AnyConnect: Configuración de SSL VPN básico para cabecera de router Cisco IOS con CLI

Introducción

Contenido

Este documento describe la configuración básica de un router Cisco IOS® como cabecera AnyConnect Secure Sockets Layer VPN (SSL VPN).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- IOS de Cisco
- AnyConnect Secure Mobility Client
- Operación SSL general

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Información de licencia para diferentes versiones de IOS

- El conjunto de funciones de securityk9 es necesario para utilizar las funciones SSL VPN, independientemente de la versión de Cisco IOS utilizada.
- Cisco IOS 12.x - la función SSL VPN se integra en todas las imágenes 12.x que comienzan con 12.4(6)T que tienen al menos una licencia de seguridad (ie. advsecurityk9, adventerprisek9, etc.).
- Cisco IOS 15.0: las versiones anteriores requieren que se instale un archivo LIC en el router, lo que permitirá conexiones de 10, 25 o 100 usuarios. Licencias de derecho de uso* implementadas en 15.0(1)M4
- Cisco IOS 15.1: las versiones anteriores requieren que se instale un archivo LIC en el router, lo que permitirá conexiones de 10, 25 o 100 usuarios. Las licencias de derecho de uso* se implementaron en 15.1(1)T2, 15.1(2)T2, 15.1(3)T y 15.1(4)M1
- Cisco IOS 15.2: todas las versiones 15.2 ofrecen licencias Right to Use* para SSLVPN
- Cisco IOS 15.3 y versiones posteriores: las versiones anteriores ofrecen las licencias Derecho de uso*. A partir de 15.3(3)M, la función SSLVPN está disponible después de arrancar en un paquete tecnológico de securityk9

En el caso de las licencias de RTU, se activará una licencia de evaluación cuando se configure la primera función webvpn (es decir, webvpn gateway GATEWAY1) y se haya aceptado el acuerdo de licencia del usuario final (EULA). Después de 60 días, esta licencia de evaluación se convierte en una licencia permanente. Estas licencias se basan en el honor y requieren la compra de una licencia en papel para utilizar la función. Además, en lugar de limitarse a cierto número de usos, la RTU permite el número máximo de conexiones simultáneas que la plataforma del router puede soportar simultáneamente.

Importantes mejoras de software

Estos ID de bug dieron como resultado características o correcciones significativas para AnyConnect:

- CSCti89976: soporte agregado para AnyConnect 3.x a IOS
- CSCtx38806: Solución para la vulnerabilidad BEAST, Microsoft KB258542

Configurar

Paso 1. Confirmar licencia habilitada

El primer paso cuando se configura AnyConnect en una cabecera del router IOS es confirmar que la licencia se ha instalado correctamente (si procede) y se ha habilitado. Consulte la información sobre licencias de la sección anterior para obtener información específica sobre licencias en diferentes versiones. Depende de la versión del código y la plataforma si la licencia show enumera una licencia SSL_VPN o una licencia de seguridad9. Independientemente de la versión y la licencia, el CLUF deberá ser aceptado y la licencia se mostrará como Activo.

Paso 2. Cargar e instalar el paquete de AnyConnect Secure Mobility Client en el router

Para cargar una imagen de AnyConnect en la VPN, la cabecera tiene dos propósitos. En primer lugar, solo se permitirá la conexión a los sistemas operativos que tengan imágenes de AnyConnect presentes en la cabecera de AnyConnect. Por ejemplo, los clientes de Windows requieren que se instale un paquete de Windows en la cabecera, los clientes de 64 bits de Linux requieren un paquete de 64 bits de Linux, etc. En segundo lugar, la imagen de AnyConnect instalada en la cabecera se enviará automáticamente al equipo cliente cuando se conecte. Los usuarios que se conecten por primera vez podrán descargar el cliente desde el portal web y los usuarios que regresen podrán actualizar, siempre que el paquete AnyConnect en la cabecera sea más reciente que el que está instalado en su equipo cliente.

Los paquetes de AnyConnect se pueden obtener a través de la sección AnyConnect Secure Mobility Client del sitio web de descargas de software de Cisco. Aunque hay muchas opciones disponibles, los paquetes que se instalarán en la cabecera se etiquetarán con el sistema operativo y la implementación de cabecera (PKG). Los paquetes AnyConnect están disponibles actualmente para estas plataformas de sistemas operativos: Windows, Mac OS X, Linux (32 bits) y Linux de 64 bits. Tenga en cuenta que para Linux, hay paquetes de 32 y 64 bits. Cada sistema operativo requiere que se instale el paquete adecuado en la cabecera para permitir las conexiones.

Una vez que se ha descargado el paquete AnyConnect, se puede cargar en la memoria flash del router con el comando **copy** a través de TFTP, FTP, SCP o algunas otras opciones. Aquí tiene un ejemplo:

```
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)
```

Después de copiar la imagen de AnyConnect en la memoria flash del router, se debe instalar a través de la línea de comandos. Se pueden instalar varios paquetes AnyConnect cuando se

especifica un número de secuencia al final del comando de instalación; esto permitirá que el router actúe como cabecera para varios sistemas operativos cliente. Cuando instale el paquete de AnyConnect, también lo moverá al directorio **flash:/webvpn/** si inicialmente no se copió allí.

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

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

En las versiones del código que se lanzaron antes de 15.2(1)T, el comando para instalar el PKG es ligeramente diferente.

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

Paso 3. Generar par de llaves RSA y certificado firmado automáticamente

Al configurar SSL o cualquier función que implemente la infraestructura de clave pública (PKI) y los certificados digitales, se requiere un par de claves Rivest-Shamir-Adleman (RSA) para la firma del certificado. Este comando generará un par de llaves RSA que luego se utilizará cuando se genere el certificado PKI autofirmado. Utilice un módulo de 2048 bits, no es un requisito, pero se recomienda utilizar el módulo más grande disponible para mejorar la seguridad y compatibilidad con las máquinas cliente AnyConnect. También se recomienda utilizar una etiqueta de clave descriptiva que se asignará con la administración de claves. La generación de claves se puede confirmar con el comando **show crypto key mypubkey rsa**.

> **Nota:** Dado que hay muchos riesgos de seguridad asociados con hacer que las claves RSA sean exportables, la práctica recomendada es asegurarse de que las claves estén configuradas para que no sean exportables, que es el valor predeterminado. En este documento se tratan los riesgos que conlleva el hecho de que las claves RSA sean exportables: Implementación de Llaves RSA Dentro de un 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
```

Una vez que el par de claves RSA se ha generado correctamente, se debe configurar un punto de confianza PKI con la información de nuestro router y el par de claves RSA. El nombre común (CN) en el nombre del asunto debe configurarse con la dirección IP o el nombre de dominio completo (FQDN) que los usuarios utilizan para conectarse al gateway de AnyConnect; en este ejemplo, los clientes utilizan el FQDN de fdenofa-SSLVPN.cisco.com cuando intentan conectarse. Aunque no es obligatorio, cuando introduce correctamente en el CN, ayuda a reducir el número de errores de certificado que se solicitan al iniciar sesión.

> **Nota:** En lugar de utilizar un certificado autofirmado generado por el router, es posible utilizar un certificado emitido por una CA de terceros. Esto se puede hacer a través de varios métodos diferentes como se describe en este documento: Configuración de la Inscripción de Certificados para una PKI.

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

Después de que el punto de confianza se haya definido correctamente, el router debe generar el certificado mediante el comando **crypto pki enroll**. Con este proceso, es posible especificar otros parámetros como el número de serie y la dirección IP. Sin embargo, esto no es necesario. La generación de certificados se puede confirmar con el comando **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
```

Paso 4. Configurar cuentas de usuario VPN locales

Si bien es posible utilizar un servidor externo de autenticación, autorización y contabilidad (AAA),

para este ejemplo se utiliza la autenticación local. Estos comandos crearán un nombre de usuario VPNUSER y también crearán una lista de autenticación AAA denominada SSLVPN_AAA.

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

Paso 5. Definir el conjunto de direcciones y la lista de acceso de túnel dividido que utilizarán los clientes

Se debe crear un conjunto de direcciones IP locales para que los adaptadores de cliente AnyConnect obtengan una dirección IP. Asegúrese de configurar un conjunto lo suficientemente grande como para admitir el número máximo de conexiones de cliente AnyConnect simultáneas.

De forma predeterminada, AnyConnect funcionará en el modo de túnel completo, lo que significa que cualquier tráfico generado por la máquina cliente se enviará a través del túnel. Como esto no suele ser deseable, es posible configurar una lista de control de acceso (ACL) que, a continuación, defina el tráfico que se debe o no enviar a través del túnel. Como con otras implementaciones de ACL, la negación implícita al final elimina la necesidad de una negación explícita; por lo tanto, sólo es necesario configurar las sentencias permit para el tráfico que debe ser tunelado.

```
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
```

Paso 6. Configuración de la interfaz de plantilla virtual (VTI)

VTI dinámicas proporcionan una interfaz de acceso virtual independiente a demanda para cada sesión VPN que permite una conectividad altamente segura y escalable para VPN de acceso remoto. La tecnología DVTI reemplaza los mapas criptográficos dinámicos y el método dinámico hub-and-spoke que ayuda a establecer túneles. Como los DVTI funcionan como cualquier otra interfaz real, permiten una implementación de acceso remoto más compleja porque admiten QoS, firewall, atributos por usuario y otros servicios de seguridad tan pronto como el túnel está activo.

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

Paso 7. Configuración del gateway de WebVPN

El gateway de WebVPN es lo que define la dirección IP y los puertos que utilizará el centro distribuidor de AnyConnect, así como el algoritmo de cifrado SSL y el certificado PKI que se presentarán a los clientes. De forma predeterminada, la puerta de enlace admitirá todos los algoritmos de cifrado posibles, que varían según la versión de Cisco IOS en el router.

```
webvpn gateway SSLVPN_GATEWAY
 ip address 209.165.201.1 port 443
 http-redirect port 80
```

```
 ssl trustpoint SSLVPN_CERT
 inservice
```

Paso 8. Configuración del Contexto y la Política de Grupo de WebVPN

El contexto y la política de grupo de WebVPN definen algunos parámetros adicionales que se utilizarán para la conexión del cliente AnyConnect. Para una configuración básica de AnyConnect, el contexto simplemente sirve como mecanismo utilizado para llamar a la política de grupo predeterminada que se utilizará para AnyConnect. Sin embargo, el Contexto se puede utilizar para personalizar aún más la página de bienvenida WebVPN y la operación WebVPN. En el grupo de políticas definido, la lista SSLVPN_AAA se configura como la lista de autenticación AAA de la que los usuarios son miembros. El comando **Funcs svc-enabled** es la configuración que permite a los usuarios conectarse con AnyConnect SSL VPN Client en lugar de sólo WebVPN a través de un navegador. Por último, los comandos SVC adicionales definen parámetros que son relevantes sólo para las conexiones SVC: **svc address-pool** indica a la puerta de enlace que envíe las direcciones en SSLVPN_POOL a los clientes, **svc split include** define la política de túnel dividido por ACL 1 definida anteriormente y **svc dns-server** define el servidor DNS que se utilizará para la resolución de nombres de dominio. Con esta configuración, todas las consultas de DNS se enviarán al servidor DNS especificado. La dirección que se recibe en la respuesta de consulta dictará si el tráfico se envía o no a través del túnel.

```
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
```

Paso 9 (opcional) Configuración de un perfil de cliente

A diferencia de los ASA, Cisco IOS no tiene una interfaz GUI integrada que pueda ayudar a los administradores a crear el perfil del cliente. El perfil de cliente de AnyConnect debe crearse/editarse por separado con el Editor de perfiles independiente.

> **Consejo:** Busque anyconnect-profileeditor-win-3.1.03103-k9.exe.

Siga estos pasos para que el router implemente el perfil:

- Cargue en IOS Flash con el uso de ftp/tftp.
- Utilice este comando para identificar el perfil que se acaba de cargar:

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

> **Consejo:** En las versiones de Cisco IOS anteriores a 15.2(1)T, se debe utilizar este comando: **webvpn import svc profile <profile_name> flash:<profile.xml>**

3. En el contexto, utilice este comando para vincular el perfil a ese contexto:

```
webvpn context SSLVPN_CONTEXT
```

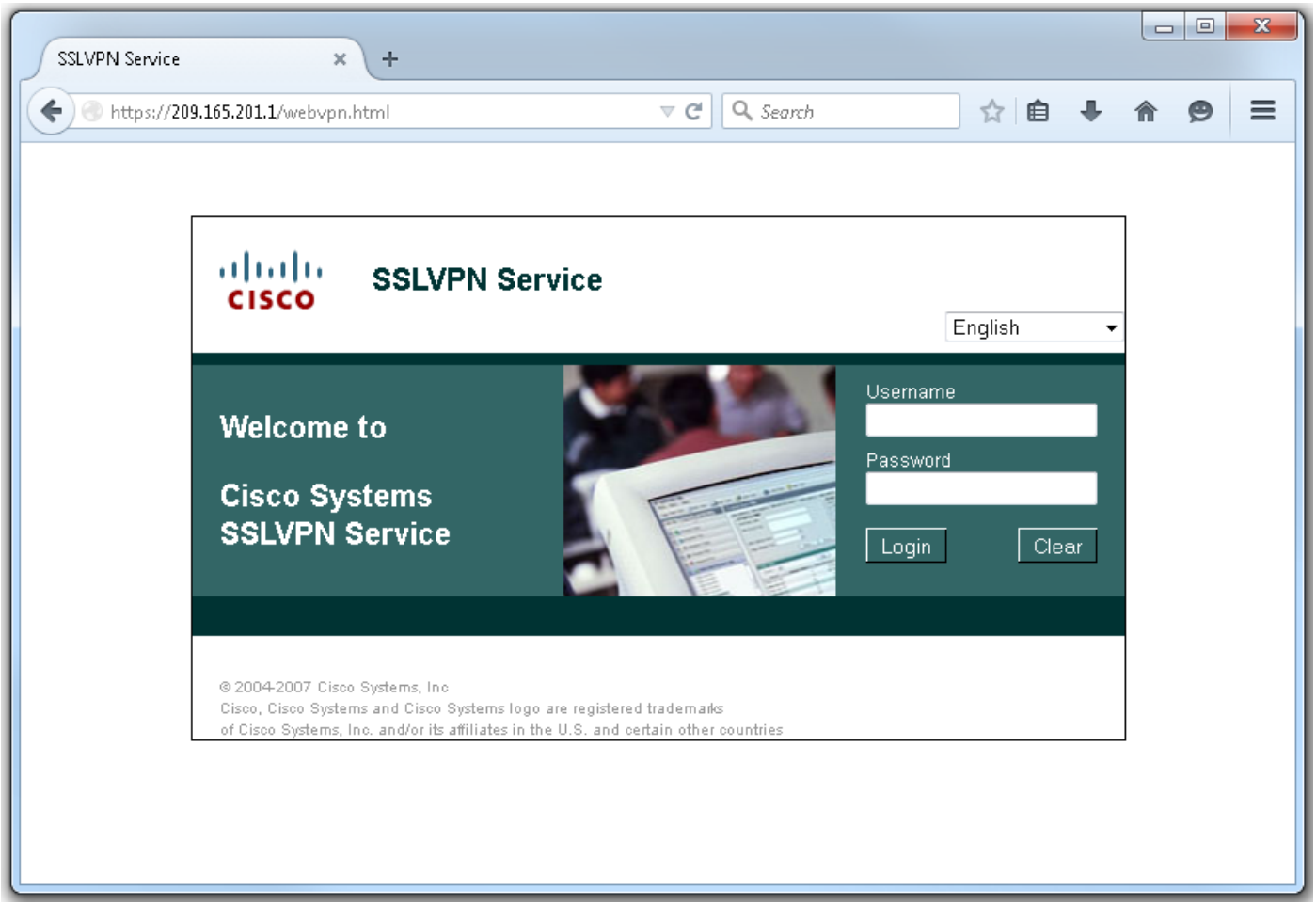
```
policy group SSLVPN_POLICY
svc profile SSLVPN_PROFILE
```

Nota: Use la Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos usados en esta sección.

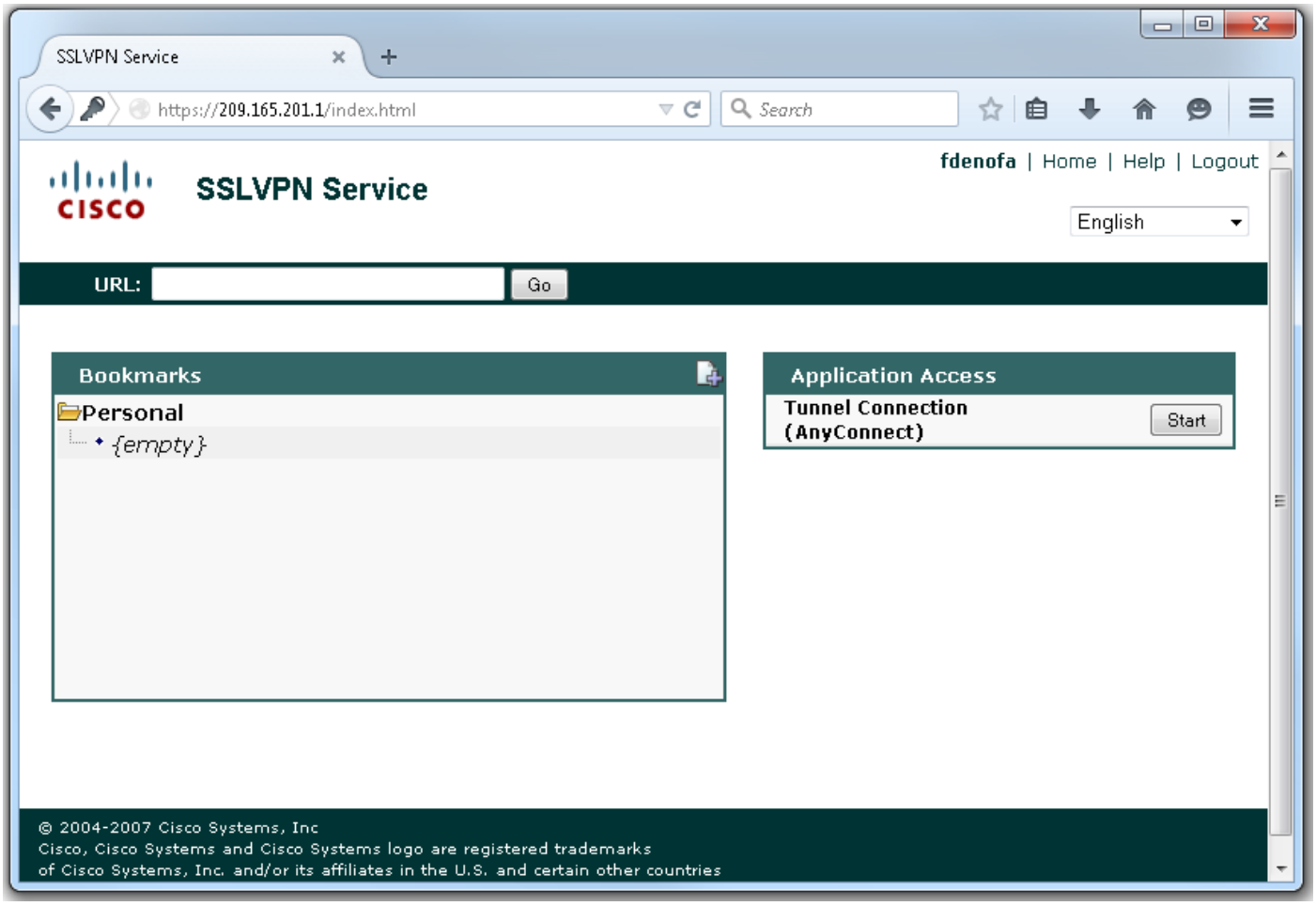
Verificación

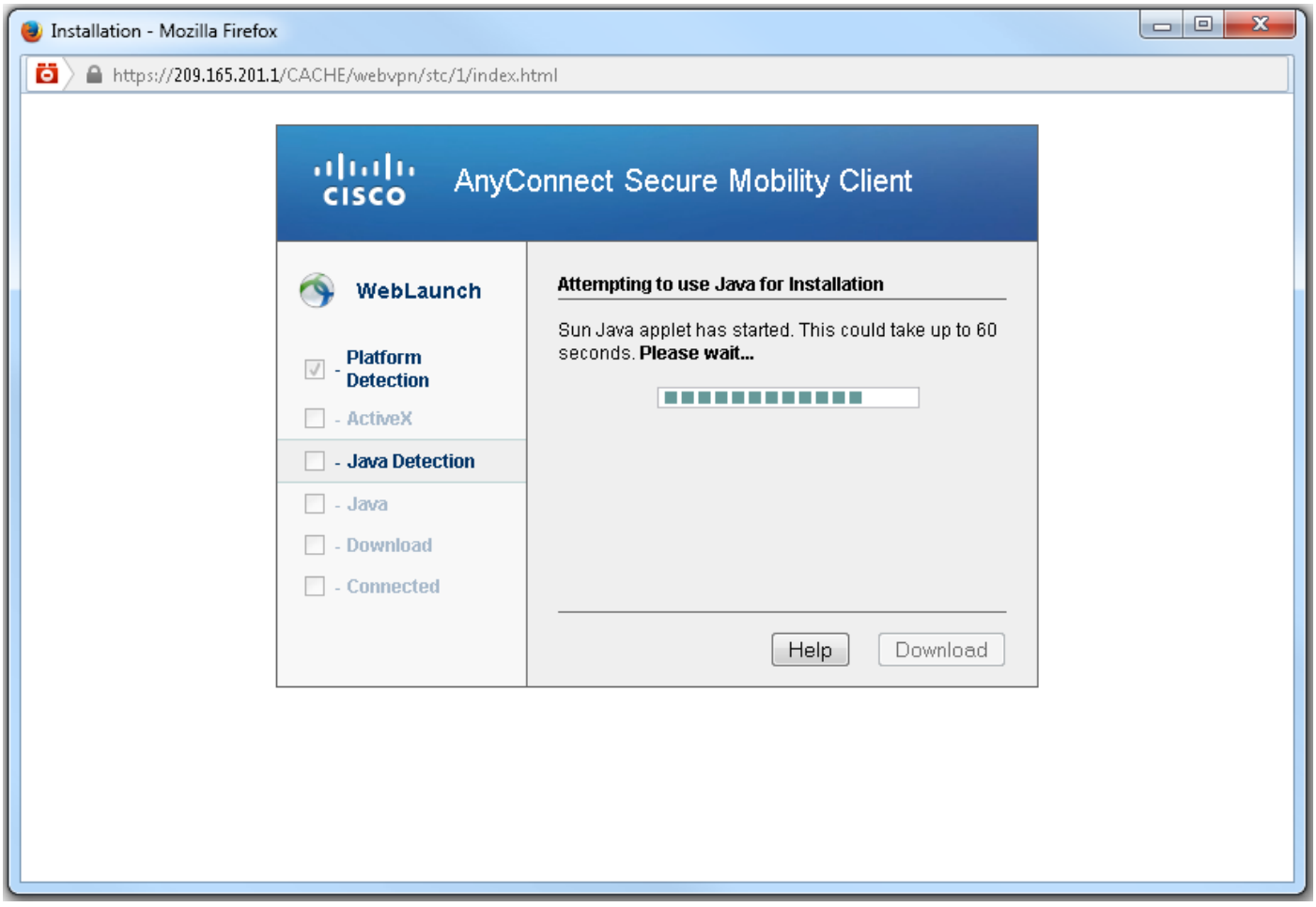
Utilize esta sección para confirmar que su configuración funcione correctamente.

Una vez finalizada la configuración, cuando acceda a la dirección y al puerto de la puerta de enlace a través del explorador, volverá a la página de inicio de WebVPN.



Después de iniciar sesión, se muestra la página de inicio de WebVPN. Desde aquí, haga clic en **Tunnel Connection (AnyConnect).** Cuando se utiliza Internet Explorer, ActiveX se utiliza para presionar e instalar el cliente AnyConnect. Si no se detecta, se utilizará Java en su lugar. Todos los demás navegadores utilizan Java inmediatamente.

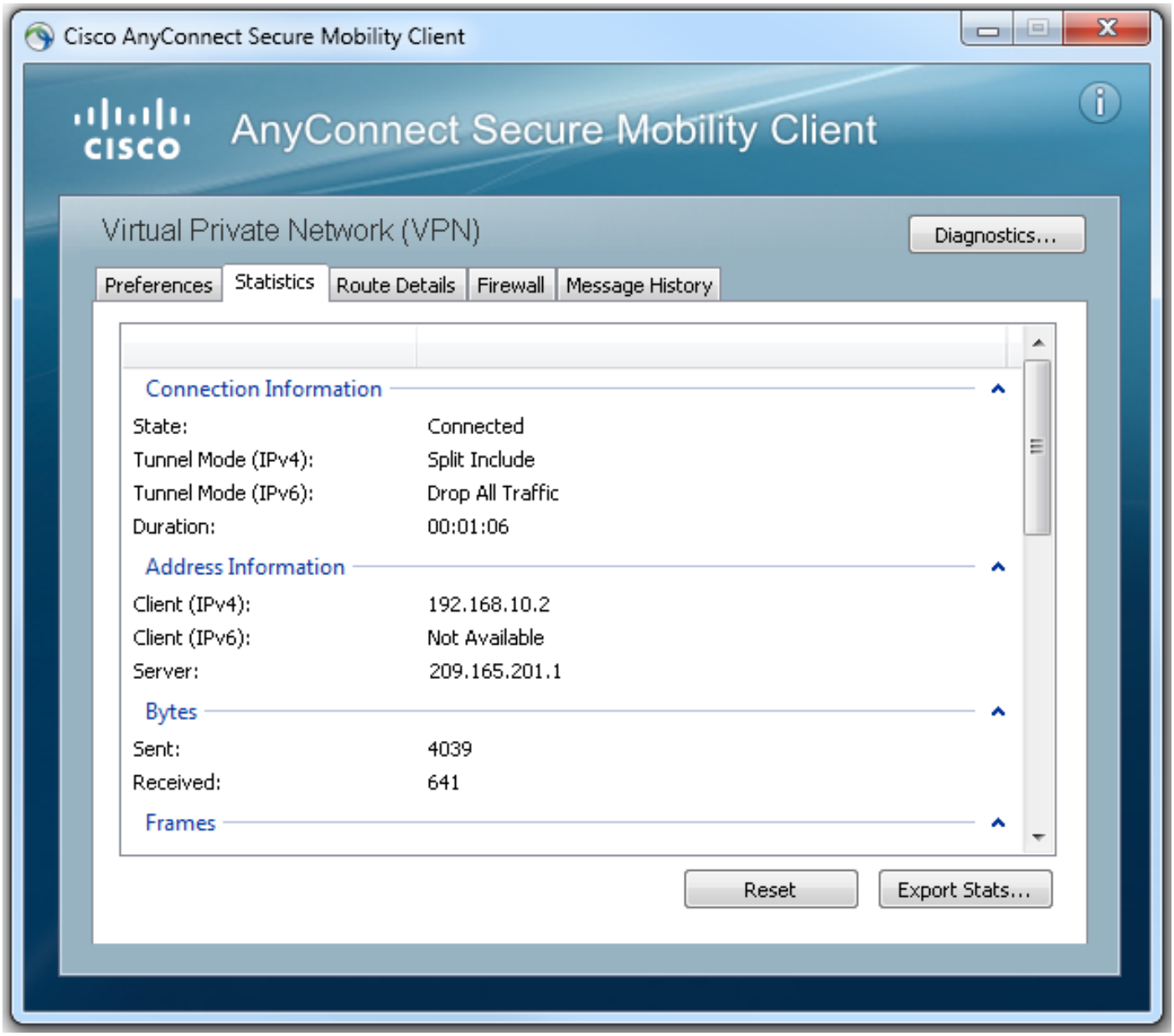


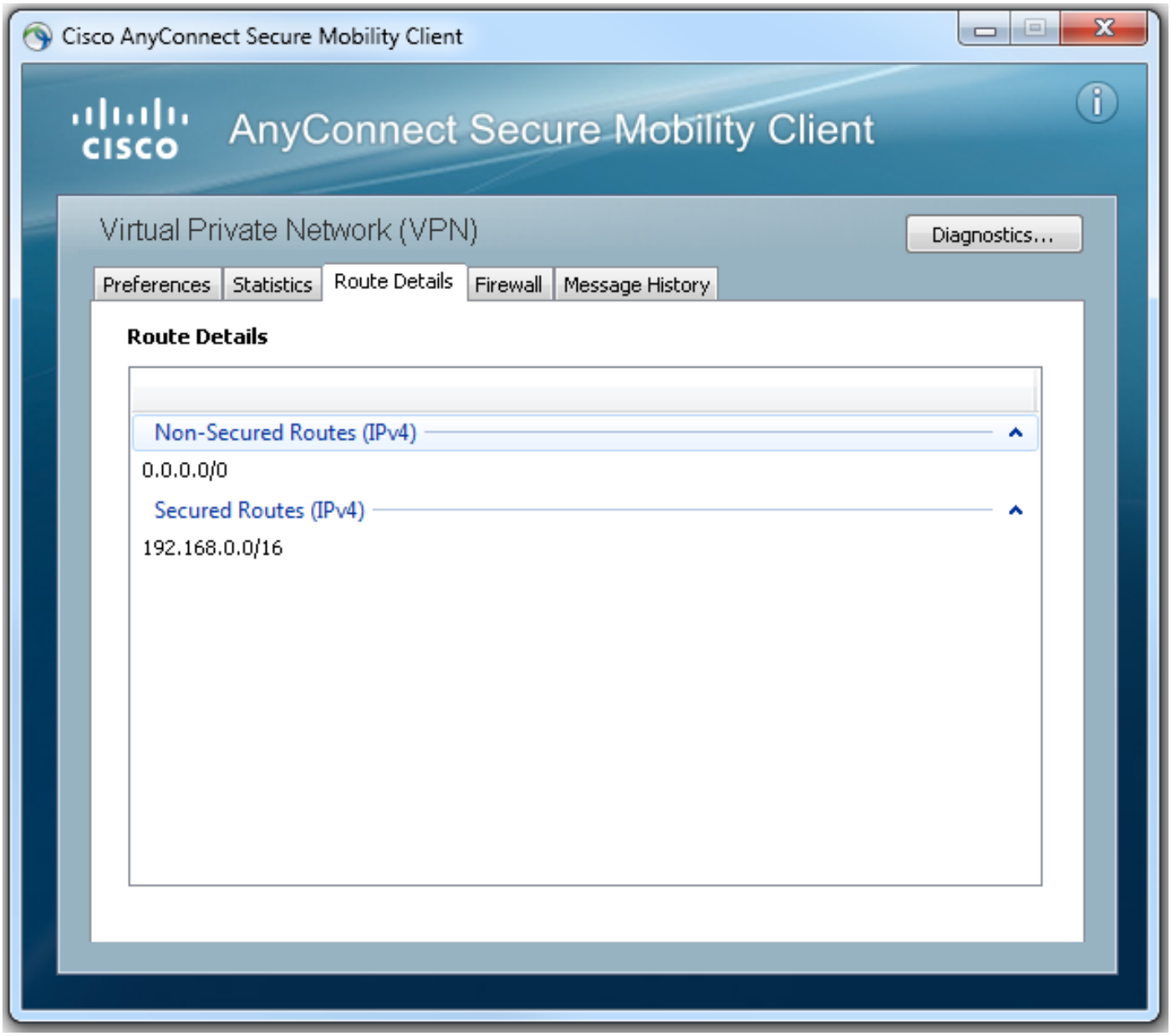


Una vez finalizada la instalación, AnyConnect intentará conectarse automáticamente a la puerta de enlace WebVPN. Como se está utilizando un certificado autofirmado para que la puerta de

enlace se identifique, aparecerán varias advertencias de certificado durante el intento de conexión. Se esperan y deben aceptarse para que la conexión continúe. Para evitar estas advertencias de certificado, el certificado autofirmado que se presenta debe estar instalado en el almacén de certificados de confianza de la máquina cliente, o si se está utilizando un certificado de terceros, el certificado de autoridad de certificación debe estar en el almacén de certificados de confianza.

Cuando la conexión complete la negociación, haga clic en el icono **de engranaje** situado en la parte inferior izquierda de AnyConnect, se mostrará información avanzada sobre la conexión. En esta página, es posible ver algunas estadísticas de conexión y detalles de ruta obtenidos de la ACL de túnel dividido en la configuración de la política de grupo.


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...



Este es el resultado final de la configuración en ejecución de los pasos de configuración:

```
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
```

Troubleshoot

En esta sección se brinda información que puede utilizar para resolver problemas en su configuración.

Hay algunos componentes comunes que se deben comprobar al resolver problemas de conexión de AnyConnect:

- Como el cliente debe presentar un certificado, es un requisito que el certificado especificado en el gateway de WebVPN sea válido. Para emitir un **show crypto pki certificate** mostrará información que pertenece a todos los certificados en el router.
- Siempre que se realiza un cambio en la configuración de WebVPN, se recomienda ejecutar un comando no inservice e inservice tanto en la puerta de enlace como en el contexto. Esto garantiza que los cambios surtan efecto correctamente.
- Como se mencionó anteriormente, es un requisito tener un PKG de AnyConnect para cada sistema operativo cliente que se conectará a esta puerta de enlace. Por ejemplo, los clientes de Windows requieren una PKG de Windows, los clientes de 32 bits de Linux requieren una PKG de 32 bits de Linux, etc.
- Cuando considera que tanto el cliente AnyConnect como el WebVPN basado en navegador utilizan SSL, para poder acceder a la página de inicio de WebVPN generalmente indica que AnyConnect podrá conectarse (suponga que la configuración pertinente de AnyConnect es correcta).

Cisco IOS ofrece varias opciones debug webvpn que se pueden utilizar para resolver problemas de conexiones defectuosas. Este es el resultado generado a partir de debug webvpn aaa, debug wevpn tunnel y show webvpn session tras un intento de conexión exitoso:

```
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
```

Información Relacionada

- Guía de Configuración de SSL VPN, Cisco IOS Release 15M&T
- Ejemplo de Configuración de AnyConnect VPN Client (SSL) en el Router IOS con CCP
- Soporte Técnico y Documentación - Cisco Systems