AnyConnect: Configureer basis-SSL VPN voor Cisco IOS-routerhead-end met CLI

Inleiding

Inhoud

Dit document beschrijft de basisconfiguratie van een Cisco IOS® router als een AnyConnect Secure Socket Layer VPN (SSL VPN) Head-end.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco IOS-Cisco
- AnyConnect beveiligde mobiliteit-client
- Algemene SSL-handeling

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco 892W router met 15.3(3)M5
- AnyConnect beveiligde mobiliteit-client 3.1.0809

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Achtergrondinformatie

Licentie-informatie voor verschillende IOS-versies

- De security9 optie is vereist om de SSL VPN functies te gebruiken, ongeacht welke Cisco IOS versie wordt gebruikt.
- Cisco IOS 12.x - de SSL VPN-functie is geïntegreerd in alle 12.x-afbeeldingen die beginnen met 12.4(6)T en ten minste een beveiligingslicentie hebben (dat wil zeggen. advsecurity (k9, adventerprisek9, enzovoort).
- Cisco IOS 15.0 - eerdere versies vereisen een LIC-bestand dat op de router moet worden geïnstalleerd zodat 10, 25 of 100 gebruikersverbindingen mogelijk zijn. Recht op gebruik* licenties zijn geïmplementeerd in 15.0(1)M4
- Cisco IOS 15.1 - eerdere versies vereisen dat een LIC-bestand op de router wordt geïnstalleerd zodat 10, 25 of 100 gebruikersverbindingen mogelijk zijn. Recht op gebruik*-licenties zijn geïmplementeerd in 15.1(1)T2, 15.1(2)T2, 15.1(3)T en 15.1(4)M1
- Cisco IOS 15.2 - alle 15.2 versies bieden recht op gebruik*-licenties voor SSLVPN
- Cisco IOS 15.3 en hoger - eerdere versies bieden het recht om* licenties te gebruiken. Vanaf 15.3(3)M is de SSLVPN-functie beschikbaar nadat u hebt opgestart in een security k9 technologie-pakket

Voor RTU-licenties wordt een evaluatielicentie ingeschakeld wanneer de eerste webverbinding is geconfigureerd (dat wil zeggen, webgateway GATEWAY1) en de Gebruiksrechtovereenkomst (EULA) is geaccepteerd. Na 60 dagen wordt deze licentie een permanente licentie. Deze licenties zijn op basis van eer aangeschaft en vereisen een papieren licentie om deze optie te kunnen gebruiken. Bovendien, in plaats van beperkt te zijn tot een bepaald aantal toepassingen, staat de RTU toe voor het maximum aantal gelijktijdige verbindingen dat het routerplatform tegelijkertijd kan ondersteunen.

Belangrijke softwareverbeteringen

Deze bug-ID's hebben belangrijke functies of oplossingen voor AnyConnect opgeleverd:

- CSCti8976: extra ondersteuning voor AnyConnect 3.x aan IOS
- CSCtx3806: Fix voor kwetsbaarheid bij BEAST, Microsoft KB2585542

Configureren

Stap 1. Controleer dat Licentie is ingeschakeld

De eerste stap wanneer AnyConnect op een IOS-routerhead-end wordt geconfigureerd is om te bevestigen dat de licentie correct geïnstalleerd (indien van toepassing) en ingeschakeld is. Raadpleeg de licentieinformatie in de voorgaande sectie voor de licentiespecificaties in verschillende versies. Het hangt af van de versie van code en platform of de show licentie een SSL_VPN of een security9 licentie identificeert. Ongeacht de versie en licentie moet de EULA worden geaccepteerd en de licentie wordt weergegeven als actief.

Stap 2. AnyConnect Secure Mobility Client-pakket op router uploaden en installeren

Om een AnyConnect-afbeelding naar VPN te uploaden, heeft de head-end twee doeleinden. Ten eerste zijn alleen besturingssystemen met AnyConnect-afbeeldingen die op de AnyConnect-head-end zijn aangebracht, toegestaan. Voor Windows clients is bijvoorbeeld vereist dat er een Windows-pakket op het head-end wordt geïnstalleerd, voor Linux 64-bits klanten is een Linux 64-bits pakket nodig, enzovoort. Ten tweede wordt het AnyConnect-beeld dat op het head-end is geïnstalleerd, automatisch naar de client geduwd na een verbinding. Gebruikers die voor het eerst een verbinding maken, kunnen de client downloaden van het webportaal en gebruikers die teruggaan kunnen een upgrade uitvoeren, mits het AnyConnect-pakket op het head-end nieuwer is dan wat op hun clientmachine is geïnstalleerd.

AnyConnect-pakketten kunnen worden verkregen via het gedeelte AnyConnect Secure Mobility Client van de Cisco-softwaredownloads-website. Hoewel er veel opties beschikbaar zijn, zullen de op het hoofd te installeren pakketten worden voorzien van een etiket met het besturingssysteem en de head-end-installatie (PKG). AnyConnect-pakketten zijn momenteel beschikbaar voor deze besturingssysteemplatforms: Windows, Mac OS X, Linux (32-bits) en Linux 64-bits. Merk op dat voor Linux er zowel 32- als 64-bits pakketten zijn. Elk besturingssysteem moet het juiste pakket op het kop zijn geïnstalleerd zodat verbindingen mogelijk zijn.

Nadat het AnyConnect-pakket is gedownload, kan het met de copyrightwetgeving van de router via TFTP, FTP, SCP of een paar andere opties worden geüpload naar de flitser van de router. Hierna volgt een voorbeeld:

```
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)
```

Nadat u de AnyConnect-afbeelding naar de flitser van de router hebt gekopieerd, moet deze via de opdrachtregel worden geïnstalleerd. Er kunnen meerdere AnyConnect-pakketten worden geïnstalleerd wanneer u een volgnummer aan het einde van de installatie-opdracht specificeert; Dit zal de router in staat stellen om als head-end op te treden voor meerdere besturingssystemen

van klanten. Wanneer u het AnyConnect-pakket installeert, wordt het ook naar de **flitser** verplaatst**:/web/folder** als het aanvankelijk niet werd gekopieerd.

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

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

Op versies van code die vóór 15.2(1)T zijn vrijgegeven, is de opdracht om de PKG te installeren iets anders.

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

Stap 3. Generate RSA-trapezium en zelfondertekend certificaat

Wanneer u SSL of een functie configureren die PKI-infrastructuur (Public Key Infrastructure) en digitale certificaten implementeert, is een Rivest-Shamir-Adleman (RSA)-toetsenbord vereist voor het ondertekenen van het certificaat. Deze opdracht genereert een RSA-toetsenbord dat vervolgens wordt gebruikt wanneer het zelf-getekende PKI-certificaat wordt gegenereerd. Gebruik van een modulus van 2048 bits, dit is geen vereiste, maar aanbevolen wordt de grootste modulus te gebruiken die beschikbaar is voor verbeterde beveiliging en compatibiliteit met de AnyConnect-clientmachines. Het wordt ook aanbevolen een beschrijvend sleutellabel te gebruiken dat bij het sleutelbeheer wordt toegewezen. De sleutelgeneratie kan worden bevestigd met de opdracht **Show crypto-toets mypubkey rsa**.

> **Opmerking:** Aangezien er veel veiligheidsrisico's verbonden zijn aan het exporteerbaar maken van RSA-toetsen, is de aanbevolen praktijk ervoor te zorgen dat de sleutels zodanig zijn geconfigureerd dat ze niet exporteerbaar zijn, hetgeen de standaardinstelling is. De risico's die betrokken zijn bij het exporteren van de RSA-toetsen worden in dit document besproken: Het implementeren van RSA-toetsen binnen een 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
```

Zodra de RSA-toetsencombinatie met succes is gegenereerd moet een PKI-betrouwbaar punt met de informatie van onze router en RSA-toetsenbord worden geconfigureerd. De Gemeenschappelijke Naam (CN) in de Onderwerp-naam moet worden geconfigureerd met het IP-adres of FQDN-naam (Full Qualified Domain Name, FQDN) die gebruikers gebruiken om verbinding te maken met de AnyConnect-poort; in dit voorbeeld gebruiken de klanten FQDN van fdenofa-SSLVPN.cisco.com wanneer zij proberen te verbinden. Hoewel dit niet verplicht is, wanneer u juist in de GN invoert, helpt het het aantal certificaatfouten te verminderen die bij inloggen worden veroorzaakt.

> **Opmerking:** In plaats van een zelfondertekend certificaat te gebruiken dat door de router gegenereerd is, is het mogelijk een certificaat te gebruiken dat door een CA van derden is afgegeven. Dit kan worden gedaan via een paar verschillende methoden zoals die in dit document worden besproken: certificaatinschrijving voor een PKI configureren.

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

Nadat het trustpoint correct is gedefinieerd, moet de router het certificaat genereren door gebruik te maken van de opdracht **van de** vastlegging **crypto** pki. Tijdens dit proces kan u een paar andere parameters specificeren, zoals het serienummer en IP-adres. Dit is echter niet nodig. De certificatenproductie kan worden bevestigd met de opdracht **voor** de **show crypto pki certificaten**.

```
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
```

Stap 4. Configuratie van lokale VPN-gebruikersaccounts

Hoewel het mogelijk is om een externe AAA-server (Verificatie, autorisatie en accounting) te gebruiken, wordt bijvoorbeeld lokale verificatie gebruikt. Deze opdrachten maken een gebruikersnaam VPNUSER en maken ook een AAA-verificatielijst met de naam SSLVPN_AAA.

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

Stap 5. Bepaal de adresgroep en de toegangslijst van de tunnels die door klanten moet worden gebruikt

Er moet een lokale IP-adrespool worden gemaakt zodat AnyConnect-clientadapters een IP-adres kunnen verkrijgen. Zorg ervoor dat u een grote genoeg pool vormt ter ondersteuning van het maximale aantal gelijktijdige AnyConnect-clientverbindingen.

Standaard zal AnyConnect werken in de volledige tunnelmodus, hetgeen betekent dat elk verkeer dat door de clientmachine gegenereerd wordt, over de tunnel wordt verzonden. Aangezien dit doorgaans niet wenselijk is, is het mogelijk om een toegangscontrolelijst (ACL) te configureren die dan verkeer definieert dat al dan niet over de tunnel moet worden verzonden. Net als bij andere ACL-implementaties heft de impliciete ontkennen aan het einde de noodzaak van een expliciete ontkenning op; daarom is het alleen nodig om vergunningen af te geven voor het verkeer dat moet worden getunneld .

```
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
```

Stap 6. Het configureren van de virtuele sjabloon voor interface (VTI)

Dynamische VTI's voorzien in een on-demand afzonderlijke Virtual-access interface voor elke VPN-sessie die zeer beveiligde en schaalbare connectiviteit voor VPN's op afstand toestaat. De DVTI-technologie vervangt dynamische crypto-kaarten en de dynamische hub-and-sprak methode die helpt tunnels op te zetten. Omdat DVTI's net als elke andere echte interface functioneren, maken zij een complexere invoering van externe toegang mogelijk omdat zij QoS, firewall, per-gebruiker eigenschappen en andere beveiligingsdiensten ondersteunen zodra de tunnel actief is.

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

Stap 7. Configuratie van WebVPN-gateway

De WebVPN Gateway is wat het IP-adres en de IP-poort(s) definieert die zullen worden gebruikt door het AnyConnect-head-end, evenals het SSL-encryptie-algoritme en het PKI-certificaat, dat aan de klanten zal worden aangeboden. Standaard zal de gateway alle mogelijke encryptie-algoritmen ondersteunen, die afhankelijk van de Cisco IOS-versie op de router verschillen.

```
webvpn gateway SSLVPN_GATEWAY
 ip address 209.165.201.1 port 443
```

```
 http-redirect port 80
 ssl trustpoint SSLVPN_CERT
 inservice
```

Stap 8. WebVPN-context en groepsbeleid configureren

In de context en het groepsbeleid van WebeVPN worden enkele extra parameters gedefinieerd die voor de verbinding van de AnyConnect-client zullen worden gebruikt. Voor een basisconfiguratie van AnyConnect fungeert de Context eenvoudigweg als een mechanisme dat wordt gebruikt om het standaard groepbeleid te bellen dat voor AnyConnect zal worden gebruikt. Hoe dan ook, de Context kan worden gebruikt om de WebVPN spetpagina en de WebVPN-handeling verder aan te passen. In de gedefinieerde Beleidsgroep wordt de SSLVPN_AAA lijst geconfigureerd als de AAA-verificatielijst waarvan de gebruikers lid zijn. De **functies svc-enabled** opdracht is het configuratiestuk dat gebruikers in staat stelt om met de AnyConnect SSL VPN-client in plaats van alleen WebVPN te verbinden door een browser. Ten slotte definiëren de extra SVC-opdrachten parameters die alleen van belang zijn voor SVC-verbindingen: **svc adres-pool** vertelt de gateway om adressen in de SSLVPN_POOL aan de klanten uit te delen, **svc split** definieert het gesplitste tunnelbeleid per ACL 1 hierboven gedefinieerd en **svc dns-server** definieert de DNS server die gebruikt zal worden voor het oplossen van domeinnamen. Met deze configuratie worden alle DNS-vragen naar de gespecificeerde DNS-server verzonden. Het adres dat wordt ontvangen in de query-reactie zal bepalen of het verkeer al dan niet in de tunnel wordt verstuurd.

```
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
```

Stap 9 (optioneel) Configuratie van een clientprofiel

Anders dan op ASA's heeft Cisco IOS geen ingebouwde GUI-interface die beheerders kan helpen bij het maken van het clientprofiel. Het AnyConnect-clientprofiel moet afzonderlijk met de zelfstandige profieleditor worden gemaakt/bewerkt.

> **Tip**: Kijk naar een willekeurige-verbinding-profileeditor-win-3.1.03103-k9.exe.

Volg deze stappen om de router het profiel te laten opstellen:

- Upload het naar IOS Flash met het gebruik van ftp/tftp.
- Gebruik deze opdracht om het profiel te identificeren dat zojuist is geüpload:

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

> **Tip**: Op Cisco IOS-versies ouder dan 15.2(1)T, moet deze opdracht worden gebruikt: **webvPN import svc-profiel <profile_name> flitser:<profile.xml**

3. Gebruik deze opdracht in de context om het profiel aan deze context te koppelen:

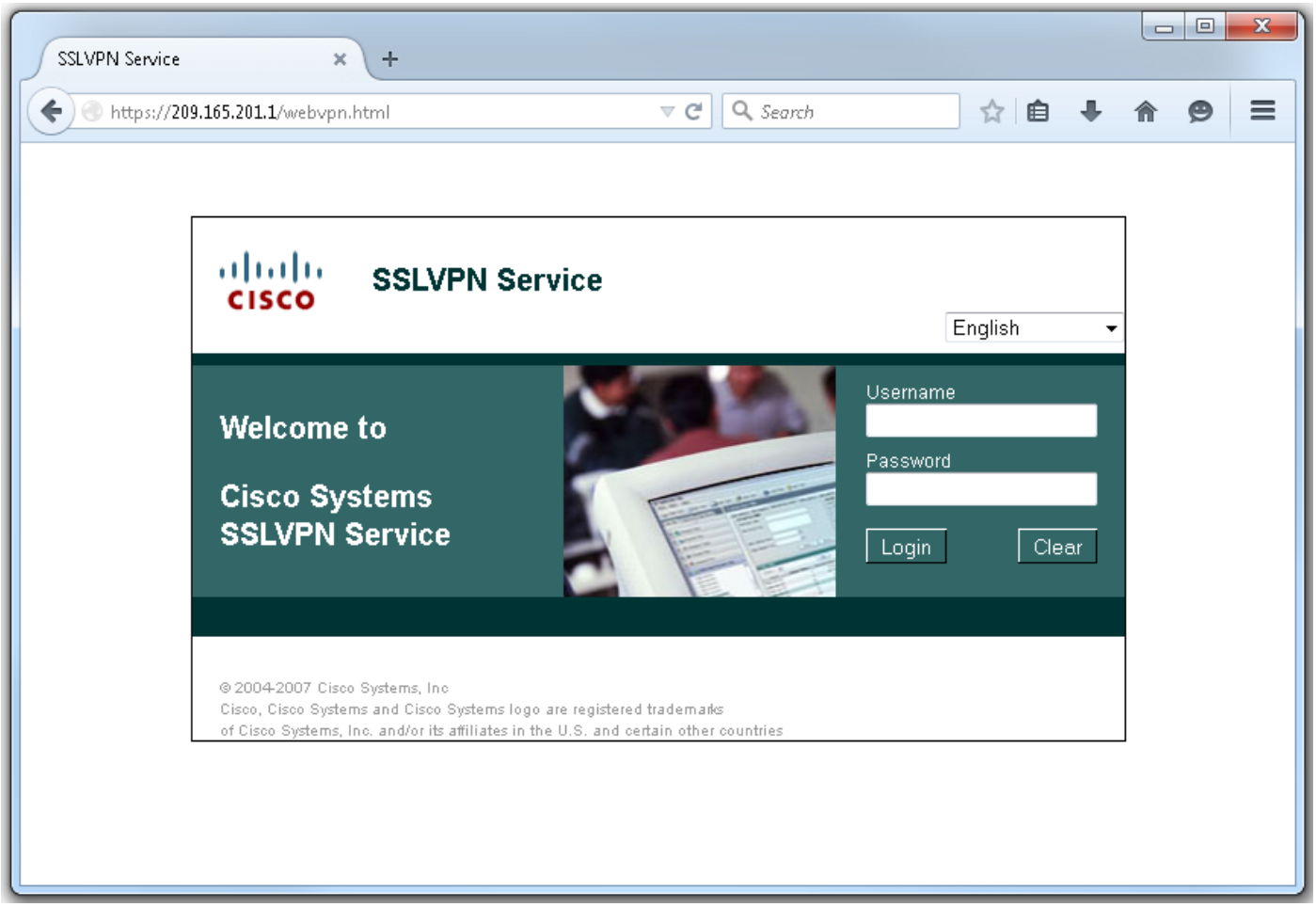
```
webvpn context SSLVPN_CONTEXT
 policy group SSLVPN_POLICY
 svc profile SSLVPN_PROFILE
```

Opmerking: Gebruik de Command Lookup Tool (alleen voor geregistreerde gebruikers) voor meer informatie over de opdrachten die in deze sectie worden gebruikt.

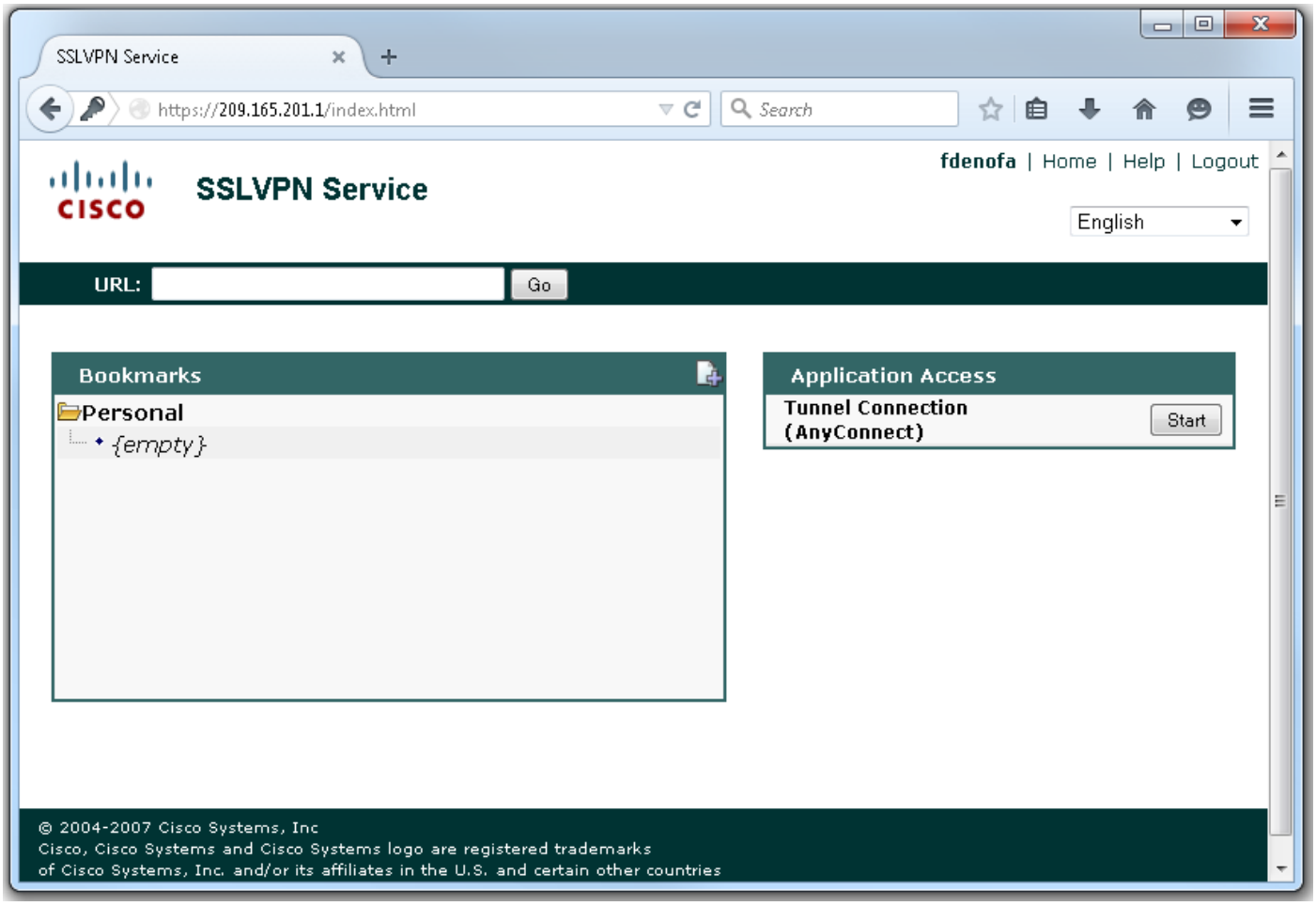
Verifiëren

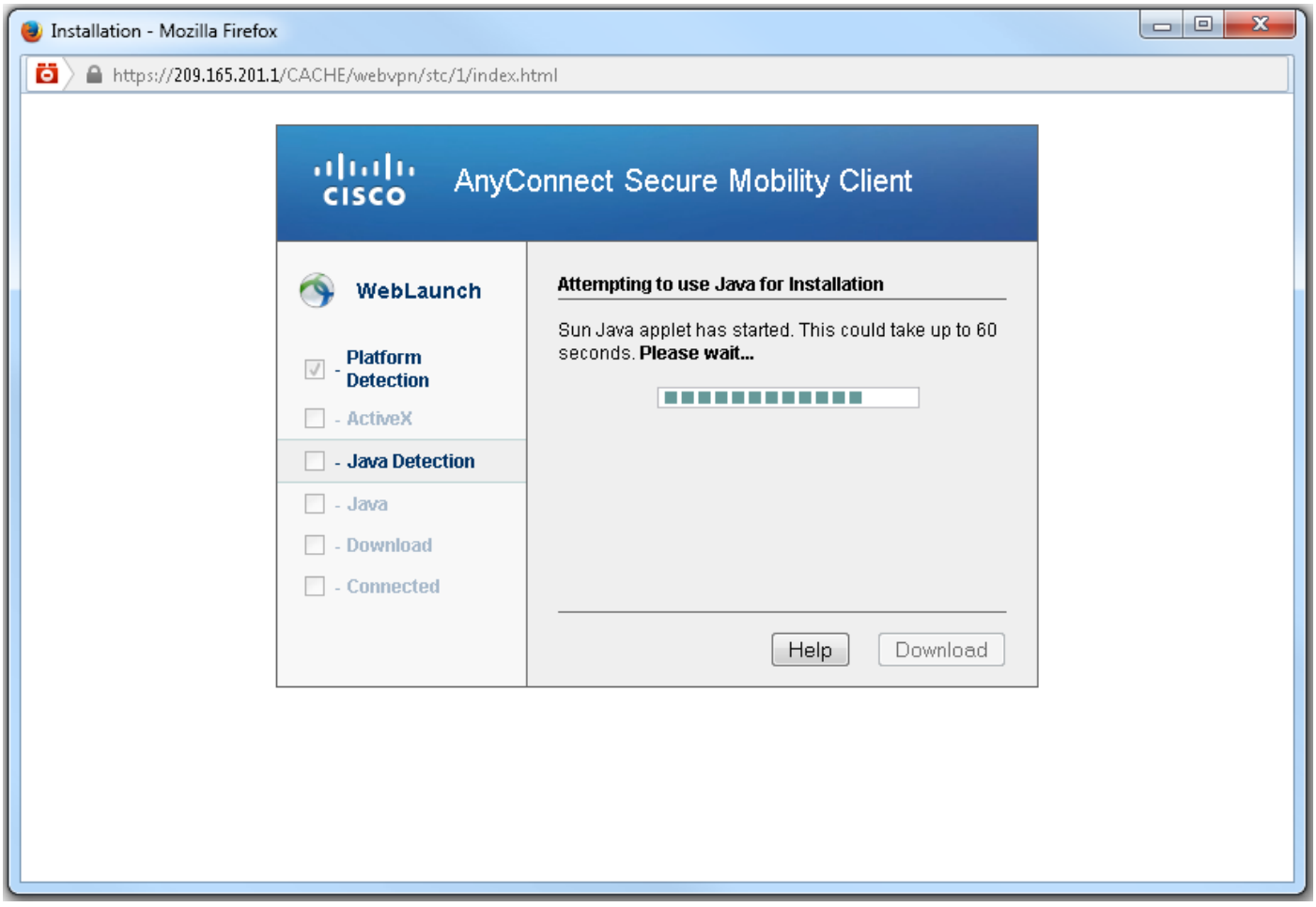
Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Zodra de configuratie is voltooid, wanneer u toegang heeft tot het adres van de gateway en poort via browser, zal deze terugkeren naar de WebVPN splash pagina.



Nadat u hebt inlogd, wordt de startpagina van WebeVPN weergegeven. Klik hier op **Tunnel Connection (AnyConnect).** Wanneer Internet Explorer wordt gebruikt, wordt ActiveX gebruikt om de AnyConnect-client omlaag te drukken en te installeren. Als deze niet wordt gedetecteerd, wordt in plaats daarvan Java gebruikt. Alle andere browsers gebruiken Java onmiddellijk.

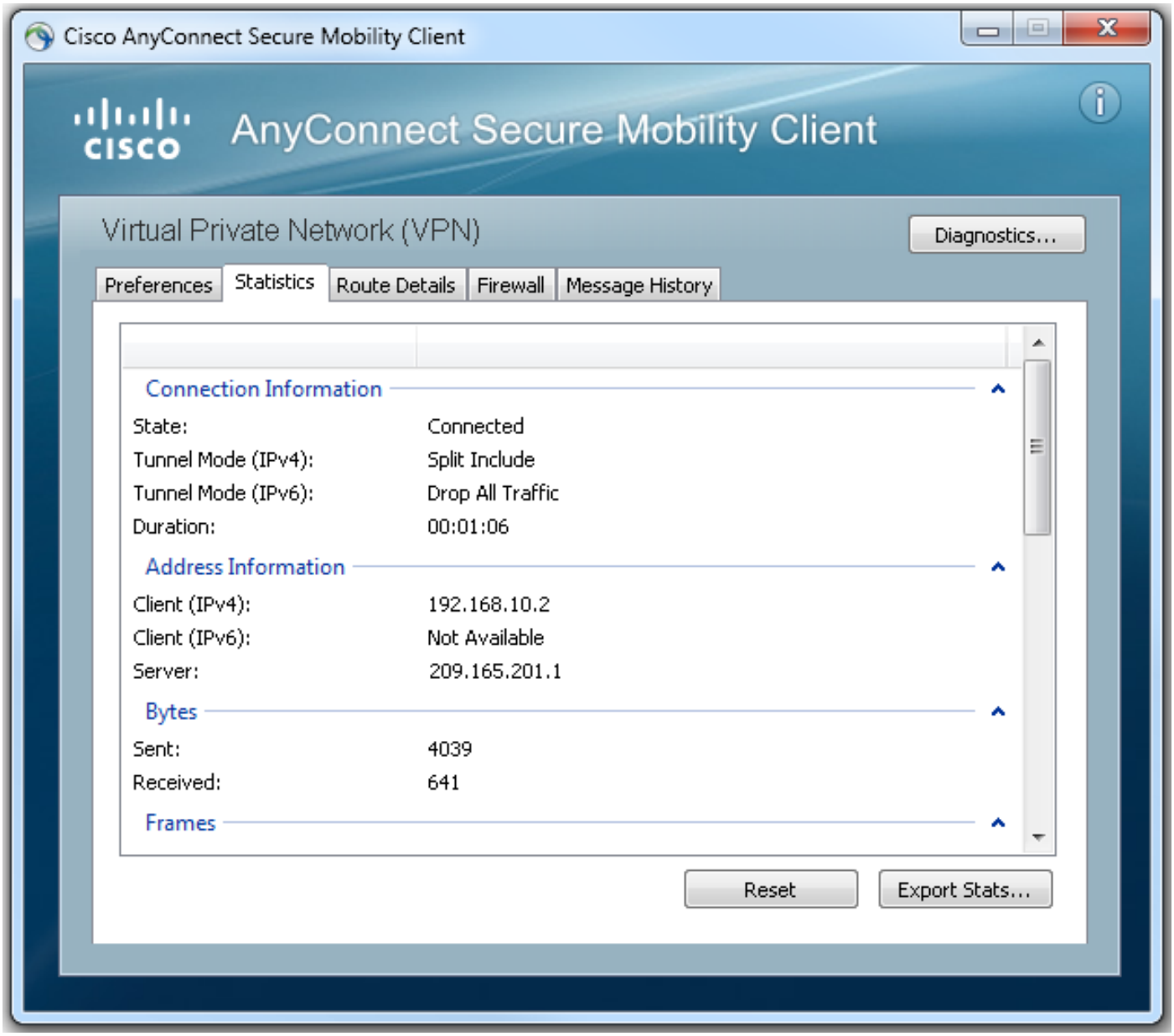


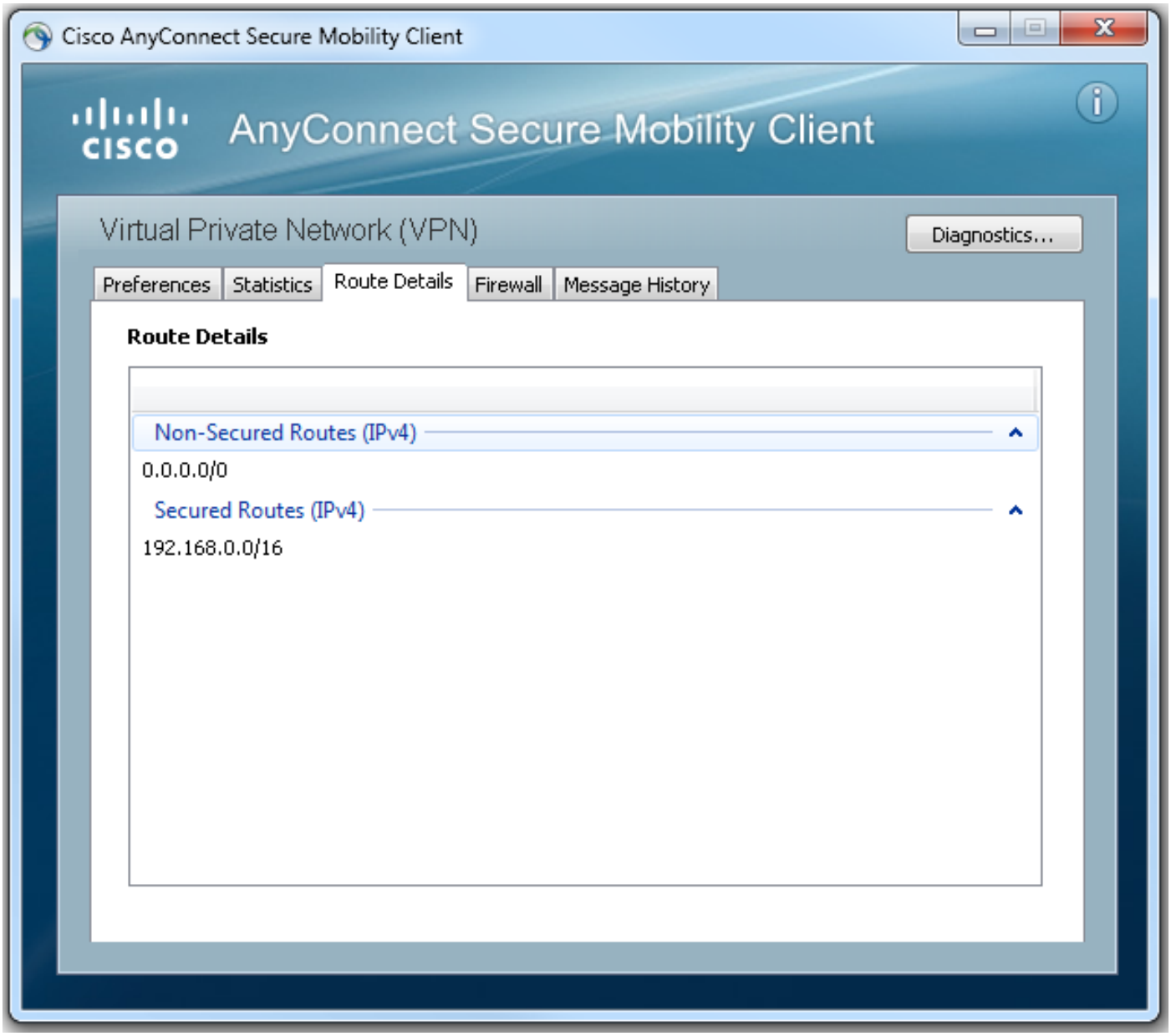


Nadat de installatie is voltooid, zal AnyConnect automatisch proberen een verbinding te maken met de WebVPN-gateway. Aangezien een zichzelf ondertekend certificaat voor de Gateway wordt

gebruikt om zichzelf te identificeren, zullen er tijdens de verbindingspoging meerdere certificaatwaarschuwingen verschijnen. Deze worden verwacht en moeten worden geaccepteerd zodat de verbinding kan worden voortgezet. Om deze certificeringswaarschuwingen te voorkomen, moet het zelf ondertekende certificaat dat wordt overgelegd, worden geïnstalleerd in de vertrouwde certificatenwinkel van de clientmachine, of indien een certificaat van derden wordt gebruikt, moet het certificaat van de certificaatinstantie zich in het vertrouwde certificatenhuis bevinden.

Wanneer de verbinding wordt voltooid, klikt u linksonder op het pictogram op het **tandwiel**. Geeft u geavanceerde informatie over de verbinding weer. Op deze pagina is het mogelijk om bepaalde verbindingsstatistieken en routedetails te bekijken die van de gesplitste tunnel ACL in de configuratie van het Beleid van de Groep worden verkregen.


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...



Hier is het resultaat van de configuratie van de laatste configuratie van de configuratie:

```
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
```

Problemen oplossen

Deze sectie verschaft informatie die u kunt gebruiken om problemen met uw configuratie op te lossen.

Er zijn een paar gebruikelijke onderdelen om te controleren of u problemen hebt met de AnyConnect-verbinding:

- Aangezien de client een certificaat moet indienen, is het vereist dat het certificaat dat in de WebVPN Gateway is gespecificeerd, geldig is. Om een **show crypto kaart certificaat** uit te geven zal informatie tonen die op alle certificaten op de router betrekking heeft.
- Wanneer een verandering in de configuratie van WebVPN wordt aangebracht, is het een beste praktijk om geen inservice en inservice op zowel de Gateway als de Context uit te geven. Dit zorgt ervoor dat de wijzigingen naar behoren worden uitgevoerd.
- Zoals eerder vermeld, is het vereist om een AnyConnect PKG te hebben voor elk client besturingssysteem dat verbinding maakt met deze gateway. Windows clients hebben bijvoorbeeld een Windows PKG, Linux 32-bits client vereist een Linux 32-bits PKG enzovoort.
- Wanneer u zowel de AnyConnect-client als de op een browser gebaseerde Webex-client beschouwt om SSL te gebruiken, geeft u toegang tot de WebVPN-spatpagina over het algemeen aan dat AnyConnect zal kunnen verbinden (neem aan dat de relevante AnyConnect-configuratie juist is).

Cisco IOS biedt sommige verschillende debug-webopties die kunnen worden gebruikt voor het opsporen van storingen in probleemoplossing. Dit is de output die gegenereerd wordt uit debug webvpn aaa, debug-tunnels in VPN en laat websessie zien bij een succesvolle poging om verbinding te maken:

```
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
```

Gerelateerde informatie

- SSL VPN Configuration Guide, Cisco IOS release 15M&T
- AnyConnect VPN (SSL) client op IOS-router met Configuratievoorbeeld
- Technische ondersteuning en documentatie – Cisco Systems