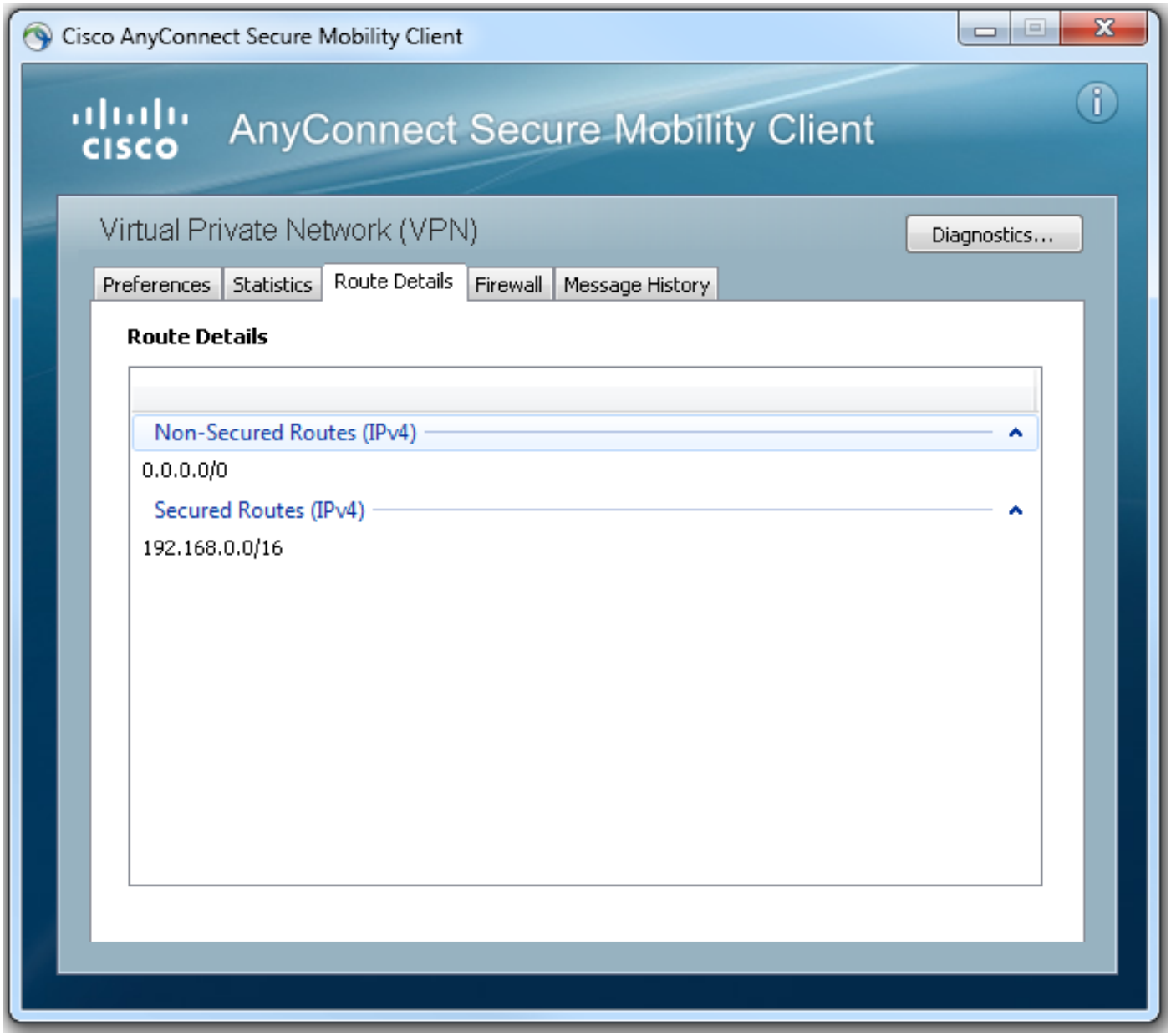


بمجرد اكتمال التثبيت، سيحاول AnyConnect تلقائيا الاتصال بوابة WebVPN. نظرا لاستخدام شهادة موقعة ذاتيا للعبارة لتعريف نفسها، ستظهر تحذيرات متعددة للشهادة

أثناء محاولة الاتصال. هذه متوقعة ويجب قبولها لمتابعة الاتصال. لتجنب تحذيرات الترخيص هذه، يجب أن تكون الشهادة ذاتية التوقيع التي يتم تقديمها مثبتة في مخزن الشهادات الموثوق به الخاص بجهاز العميل، أو إذا كانت شهادة جهة خارجية قيد الاستخدام، فيجب أن تكون شهادة المرجع المصدق في مخزن الشهادات الموثوق به.

عندما ينتهي الاتصال من التفاوض، انقر على رمز **التروس** في أسفل يسار AnyConnect، سيعرض بعض المعلومات المتقدمة حول الاتصال. في هذه الصفحة، من الممكن عرض بعض إحصائيات الاتصال وتفاصيل المسار التي تم الوصول إليها من قائمة التحكم في الوصول (ACL) الخاصة بالنفق المقسم في تكوين "نهج المجموعة".


Cisco AnyConnect Secure Mobility Client
AnyConnect Secure Mobility Client
Virtual Private Network (VPN)
Diagnostics...
Preferences
Statistics
Route Details
Firewall
Message History
Connection Information
State: Connected
Tunnel Mode (IPv4): Split Include
Tunnel Mode (IPv6): Drop All Traffic
Duration: 00:01:06
Address Information
Client (IPv4): 192.168.10.2
Client (IPv6): Not Available
Server: 209.165.201.1
Bytes
Sent: 4039
Received: 641
Frames
Reset
Export Stats...



وفيما يلي النتيجة النهائية running-configuration من خطوات التكوين:

```
crypto pki trustpoint SSLVPN_TP_SELFSIGNED
 enrollment selfsigned
 serial-number
 subject-name cn=892_SELF_SIGNED_CERT
 revocation-check none
 rsakeypair SELF_SIGNED_RSA
!
crypto vpn anyconnect flash:/webvpn/anyconnect-win-3.1.08009-k9.pkg sequence 1
crypto vpn anyconnect profile SSLVPN_PROFILE flash:test-profile.xml ! access-list 1 permit
192.168.0.0 0.0.255.255 ! ip local pool SSLVPN_POOL 192.168.10.1 192.168.10.10 ! webvpn gateway
SSLVPN_GATEWAY ip address 209.165.201.1 port 443 ssl trustpoint SSLVPN_TP_SELFSIGNED inservice !
webvpn context SSLVPN_CONTEXT virtual-template 1
aaa authentication list SSLVPN_AAA
gateway SSLVPN_GATEWAY
! ssl authenticate verify all inservice ! policy group SSLVPN_POLICY functions svc-enabled svc
address-pool "SSLVPN_POOL" netmask 255.255.255.0 svc split include acl 1 svc dns-server primary
8.8.8.8
svc profile SSLVPN_PROFILE default-group-policy SSLVPN_POLICY
```

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكن استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

هناك عدد قليل من المكونات المشتركة للتحقق منها عند أستكشاف أخطاء اتصال AnyConnect وإصلاحها:

- بما أن العميل يجب أن يقدم شهادة، فمن الضروري أن تكون الشهادة المحددة في بوابة WebVPN صحيحة. لإصدار **شهادة** PKI **show crypto** تظهر المعلومات المتعلقة بجميع الشهادات على الموجه.
- عند إجراء تغييرات على تكوين WebVPN، فمن أفضل الممارسات إصدار no inservice and inService على كل من البوابة والسياق. وهذا يضمن أن التغييرات ستدخل حيز التنفيذ بشكل صحيح.
- كما تمت الإشارة سابقا، من الضروري توفر وحدة PKG خاصة ب AnyConnect لكل نظام تشغيل عميل سيتم توصيله بهذه البوابة. على سبيل المثال، تتطلب عملاء Linux إصدار 32 بت PKG لنظام Linux، وتتطلب عملاء Windows Windows PKG لنظام Windows، إصدار 32 بت، وهكذا.
- عندما تضع في الاعتبار كل من عميل AnyConnect وشبكة WebVPN المستندة إلى المستعرض المستخدم SSL، لتكون قادرا على الوصول إلى صفحة ترحيل WebVPN (مع افتراض أن AnyConnect ستكون قادرة على الاتصال) تشير بشكل عام إلى أن AnyConnect المناسب صحيح).

يوفر Cisco IOS بعض خيارات تصحيح الأخطاء المختلفة ل WebVPN التي يمكن استخدامها لاستكشاف أخطاء الاتصالات الفاشلة وإصلاحها. هذا هو المخرج الذي تم إنشاؤه من debug webVPN aaa، و debug wevpn tunnel، و show webVPN session عند محاولة اتصال ناجحة:

```
fdenofa-892#show debugging


WebVPN Subsystem:
  WebVPN AAA debugging is on
  WebVPN tunnel debugging is on
  WebVPN Tunnel Events debugging is on
  WebVPN Tunnel Errors debugging is on


*May 26 20:11:06.381: WV-AAA: Nas Port ID set to 64.102.157.2.
*May 26 20:11:06.381: WV-AAA: AAA authentication request sent for user: "VPNUSER"AAA returned
status: 2 for session 37
*May 26 20:11:06.381: WV-AAA: AAA Authentication Passed!
*May 26 20:11:06.381: WV-AAA: User "VPNUSER" has logged in from "64.102.157.2" to gateway
"SSLVPN_GATEWAY"
             context "SSLVPN_CONTEXT"
*May 26 20:11:12.265:
*May 26 20:11:12.265:
*May 26 20:11:12.265: [WV-TUNL-EVT]:[8A3AE410] CSTP Version recd , using 1
*May 26 20:11:12.265: [WV-TUNL-EVT]:[8A3AE410] Allocating IP 192.168.10.9 from address-pool
SSLVPN_POOL
*May 26 20:11:12.265: [WV-TUNL-EVT]:[8A3AE410] Using new allocated IP 192.168.10.9 255.255.255.0
*May 26 20:11:12.265:  Inserting static route: 192.168.10.9 255.255.255.255 Virtual-Access2 to
routing table
*May 26 20:11:12.265: [WV-TUNL-EVT]:[8A3AE410] Full Tunnel CONNECT request processed, HTTP reply
created
*May 26 20:11:12.265: HTTP/1.1 200 OK
*May 26 20:11:12.265: Server: Cisco IOS SSLVPN
```

```
*May 26 20:11:12.265: X-CSTP-Version: 1
*May 26 20:11:12.265: X-CSTP-Address: 192.168.10.9
*May 26 20:11:12.269: X-CSTP-Netmask: 255.255.255.0
*May 26 20:11:12.269: X-CSTP-Keep: false
*May 26 20:11:12.269: X-CSTP-DNS: 8.8.8.8
*May 26 20:11:12.269: X-CSTP-Lease-Duration: 43200
*May 26 20:11:12.269: X-CSTP-MTU: 1280
*May 26 20:11:12.269: X-CSTP-Split-Include: 192.168.0.0/255.255.0.0
*May 26 20:11:12.269: X-CSTP-DPD: 300
*May 26 20:11:12.269: X-CSTP-Disconnected-Timeout: 2100
*May 26 20:11:12.269: X-CSTP-Idle-Timeout: 2100
*May 26 20:11:12.269: X-CSTP-Session-Timeout: 0
*May 26 20:11:12.269: X-CSTP-Keepalive: 30
*May 26 20:11:12.269: X-DTLS-Session-ID:
85939A3FE33ABAE5F02F8594D56DEDE389F6FB3C9EEC4D211EB71C0820DF8DC8
*May 26 20:11:12.269: X-DTLS-Port: 443
*May 26 20:11:12.269: X-DTLS-Header-Pad-Length: 3
*May 26 20:11:12.269: X-DTLS-CipherSuite: AES256-SHA
*May 26 20:11:12.269: X-DTLS-DPD: 300
*May 26 20:11:12.269: X-DTLS-KeepAlive: 30
*May 26 20:11:12.269:
*May 26 20:11:12.269:
*May 26 20:11:12.269:
*May 26 20:11:12.269: [WV-TUNL-EVT]:[8A3AE410] For User VPNUSER, DPD timer started for 300
seconds
*May 26 20:11:12.273: [WV-TUNL-EVT]:[8A3AE410] CSTP Control, Recvd a Req Cntl Frame (User
VPNUSER, IP 192.168.10.9)
Severity ERROR, Type CLOSE_ERROR
Text: reinitiate tunnel to negotiate a different MTU
*May 26 20:11:12.273: [WV-TUNL-EVT]:[8A3AE410] CSTP Control, Recvd Close Error Frame
*May 26 20:11:14.105:
*May 26 20:11:14.105:
*May 26 20:11:14.105: [WV-TUNL-EVT]:[8A3AE690] CSTP Version recd , using 1
*May 26 20:11:14.109: [WV-TUNL-EVT]:[8A3AE690] Tunnel Client reconnecting removing existing tunl
ctx
*May 26 20:11:14.109: [WV-TUNL-EVT]:[8A3AE410] Closing Tunnel Context 0x8A3AE410 for Session
0x8A3C2EF8 and User VPNUSER
*May 26 20:11:14.109: [WV-TUNL-EVT]:[8A3AE690] Reusing IP 192.168.10.9 255.255.255.0
*May 26 20:11:14.109:  Inserting static route: 192.168.10.9 255.255.255.255 Virtual-Access2 to
routing table
*May 26 20:11:14.109: [WV-TUNL-EVT]:[8A3AE690] Full Tunnel CONNECT request processed, HTTP reply
created
*May 26 20:11:14.109: HTTP/1.1 200 OK
*May 26 20:11:14.109: Server: Cisco IOS SSLVPN
*May 26 20:11:14.109: X-CSTP-Version: 1
*May 26 20:11:14.109: X-CSTP-Address: 192.168.10.9
*May 26 20:11:14.109: X-CSTP-Netmask: 255.255.255.0
*May 26 20:11:14.109: X-CSTP-Keep: false
*May 26 20:11:14.109: X-CSTP-DNS: 8.8.8.8
*May 26 20:11:14.113: X-CSTP-Lease-Duration: 43200
*May 26 20:11:14.113: X-CSTP-MTU: 1199
*May 26 20:11:14.113: X-CSTP-Split-Include: 192.168.0.0/255.255.0.0
*May 26 20:11:14.113: X-CSTP-DPD: 300
*May 26 20:11:14.113: X-CSTP-Disconnected-Timeout: 2100
*May 26 20:11:14.113: X-CSTP-Idle-Timeout: 2100
*May 26 20:11:14.113: X-CSTP-Session-Timeout: 0
*May 26 20:11:14.113: X-CSTP-Keepalive: 30
*May 26 20:11:14.113: X-DTLS-Session-ID:
22E54D9F1F6344BCB5BB30BC8BB3737907795E6F3C3665CDD294CBBA1DA4D0CF
*May 26 20:11:14.113: X-DTLS-Port: 443
*May 26 20:11:14.113: X-DTLS-Header-Pad-Length: 3
*May 26 20:11:14.113: X-DTLS-CipherSuite: AES256-SHA
*May 26 20:11:14.113: X-DTLS-DPD: 300
*May 26 20:11:14.113: X-DTLS-KeepAlive: 30
```

```
*May 26 20:11:14.113:
*May 26 20:11:14.113:
*May 26 20:11:14.113:
*May 26 20:11:14.113: [WV-TUNL-EVT]:[8A3AE690] For User VPNUSER, DPD timer started for 300
seconds
```

```
fdenofa-892#show webvpn session user VPNUSER context SSLVPN_CONTEXT

Session Type      : Full Tunnel
Client User-Agent : AnyConnect Windows 3.1.08009

Username          : VPNUSER              Num Connection : 5
Public IP         : 64.102.157.2         VRF Name       : None
Context           : SSLVPN_CONTEXT       Policy Group   : SSLVPN_POLICY
Last-Used         : 00:00:00             Created        : *16:11:06.381 EDT Tue May 26 2015
Session Timeout   : Disabled             Idle Timeout   : 2100
DNS primary serve : 8.8.8.8
DPD GW Timeout    : 300                  DPD CL Timeout : 300
Address Pool      : SSLVPN_POOL          MTU Size       : 1199
Rekey Time        : 3600                 Rekey Method   :
Lease Duration    : 43200
Tunnel IP         : 192.168.10.9         Netmask        : 255.255.255.0
Rx IP Packets     : 0                    Tx IP Packets  : 42
CSTP Started      : 00:00:13             Last-Received  : 00:00:00
CSTP DPD-Req sent : 0                    Virtual Access : 2
Msie-ProxyServer  : None                 Msie-PxyPolicy : Disabled
Msie-Exception    :
Split Include     : ACL 1
Client Ports      : 17462 17463 17464 17465 17471
```

معلومات ذات صلة

- دليل تكوين SSL VPN، Cisco IOS، الإصدار 15M&T
- عميل AnyConnect VPN (SSL) على موجه IOS باستخدام مثال تكوين CCP
- الدعم التقني والمستندات - Cisco Systems

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).