AnyConnect Konfigurieren eines grundlegenden SSL VPNs für das Cisco IOS-Router-Headend mit CLI

Einführung

Inhalt

Dieses Dokument beschreibt die grundlegende Konfiguration eines Cisco IOS® Routers als AnyConnect Secure Sockets Layer VPN (SSL VPN)-Headend.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco IOS
- AnyConnect Secure Mobility Client
- Allgemeiner SSL-Betrieb

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco 892W-Router mit 15.3(3)M5
- AnyConnect Secure Mobility Client 3.1.08009

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

Lizenzinformationen für verschiedene IOS-Versionen

- Das Feature-Set securityk9 ist für die Verwendung der SSL VPN-Funktionen erforderlich, unabhängig davon, welche Cisco IOS-Version verwendet wird.
- Cisco IOS 12.x: Die SSL VPN-Funktion ist in alle 12.x-Images integriert, die mit 12.4(6)T beginnen und mindestens über eine Sicherheitslizenz (d. h. adventerprisek9 usw.).
- Cisco IOS 15.0 - Bei früheren Versionen muss auf dem Router eine LIC-Datei installiert werden, die 10, 25 oder 100 Benutzerverbindungen ermöglicht. Nutzungsrechte* Lizenzen wurden in 15.0(1)M4 implementiert
- Cisco IOS 15.1 - Bei früheren Versionen muss auf dem Router eine LIC-Datei installiert werden, die 10, 25 oder 100 Benutzerverbindungen ermöglicht. Nutzungsrechte* Lizenzen wurden in 15.1(1)T2, 15.1(2)T2, 15.1(3)T und 15.1(4)M1 implementiert
- Cisco IOS 15.2 - Alle 15.2-Versionen bieten Nutzungsrechte* Lizenzen für SSL VPN.
- Cisco IOS 15.3 und höher: Ältere Versionen bieten Nutzungsrechte* Lizenzen. Ab 15.3(3)M ist die SSL VPN-Funktion verfügbar, nachdem Sie das SecureK9-Technologiepaket gestartet haben

Für die RTU-Lizenzierung wird eine Evaluierungslizenz aktiviert, wenn die erste Webvpn-Funktion konfiguriert wurde (das heißt das webvpn-Gateway GATEWAY1) und der Endbenutzer-Lizenzvertrag (EULA) akzeptiert wurde. Nach 60 Tagen wird diese Testlizenz zu einer permanenten Lizenz. Diese Lizenzen sind honorarbasiert und erfordern eine Papierlizenz, um diese Funktion nutzen zu können. Darüber hinaus ermöglicht der RTU-Wert nicht die Beschränkung auf eine bestimmte Anzahl von Anwendungen, sondern die gleichzeitige Unterstützung mehrerer Verbindungen durch die Router-Plattform.

Erhebliche Software-Erweiterungen

Diese Bug-IDs führten zu wichtigen Funktionen oder Fixes für AnyConnect:

- CSCti89976: Unterstützung für AnyConnect 3.x zu IOS hinzugefügt
- CSCtx38806: Fehlerbehebung für BEAST-Schwachstellen, Microsoft KB2585542

Konfiguration

Schritt 1: Lizenz bestätigen ist aktiviert

Der erste Schritt bei der Konfiguration von AnyConnect auf einem IOS-Router-Headend besteht darin, zu überprüfen, ob die Lizenz korrekt installiert (falls zutreffend) und aktiviert wurde. Die Lizenzspezifikationen für verschiedene Versionen finden Sie in den Lizenzinformationen im vorherigen Abschnitt. Es hängt von der Version des Codes und der Plattform ab, ob die show-Lizenz eine SSL_VPN- oder Security9-Lizenz enthält. Unabhängig von der Version und Lizenz muss der EULA akzeptiert werden, und die Lizenz wird als aktiv angezeigt.

Schritt 2: Laden Sie das AnyConnect Secure Mobility Client-Paket auf den Router hoch, und installieren Sie es.

Um ein AnyConnect-Image in das VPN hochzuladen, dient das Headend zwei Zwecken. Erstens dürfen nur Betriebssysteme mit AnyConnect-Images am AnyConnect-Headend eine Verbindung herstellen. Windows-Clients benötigen beispielsweise ein Windows-Paket, um auf dem Headend installiert zu werden, Linux 64-Bit-Clients benötigen ein Linux 64-Bit-Paket usw. Zweitens wird das auf dem Headend installierte AnyConnect-Image beim Herstellen einer Verbindung automatisch auf den Client-Computer heruntergefahren. Benutzer, die zum ersten Mal eine Verbindung herstellen, können den Client vom Webportal herunterladen, und Benutzer, die zurückkehren, können ein Upgrade durchführen, vorausgesetzt, das AnyConnect-Paket am Headend ist aktueller als das, was auf ihrem Client-Computer installiert ist.

AnyConnect-Pakete können über den AnyConnect Secure Mobility Client auf der Cisco Software Downloads-Website bezogen werden. Es stehen zwar viele Optionen zur Verfügung, aber die Pakete, die auf dem Headend installiert werden sollen, werden mit dem Betriebssystem und der Head-End-Bereitstellung (PKG) gekennzeichnet. AnyConnect-Pakete sind derzeit für folgende Betriebssysteme verfügbar: Windows, Mac OS X, Linux (32-Bit) und Linux 64-Bit. Beachten Sie, dass es für Linux sowohl 32- als auch 64-Bit-Pakete gibt. Jedes Betriebssystem erfordert, dass das richtige Paket am Headend installiert wird, damit Verbindungen zulässig sind.

Nachdem das AnyConnect-Paket heruntergeladen wurde, kann es mit dem Befehl **copy** über TFTP, FTP, SCP oder einige andere Optionen auf den Flash-Speicher des Routers hochgeladen werden. Hier ein Beispiel:

```
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)
```

Nachdem Sie das AnyConnect-Image in den Flash-Speicher des Routers kopiert haben, muss es über die Befehlszeile installiert werden. Mehrere AnyConnect-Pakete können installiert werden, wenn Sie am Ende des Installationsbefehls eine Folgenummer angeben. Dadurch kann der Router als Headend für mehrere Client-Betriebssysteme fungieren. Wenn Sie das AnyConnect-Paket installieren, wird es auch in das **Flash:/webvpn/-Verzeichnis** verschoben, wenn es ursprünglich nicht kopiert wurde.

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

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

Bei Versionen von Code, die vor 15.2(1)T veröffentlicht wurden, ist der Befehl zur Installation der PKG etwas anders.

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

Schritt 3: Generieren von RSA-Keypair und selbstsigniertem Zertifikat

Wenn Sie SSL oder eine Funktion konfigurieren, die Public Key Infrastructure (PKI) und digitale Zertifikate implementiert, ist für die Signierung des Zertifikats ein Rivest-Shamir-Adleman (RSA)-Tastenfeld erforderlich. Mit diesem Befehl wird ein RSA-Tastenfeld generiert, das dann verwendet wird, wenn das selbst signierte PKI-Zertifikat generiert wird. Verwenden Sie einen 2048-Bit-Modulus, der keine Anforderung darstellt, aber es wird empfohlen, den größten verfügbaren Modulus zu verwenden, um die Sicherheit und Kompatibilität mit den AnyConnect-Client-Geräten zu erhöhen. Es wird außerdem empfohlen, ein beschreibendes Schlüssellabel zu verwenden, das mit der Schlüsselverwaltung zugewiesen wird. Die Schlüsselgenerierung kann mit dem Befehl **show crypto key mypubkey rsa** bestätigt werden.

> **Hinweis:** Da die Exportierbarkeit von RSA-Schlüsseln mit zahlreichen Sicherheitsrisiken verbunden ist, wird empfohlen, sicherzustellen, dass Schlüssel nicht exportierbar sind. Dies ist die Standardeinstellung. Die Risiken, die mit dem Exportieren der RSA-Schlüssel verbunden sind, werden in diesem Dokument behandelt: Bereitstellen von RSA-Schlüsseln innerhalb einer 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
```

Nachdem der RSA-Tastenblock erfolgreich generiert wurde, muss ein PKI-Trustpoint mit den Informationen des Routers und der RSA-Tastenfolge konfiguriert werden. Der Common Name (CN) im Betreffnamen sollte mit der IP-Adresse oder dem Fully Qualified Domain Name (FQDN) konfiguriert werden, die Benutzer für die Verbindung mit dem AnyConnect-Gateway verwenden. In diesem Beispiel verwenden die Clients beim Verbindungsversuch den FQDN fdenofa-SSLVPN.cisco.com. Obwohl dies nicht obligatorisch ist, können Sie durch die korrekte Eingabe in die CN die Anzahl der Zertifikatfehler reduzieren, die bei der Anmeldung angezeigt werden.

> **Hinweis:** Anstatt ein vom Router erstelltes selbstsigniertes Zertifikat zu verwenden, kann ein Zertifikat verwendet werden, das von einer Zertifizierungsstelle eines Drittanbieters ausgestellt wurde. Dies kann mit einigen verschiedenen Methoden erfolgen, wie in diesem Dokument beschrieben: Konfigurieren der Zertifikatregistrierung für eine PKI.

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

Nachdem der Vertrauenspunkt korrekt definiert wurde, muss der Router das Zertifikat mithilfe des Befehls **crypto pki enroll** generieren. Bei diesem Vorgang können einige weitere Parameter wie die Seriennummer und die IP-Adresse angegeben werden. Dies ist jedoch nicht erforderlich. Die Zertifikatgenerierung kann mit dem Befehl **show crypto pki Certificates** bestätigt werden.

```
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
```

Schritt 4: Lokale VPN-Benutzerkonten konfigurieren

Es ist zwar möglich, einen externen AAA-Server (Authentication, Authorization, and Accounting) zu verwenden, in diesem Beispiel wird jedoch die lokale Authentifizierung verwendet. Diese Befehle erstellen einen Benutzernamen VPNUSER und eine AAA-Authentifizierungsliste mit dem Namen SSLVPN_AAA.

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

Schritt 5: Festlegen der von Clients zu verwendenden Adresspool- und Split-Tunnel-Zugriffsliste

Es muss ein lokaler IP-Adresspool erstellt werden, damit AnyConnect Client-Adapter eine IP-Adresse erhalten können. Stellen Sie sicher, dass Sie einen großen Pool konfigurieren, der die maximale Anzahl gleichzeitiger AnyConnect-Clientverbindungen unterstützt.

Standardmäßig wird AnyConnect im vollständigen Tunnelmodus betrieben, d. h. der vom Client-Computer generierte Datenverkehr wird über den Tunnel übertragen. Da dies in der Regel nicht wünschenswert ist, ist es möglich, eine Zugriffskontrollliste (ACL) zu konfigurieren, die dann Datenverkehr definiert, der über den Tunnel gesendet werden soll oder sollte. Wie bei anderen ACL-Implementierungen macht die implizite Ablehnung am Ende die Notwendigkeit einer expliziten Ablehnung überflüssig. Daher ist es nur erforderlich, Genehmigungsanweisungen für den Datenverkehr zu konfigurieren, der getunnelt werden soll.

```
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
```

Schritt 6: Konfigurieren der Virtual-Template Interface (VTI)

Dynamische VTIs für jede VPN-Sitzung eine separate On-Demand-Virtual-Access-Schnittstelle bereitstellen, die hochsichere und skalierbare Verbindungen für VPNs mit Remote-Zugriff ermöglicht. Die DVTI-Technologie ersetzt dynamische Kryptokarten und das dynamische Hub-and-Spoke-Verfahren zur Einrichtung von Tunneln. Da DVTIs wie jede andere reale Schnittstelle funktionieren, ermöglichen sie eine komplexere Bereitstellung des Remote-Zugriffs, da sie QoS, Firewall, benutzerspezifische Attribute und andere Sicherheitsdienste unterstützen, sobald der Tunnel aktiv ist.

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

Schritt 7: Konfigurieren des WebVPN-Gateways

Das WebVPN-Gateway definiert die IP-Adresse und die Port(s), die vom AnyConnect-Headend verwendet werden, sowie den SSL-Verschlüsselungsalgorithmus und das PKI-Zertifikat, das den

Clients präsentiert wird. Standardmäßig unterstützt das Gateway alle möglichen Verschlüsselungsalgorithmen, die je nach Cisco IOS-Version des Routers variieren.

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

Schritt 8: Konfigurieren von WebVPN-Kontext- und Gruppenrichtlinien

Der WebVPN-Kontext und die Gruppenrichtlinie definieren einige zusätzliche Parameter, die für die AnyConnect-Clientverbindung verwendet werden. Bei einer grundlegenden AnyConnect-Konfiguration dient der Kontext lediglich als Mechanismus zum Aufrufen der Standardgruppenrichtlinie, die für AnyConnect verwendet wird. Der Kontext kann jedoch verwendet werden, um die WebVPN-Splash-Seite und den WebVPN-Vorgang weiter anzupassen. In der definierten Richtliniengruppe wird die Liste SSLVPN_AAA als AAA-Authentifizierungsliste konfiguriert, der die Benutzer angehören. Der Befehl **funktional svc-enabled** ist die Konfigurationsdatei, die Benutzern die Verbindung mit dem AnyConnect SSL VPN Client und nicht nur mit WebVPN über einen Browser ermöglicht. Schließlich definieren die zusätzlichen SVC-Befehle Parameter, die nur für SVC-Verbindungen relevant sind: **svc address-pool** weist das Gateway an, Adressen im SSLVPN_POOL an die Clients zu übergeben, **svc split** definiert die Split-Tunnel-Richtlinie pro oben definierter ACL 1, und **svc dns-server** definiert den DNS-Server, der für die Auflösung von Domänennamen verwendet wird. Bei dieser Konfiguration werden alle DNS-Abfragen an den angegebenen DNS-Server gesendet. Die Adresse, die in der Abfrageantwort empfangen wird, bestimmt, ob der Datenverkehr über den Tunnel gesendet wird.

```
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
```

Schritt 9 (Optional) Konfigurieren eines Clientprofils

Anders als bei ASAs verfügt Cisco IOS nicht über eine integrierte Benutzeroberfläche, die Administratoren bei der Erstellung des Clientprofils unterstützen kann. Das AnyConnect-Clientprofil muss mit dem Stand-Alone Profile Editor separat erstellt/bearbeitet werden.

> **Tipp:** Suchen Sie anyconnect-profile-editor-win-3.1.03103-k9.exe.

Führen Sie die folgenden Schritte aus, um vom Router das Profil bereitzustellen:

- Laden Sie sie mithilfe von ftp/tftp in IOS Flash hoch.
- Verwenden Sie diesen Befehl, um das Profil zu identifizieren, das gerade hochgeladen wurde:

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

> **Tipp:** In Cisco IOS-Versionen, die älter als 15.2(1)T sind, muss dieser Befehl verwendet

werden: **webvpn import svc profile <profile_name> flash:<profile.xml>**

3. Verwenden Sie im Kontext diesen Befehl, um das Profil mit diesem Kontext zu verknüpfen:

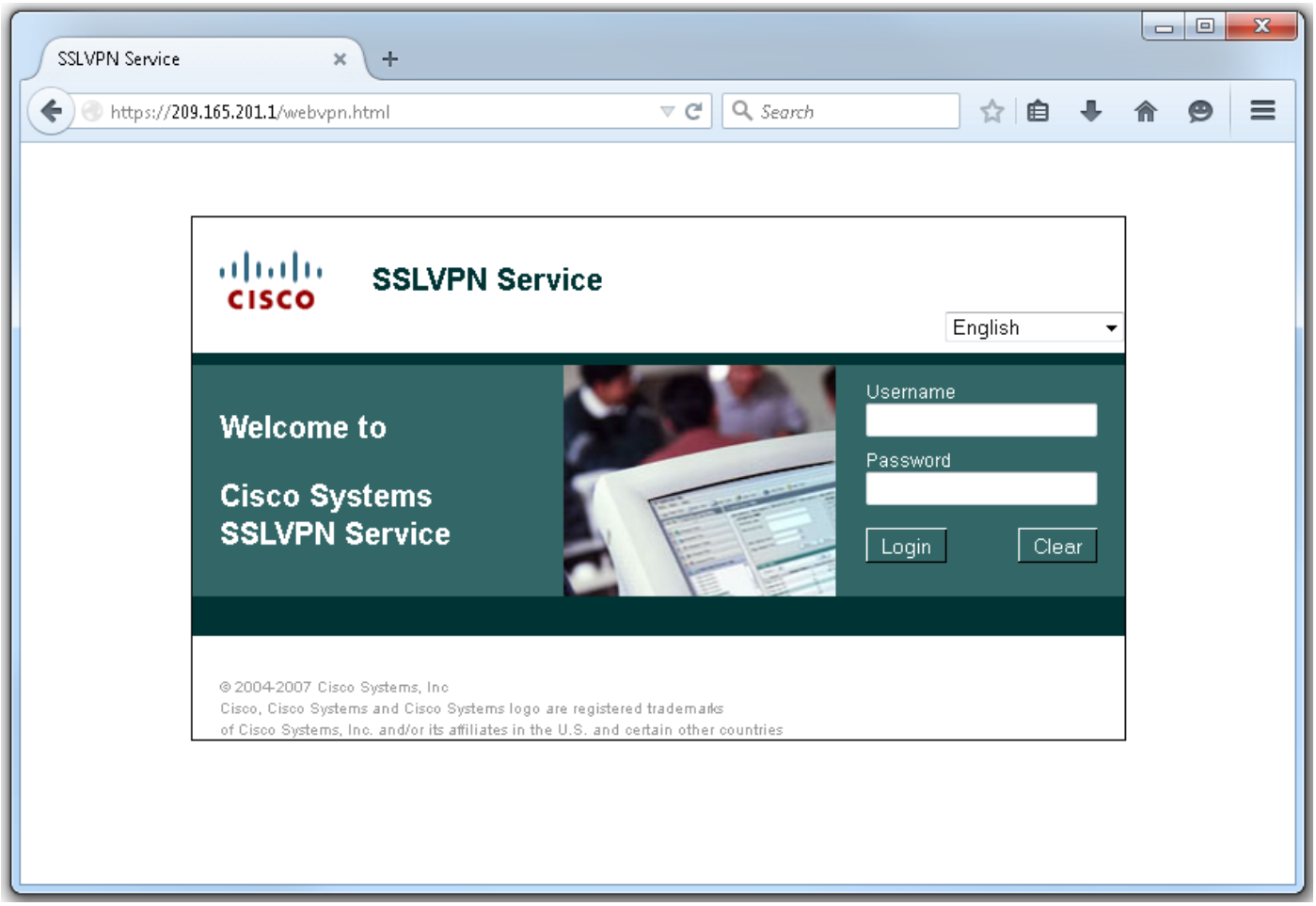
```
webvpn context SSLVPN_CONTEXT
 policy group SSLVPN_POLICY
 svc profile SSLVPN_PROFILE
```

Hinweis: Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

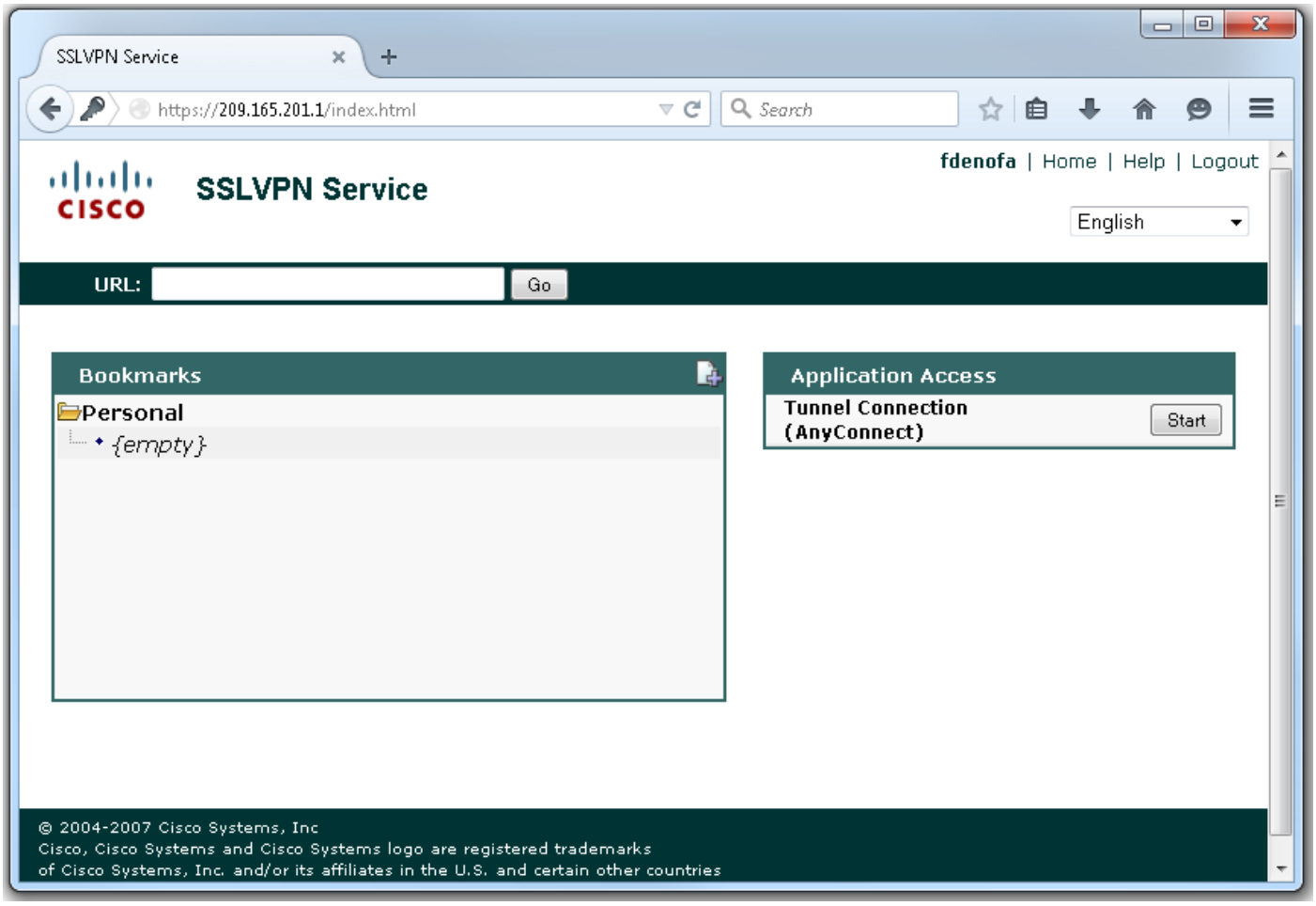
Überprüfung

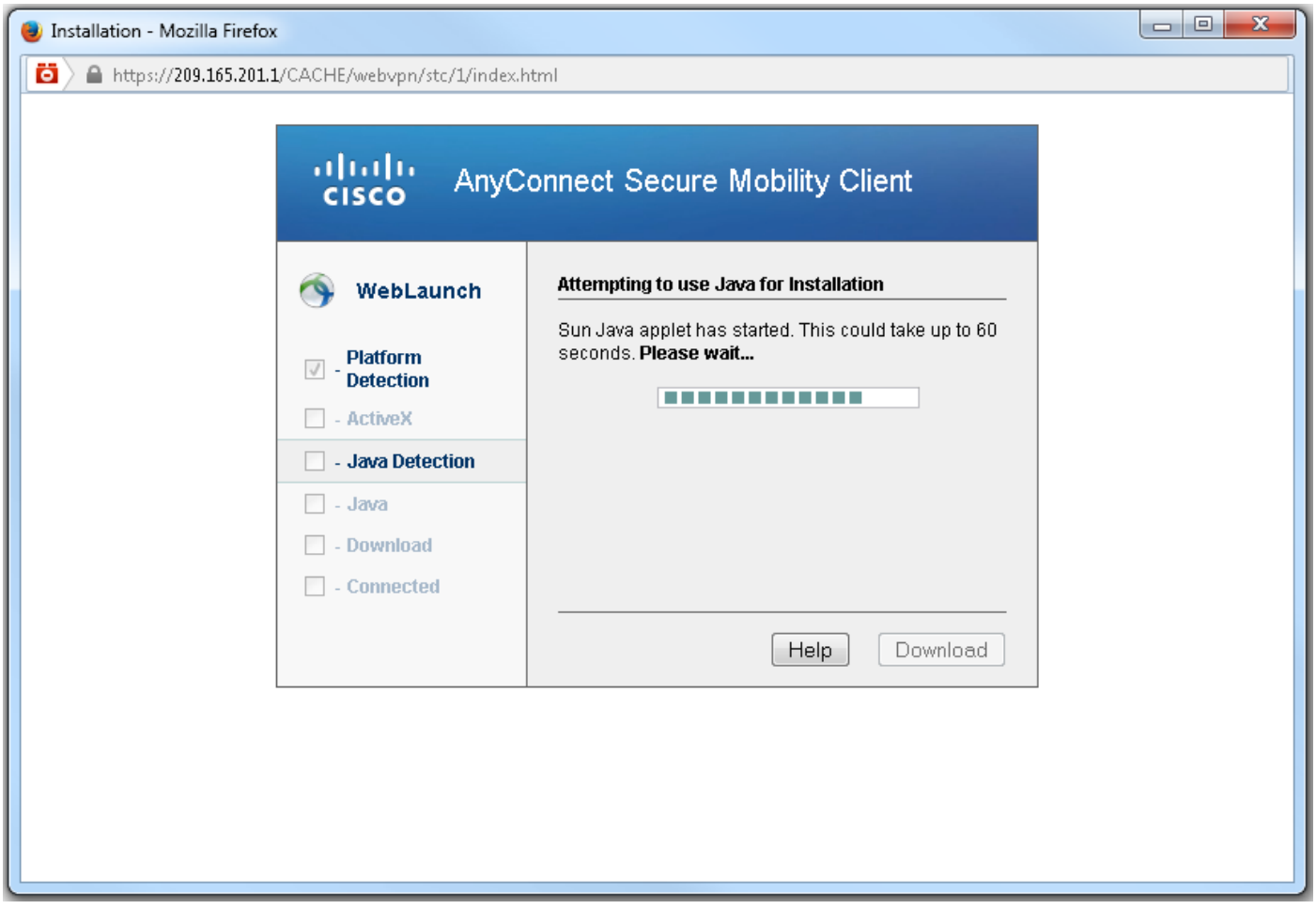
In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Wenn die Konfiguration abgeschlossen ist und Sie über einen Browser auf die Gateway-Adresse und den Port zugreifen, kehrt sie zur WebVPN-Splash-Seite zurück.



Nach der Anmeldung wird die WebVPN-Startseite angezeigt. Klicken Sie von hier auf **Tunnel Connection (AnyConnect).** Wenn Internet Explorer verwendet wird, wird ActiveX zum Herunterdrücken und Installieren des AnyConnect-Clients verwendet. Wird sie nicht erkannt, wird stattdessen Java verwendet. Alle anderen Browser verwenden sofort Java.

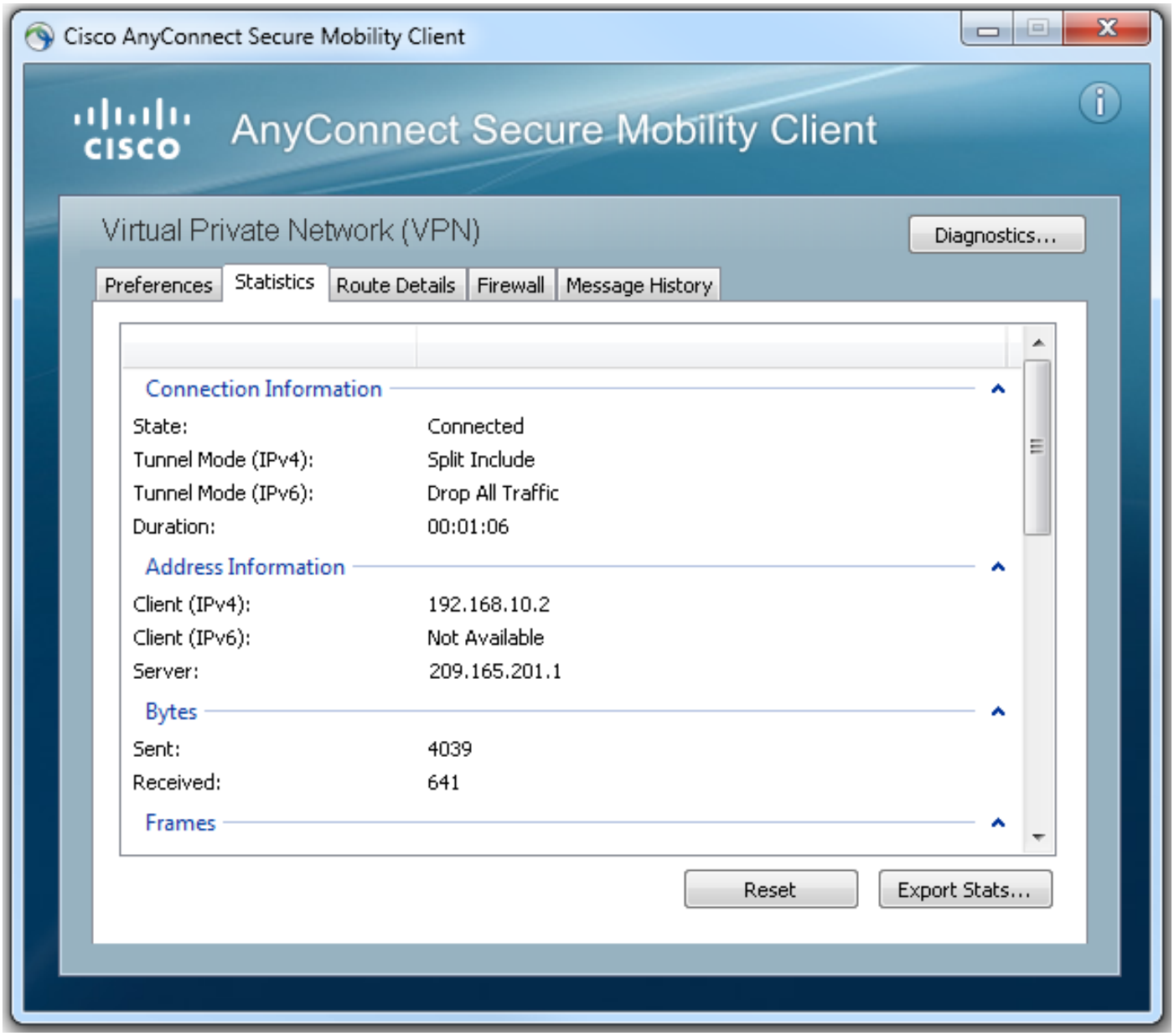


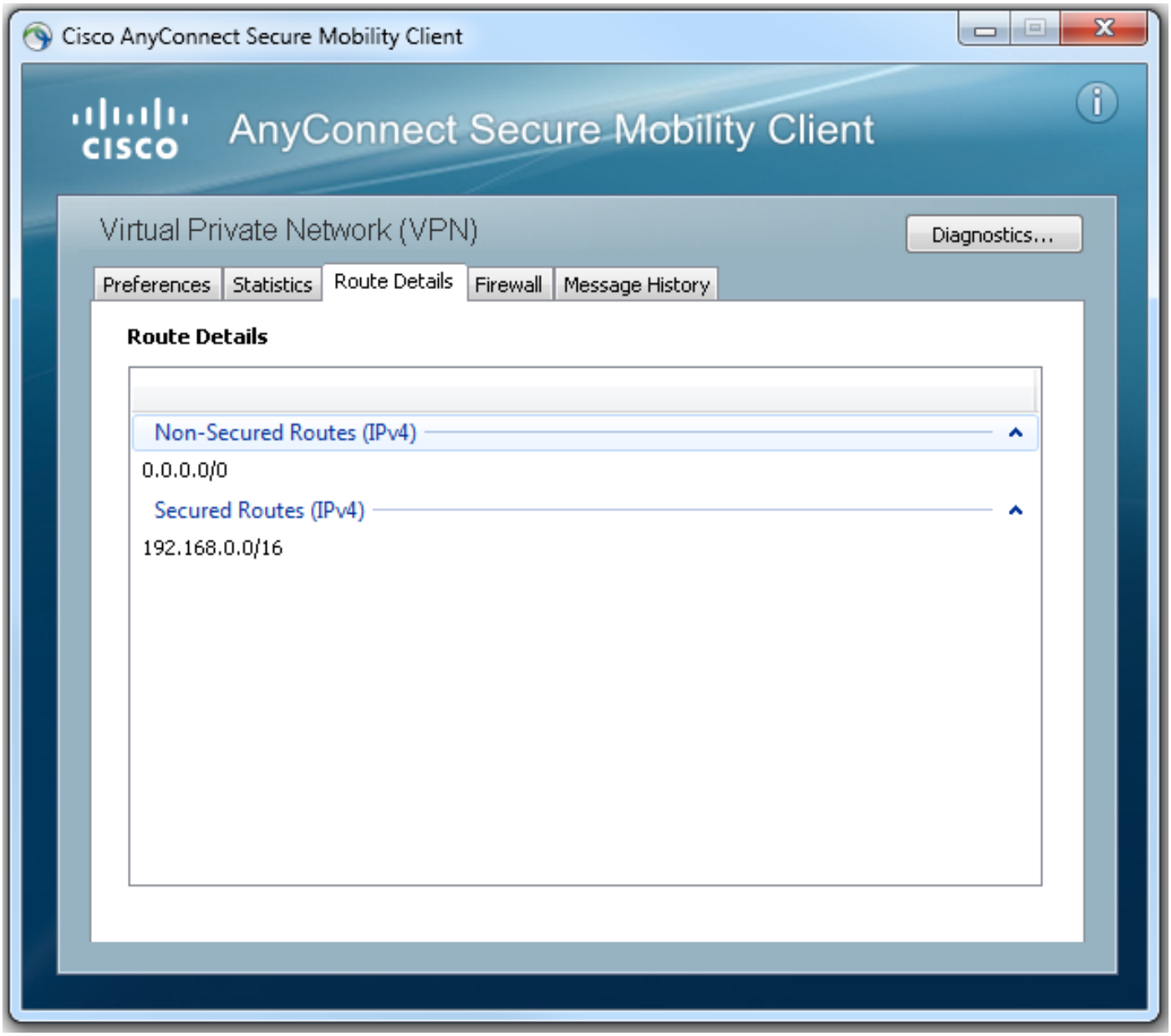


Nach Abschluss der Installation versucht AnyConnect automatisch, eine Verbindung zum WebVPN-Gateway herzustellen. Da ein selbstsigniertes Zertifikat für die Identifizierung des

Gateways verwendet wird, werden beim Verbindungsversuch mehrere Zertifikatwarnungen angezeigt. Diese werden erwartet und müssen akzeptiert werden, damit die Verbindung fortgesetzt werden kann. Um diese Zertifikatswarnungen zu vermeiden, muss das selbst signierte Zertifikat, das präsentiert wird, im vertrauenswürdigen Zertifikatsspeicher des Clientcomputers installiert werden. Wenn ein Drittanbieterzertifikat verwendet wird, muss das Zertifikat der Zertifizierungsstelle im vertrauenswürdigen Zertifikatsspeicher gespeichert sein.

Wenn die Verbindung die Aushandlung abgeschlossen hat, klicken Sie auf das Symbol **Zahnrad** in der linken unteren Ecke von AnyConnect, um erweiterte Informationen über die Verbindung anzuzeigen. Auf dieser Seite können Sie in der Gruppenrichtlinienkonfiguration einige Verbindungsstatistiken und Routendetails anzeigen, die über die Split-Tunnel-ACL erreicht wurden.


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...



Das Ergebnis der Ausführungskonfiguration aus den Konfigurationsschritten ist wie folgt:

```
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
```

Fehlerbehebung

Dieser Abschnitt enthält Informationen, die Sie zur Fehlerbehebung bei Ihrer Konfiguration verwenden können.

Es gibt einige gebräuchliche Komponenten, auf die Sie beim Beheben von Problemen mit der AnyConnect-Verbindung achten sollten:

- Da der Client ein Zertifikat vorlegen muss, muss das im WebVPN-Gateway angegebene Zertifikat gültig sein. Um ein **show crypto pki-Zertifikat** auszustellen, werden Informationen angezeigt, die sich auf alle Zertifikate auf dem Router beziehen.
- Wenn an der WebVPN-Konfiguration Änderungen vorgenommen werden, sollten sowohl im Gateway als auch im Kontext keine In-Service- und In-Service-Änderungen vorgenommen werden. Dadurch wird sichergestellt, dass die Änderungen ordnungsgemäß wirksam werden.
- Wie bereits erwähnt, muss für jedes Client-Betriebssystem, das mit diesem Gateway verbunden wird, eine AnyConnect-PKG-Vereinbarung vorhanden sein. Windows-Clients benötigen z. B. eine Windows PKG, Linux 32-Bit-Clients benötigen eine Linux 32-Bit-PKG usw.
- Wenn Sie sowohl den AnyConnect-Client als auch das browserbasierte WebVPN für die Verwendung von SSL in Betracht ziehen, bedeutet dies für den Zugriff auf die WebVPN-Splash-Seite im Allgemeinen, dass AnyConnect Verbindungen herstellen kann (unter der Annahme, dass die entsprechende AnyConnect-Konfiguration korrekt ist).

Cisco IOS bietet eine Reihe von Debug-WebPN-Optionen, mit denen Fehler bei Verbindungen behoben werden können. Dies ist die Ausgabe, die von debug webvpn aaa, debug wevpn tunnel und show webvpn session bei einem erfolgreichen Verbindungsversuch generiert wird:

```
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
```

Zugehörige Informationen

- SSL VPN-Konfigurationsleitfaden, Cisco IOS Release 15M&T
- Konfigurationsbeispiel für AnyConnect VPN (SSL)-Client auf dem IOS-Router mit CCP
- Technischer Support und Dokumentation für Cisco Systeme