AnyConnect: Configuración SSLVPN básico para el headend del router IOS con el uso del CLI

Contenido

Introducción

Este documento describe la configuración básica de un router del Cisco IOS como headend de AnyConnect SSLVPN.

Prerequisites

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Sistema operativo de Cisco internetwork (IOS)
- Cliente seguro de la movilidad de AnyConnect
- Operación de general Secure Sockets Layer (SSL)

Componentes Utilizados

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

- Cisco 892W Router que ejecuta 15.3(3)M5
- Cliente seguro 3.1.08009 de la movilidad de AnyConnect

Información de autorización para diversas versiones de IOS

- Requieren al conjunto de características securityk9 utilizar las características SSLVPN, sin importar las cuales se utiliza la versión de IOS.
- IOS 12.x - la característica SSLVPN es integrada en todas las imágenes 12.x que comiencen con 12.4(6)T que tengan por lo menos una licencia de la Seguridad (IE. advsecurityk9, adventerprisek9, y así sucesivamente).
- IOS 15.0 - las versiones anteriores requieren un archivo LIC ser instaladas en el router que tendrá en cuenta 10, 25, o 100 conexiones del usuario. Derecho a las licencias de Use* fueron implementados en 15.0(1)M4
- IOS 15.1 - las versiones anteriores requieren un archivo LIC ser instaladas en el router que tendrá en cuenta 10, 25, o 100 conexiones del usuario. Derecho a las licencias de Use* fueron implementados en 15.1(1)T2, 15.1(2)T2, 15.1(3)T, y 15.1(4)M1
- IOS 15.2 - las 15.2 versiones ofrecen a la derecha a las licencias de Use* para SSLVPN
- IOS 15.3 y más allá - las versiones anteriores ofrecen a la derecha a las licencias de Use*. Comenzando en el 15.3(3)M, la característica SSLVPN está disponible después de que usted inicie en un tecnología-paquete securityk9

Para RTU que autoriza, se configura una licencia de evaluación será habilitada cuando la primera característica del webvpn (es decir, el gateway GATEWAY1 del webvpn) y se ha validado el acuerdo de licencia de usuario final (EULA). Después de 60 días, esta licencia de evaluación se convierte en una licencia permanente. Estas licencias son honor basado y requieren una licencia de papel de ser comprado para utilizar la característica. Además, bastante que siendo limitado a algunas aplicaciones, los RTU permiten el número máximo de conexiones simultáneas que la plataforma del router pueda soportar en paralelo.

Mejoras del software significativas

Estos bug ID dieron lugar a las características o a los arreglos significativos para AnyConnect:

- CSCti89976: Apoyo añadido para AnyConnect 3.x al IOS
- CSCtx38806: Arreglo para la vulnerabilidad de la BESTIA, Microsoft KB2585542

Configurar

Paso 1. Confirme la licencia se habilita

El primer paso cuando AnyConnect se configura en un headend del router IOS es confirmar que la licencia ha estado instalada (si procede) y habilitada correctamente. Refiera a la información de autorización en la sección anterior para los específicos de la autorización en diversas versiones. Depende de la versión del código y de la plataforma si la licencia de la demostración enumera

una licencia SSL_VPN o securityk9. Sin importar la versión y la licencia, el EULA necesitará ser validado y la licencia mostrará como Active.

Paso 2. Cargue y instale el paquete seguro del cliente de la movilidad de AnyConnect en el router

Para cargar una imagen de AnyConnect a los servicios de la cabecera VPN dos propósitos. En primer lugar, solamente los sistemas operativos que tienen imágenes de AnyConnect presentes en el headend de AnyConnect serán permitidos para conectar. Por ejemplo, los clientes de Windows requieren un paquete de Windows para ser instalados en el headend, Linux que los clientes 64-bit requieren un paquete 64-bit de Linux, y así sucesivamente. En segundo lugar, la imagen de AnyConnect instalada en el headend será empujada automáticamente hacia abajo a la máquina del cliente sobre la conexión. Los usuarios que conectan podrán por primera vez descargar el cliente del portal web y a los usuarios que la vuelta podrá actualizar, con tal que el paquete de AnyConnect en el headend sea más nuevo que lo que está instalada en su máquina del cliente.

Los paquetes de AnyConnect se pueden obtener a través de la sección segura del cliente de la movilidad de AnyConnect del sitio web de las descargas de software de Cisco. Mientras que hay muchas opciones disponibles, los paquetes que deben ser instalados en el headend serán etiquetados con el sistema operativo y el despliegue del centro distribuidor (PKG). Los paquetes de AnyConnect están actualmente disponibles para estas plataformas de sistema operativo: Windows, Mac OS X, Linux (de 32 bits), y Linux 64-bit. Observe que para Linux, hay ambos 32 y paquetes 64-bit. Cada sistema operativo requiere el paquete apropiado ser instalado en el headend para que las conexiones sean permitidas.

Una vez que se ha descargado el paquete de AnyConnect, puede ser cargado al flash del router con el **comando copy** vía el TFTP, el 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 que usted copie la imagen de AnyConnect al flash del router, debe ser instalado vía la línea de comando. Los paquetes múltiples de AnyConnect pueden ser instalados cuando usted especifica un número de secuencia en el final del comando de la instalación; esto permitirá para que el router actúe como headend para los sistemas operativos del cliente múltiple. Cuando usted instala el paquete de AnyConnect, también lo moverá al **flash: directorio /webvpn/** si no fue copiado allí inicialmente.

```
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 fueron liberadas antes de 15.2(1)T, el comando de instalar el PKG es levemente diferente.

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

Paso 3. Habilite el servidor HTTP en el router

```
ip http server
ip http secure-server
```

Paso 4. Genere el par de claves RSA y el certificado autofirmado

Cuando usted configura el SSL o cualquier característica que implemente el Public Key Infrastructure (PKI) y los Certificados digitales, un keypair del Rivest-Shamir-Adleman (RSA) se requiere para la firma del certificado. El comando del siguiente generará un par de claves RSA que entonces sea utilizado cuando se genera el certificado uno mismo-firmado PKI. Cuando usted hace uso de un módulo de 2048 bits, no es un requisito, se recomienda para utilizar el módulo más grande disponible para la seguridad mejorada y la compatibilidad con las máquinas del cliente de AnyConnect. Para utilizar una escritura de la etiqueta descriptiva también se recomienda pues permitirá la facilidad de la administración de claves. La generación de claves puede ser confirmada con el **comando show crypto key mypubkey rsa**.

> **Note**: Pues hay muchos riesgos de seguridad asociados a hacer el RSA cierra exportable, la práctica recomendada es asegurarse que las claves están configuradas para ser no exportables que es el valor por defecto. Los riesgos que están implicados cuando usted hace el RSA cierran exportable se discuten en el este documento: Claves RSA que despliegan 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 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 exportable.
Key Data&colon;
```

```
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 con éxito, un trustpoint PKI se debe configurar con la información y el par de claves RSA de nuestro router. El Common Name (CN) en el Tema-nombre se debe configurar con la dirección IP o el nombre del dominio aprobado completo (FQDN) que los usuarios utilizan para conectar con el gateway de AnyConnect; en este ejemplo, los clientes utilizan el FQDN de fdenofa-SSLVPN.cisco.com cuando intentan conectar. Mientras que no es obligatorio, cuando usted ingresa correctamente en el CN, ayuda a reducir el número de errores del certificado que se indiquen en el login.

> **Note**: Bastante que usando un certificado autofirmado generado por el router, es posible utilizar un certificado publicado por CA de tercera persona. Esto se puede hacer vía algunos métodos distintos como se debate en este documento: Configurar la inscripción del certificado para un PKI.

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

Después de que el trustpoint se haya definido correctamente, el router debe generar el certificado usando el **pki crypto alista el** comando. Con este proceso, es posible especificar algunos otros parámetros tales como número de serie y dirección IP. Sin embargo, esto no se requiere. La generación del certificado puede ser confirmada con el comando **crypto de los Certificados del pki de la demostración**.

```
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 5. Cuentas de usuario de VPN locales de la configuración

Mientras que es posible utilizar una autenticación externa, servidor de la autorización, y de las estadísticas (AAA), porque esta autenticación local del ejemplo se utiliza. Estos comandos crearán un Nombre de usuario VPNUSER y también crearán una lista de la autenticación AAA nombrada SSLVPN_AAA.

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

Paso 6. Defina la lista de acceso de la agrupación de direcciones y del túnel dividido que se utilizará por los clientes

Un pool del IP Address local se debe crear para que los adaptadores del cliente de AnyConnect obtengan una dirección IP. Asegúrele la configuración bastante grande un pool para soportar el número máximo de conexiones cliente simultáneas de AnyConnect.

Por abandono, AnyConnect actuará en el modo túnel completo que significa que cualquier tráfico generado por la máquina del cliente será enviado a través del túnel. Pues esto no es típicamente deseable, es posible configurar una lista de control de acceso (ACL) que entonces defina el tráfico que debe o no se debe enviar a través del túnel. Como con otras implementaciones ACL, el implícitos niegan en el extremo eliminan la necesidad de un explícito niegan; por lo tanto, es solamente necesario configurar las declaraciones del permiso para el tráfico que debe ser tunneled.

```
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 7. Configure la interfaz de plantilla virtual (VTI)

VTIs dinámico proporcione una interfaz de acceso virtual separada a pedido para cada sesión de VPN que permita altamente seguro y la conectividad con posibilidades de ampliación para los VPN de accesos remotos. La tecnología DVTI substituye las correspondencias cifradas dinámicas y el método dinámico del hub-and-spoke que las ayudas establecen los túneles. Porque función de DVTIs como cualquier otra interfaz real que permitan para un despliegue remoto más complejo de Accesss porque soportan QoS, el Firewall, por usuario los attribtues y otros Servicios de seguridad tan pronto como el túnel sea activo.

```
interface Loopback0
```

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

Paso 8. Gateway del WebVPN de la configuración

El gateway del WebVPN es qué define la dirección IP y los puertos que serán utilizados por el headend de AnyConnect, así como el algoritmo de encripción de SSL y el certificado PKI que será presentado a los clientes. Por abandono, el gateway soportará todos los algoritmos de encripción posibles, que varían dependiendo de la versión de IOS en el router.

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

Paso 9. Contexto del WebVPN de la configuración y directiva del grupo

La directiva del contexto y del grupo del WebVPN define algunos parámetros adicionales que sean utilizados para la conexión cliente de AnyConnect. Para una configuración básica de AnyConnect, el contexto sirve simplemente como mecanismo usado para llamar la directiva del grupo predeterminado que será utilizada para AnyConnect. Sin embargo, el contexto se puede utilizar para personalizar más lejos la página del chapoteo del WebVPN y la operación del WebVPN. En el grupo de política definida, la lista SSLVPN_AAA se configura como la lista de la autenticación AAA de la cual los usuarios son un miembro. El comando SVC-**habilitado las funciones** es el pedazo de configuración que permita que los usuarios conecten con el **cliente VPN de** AnyConnect **SSL** bastante que apenas el WebVPN a través de un navegador. Pasado, los comandos svc adicionales definen los parámetros que son relevantes solamente a las conexiones de SVC: **la agrupación de direcciones svc** dice el gateway a los direccionamientos del folleto en el ACPool a los clientes, la **fractura svc incluye** define la directiva del túnel dividido por ACL 1 definida arriba, y el dns-**servidor svc** define al servidor DNS cuál será utilizado para la resolución del Domain Name. Con esta configuración, todas las interrogaciones DNS serán enviadas al servidor DNS especificado. El direccionamiento que se recibe en la respuesta de la interrogación dictará independientemente de si el tráfico está enviado a través del túnel.

```
webvpn context SSL_Context
 gateway SSLVPN_Gateway
 inservice
 policy group SSL_Policy
  aaa authentication list SSLVPN_AAA
  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
virtual-template 1
default-group-policy SSL_Policy
```

Paso 10 (opcional). Configure un perfil del cliente

A diferencia en de los ASA, el Cisco IOS no tiene una interfaz GUI incorporada que pueda ayudar a los admins en crear el perfil del cliente. El perfil del cliente de AnyConnect necesita ser creado/ser editado por separado con el editor independiente del perfil.

Tip: Busque anyconnect-profileeditor-win-3.1.03103-k9.exe

Siga los siguientes pasos para tener el router desplegar el perfil:

1. Carguelo al Flash IOS usando el ftp/tftp
2. Utilice este comando de identificar el perfil que acaba de ser cargado:

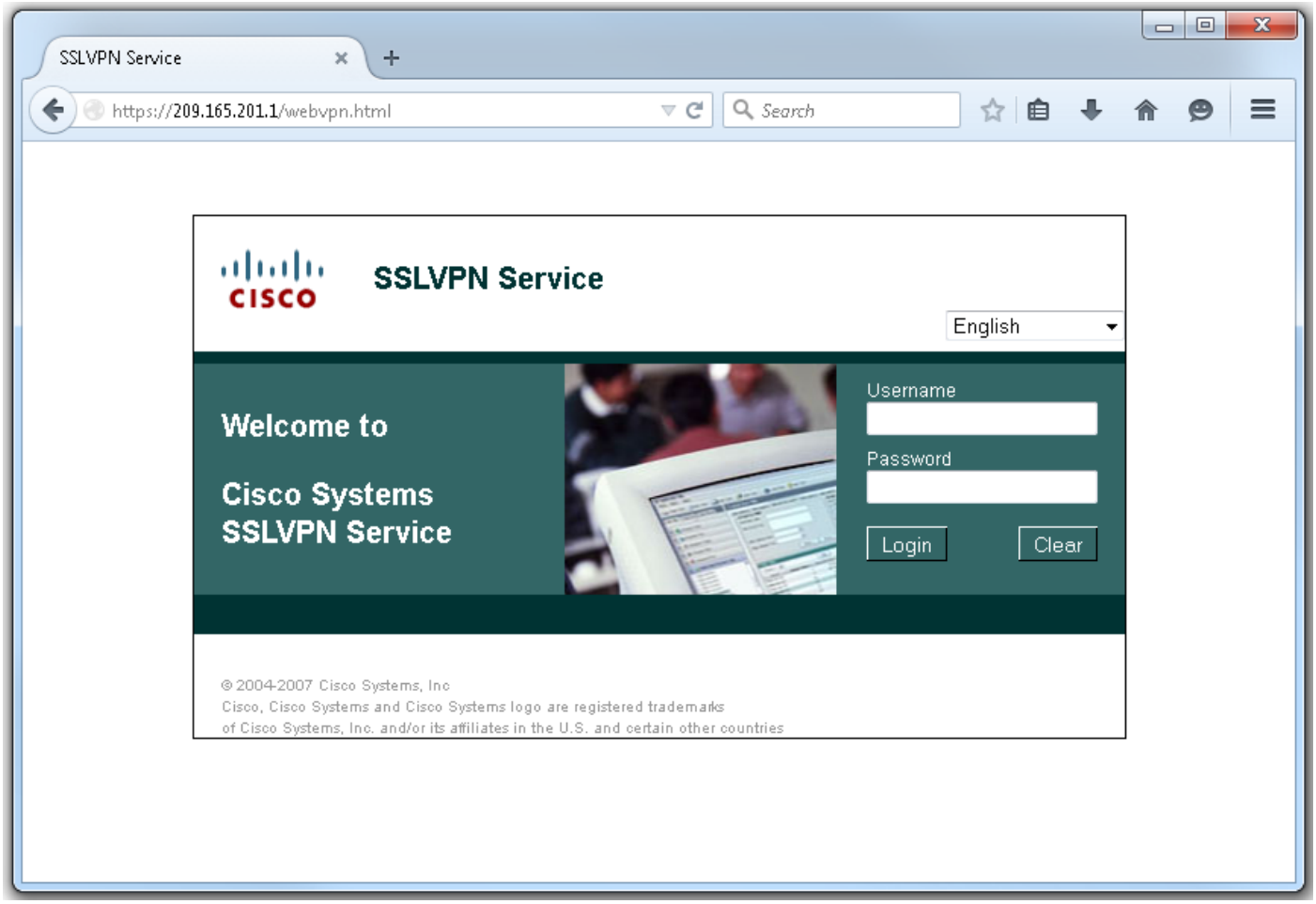
1.
```
webvpn context SSL_Context
 gateway SSLVPN_Gateway
 inservice
 policy group SSL_Policy
  aaa authentication list SSLVPN_AAA
  functions svc-enabled
  svc address-pool "SSLVPN_POOL" netmask 255.255.255.0
  svc split include acl 1
  svc dns-server primary 8.8.8.8
virtual-template 1
default-group-policy SSL_Policy
```
Tip: En las versiones de IOS más viejas que 15.2(1)T, este comando necesita ser utilizado: **flash del <profile_name> del perfil svc de la importación del webvpn: <profile.xml>**

3. Bajo contexto, utilice este comando de conectar el perfil a ese contexto:

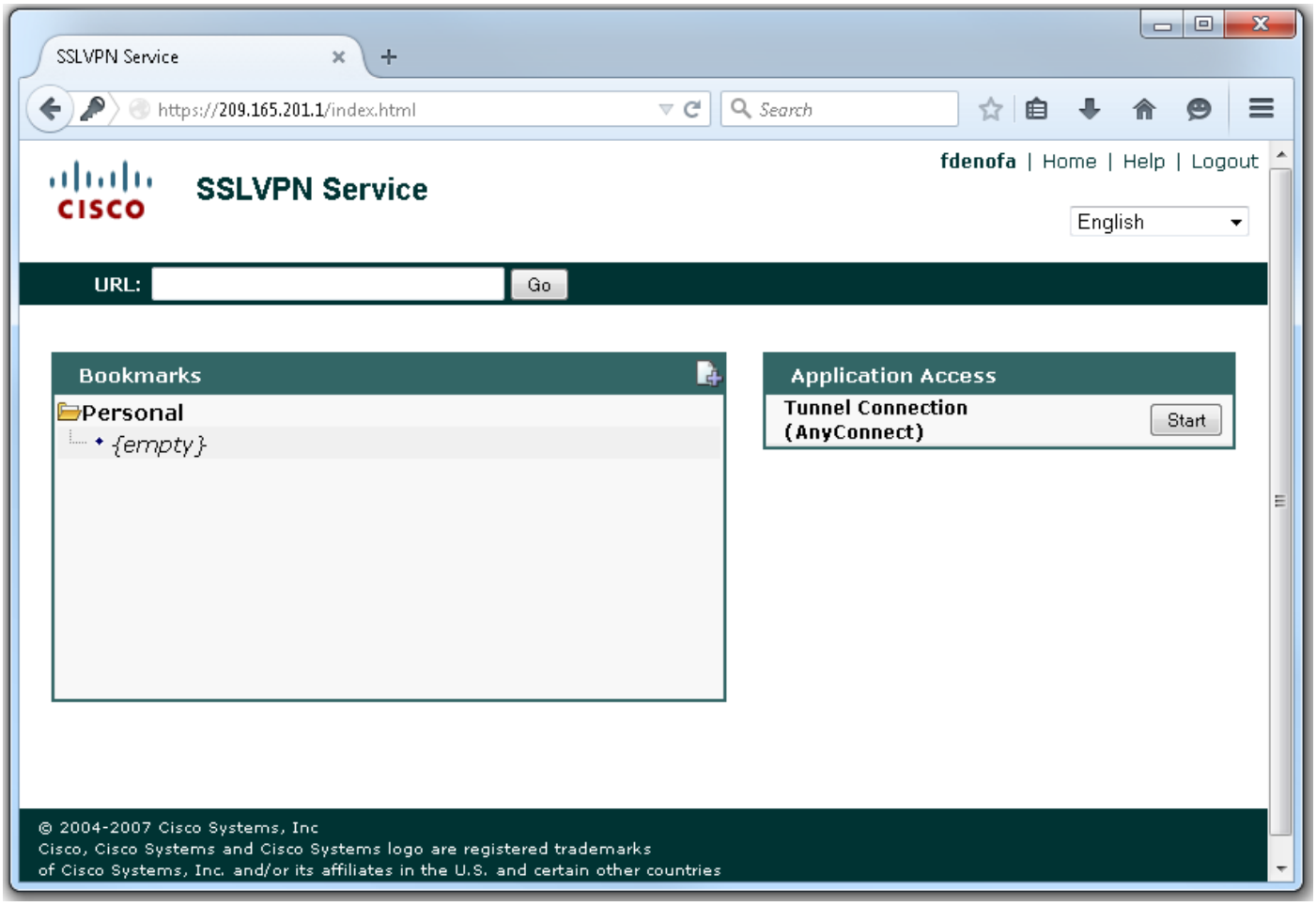
1.
```
webvpn context SSL_Context
 gateway SSLVPN_Gateway
 inservice
 policy group SSL_Policy
  aaa authentication list SSLVPN_AAA
  functions svc-enabled
  svc address-pool "SSLVPN_POOL" netmask 255.255.255.0
  svc split include acl 1
  svc dns-server primary 8.8.8.8
virtual-template 1
default-group-policy SSL_Policy
```
Note: Use la Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos usados en esta sección.

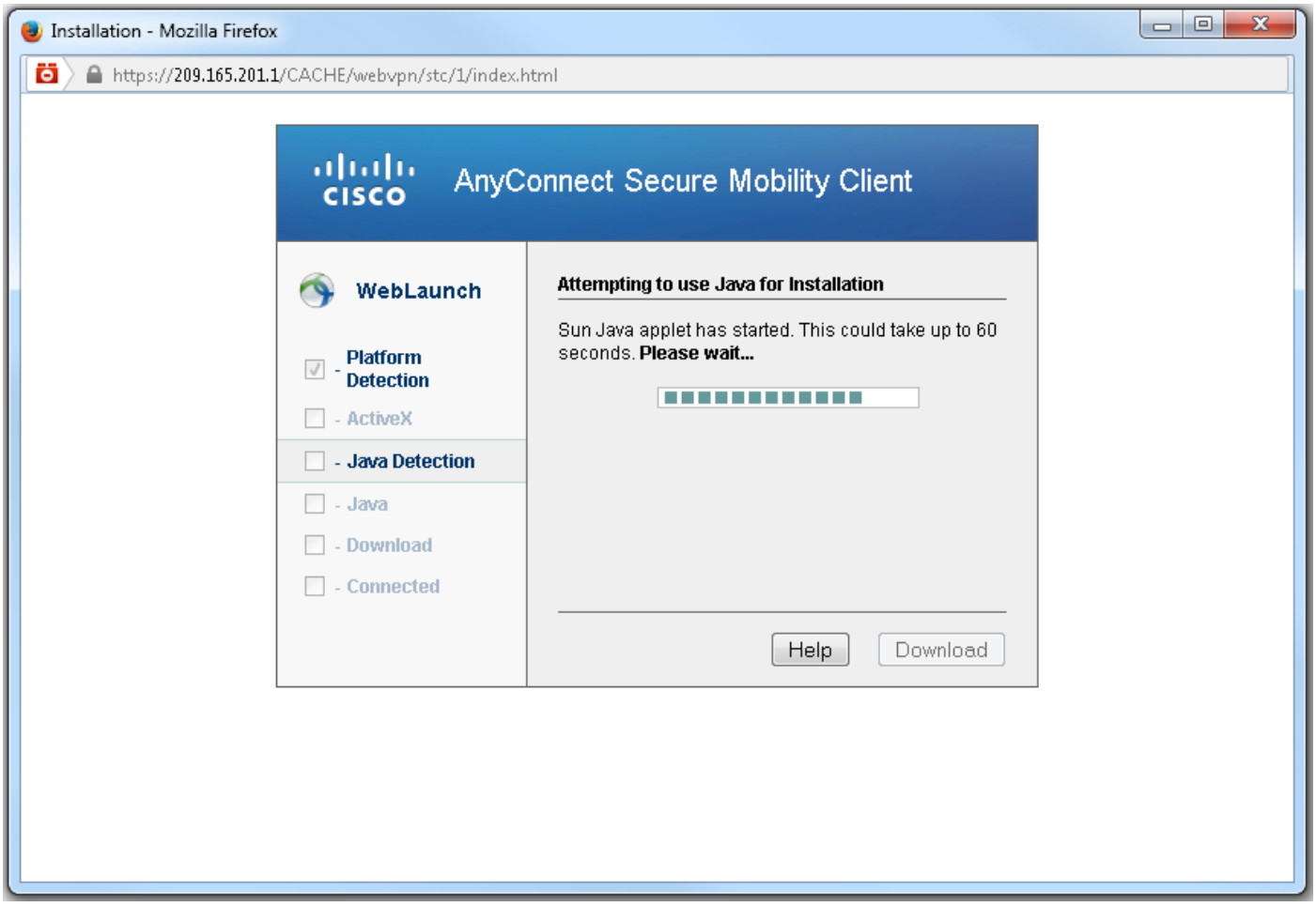
Verificación

Una vez que la configuración es completa, cuando usted accede a la dirección del gateway y vira hacia el lado de babor vía el navegador, volverá a la página del chapoteo del WebVPN.



Después de que usted inicie sesión, se visualiza el Home Page del WebVPN. De aquí, **conexión del túnel del** tecleo **(AnyConnect).** Cuando utilizan al Internet Explorer, ActiveX se utiliza para empujar hacia abajo y para instalar al cliente de AnyConnect. Si no se detecta, las Javas serán utilizadas en lugar de otro. El resto de los navegadores utilizan las Javas inmediatamente.

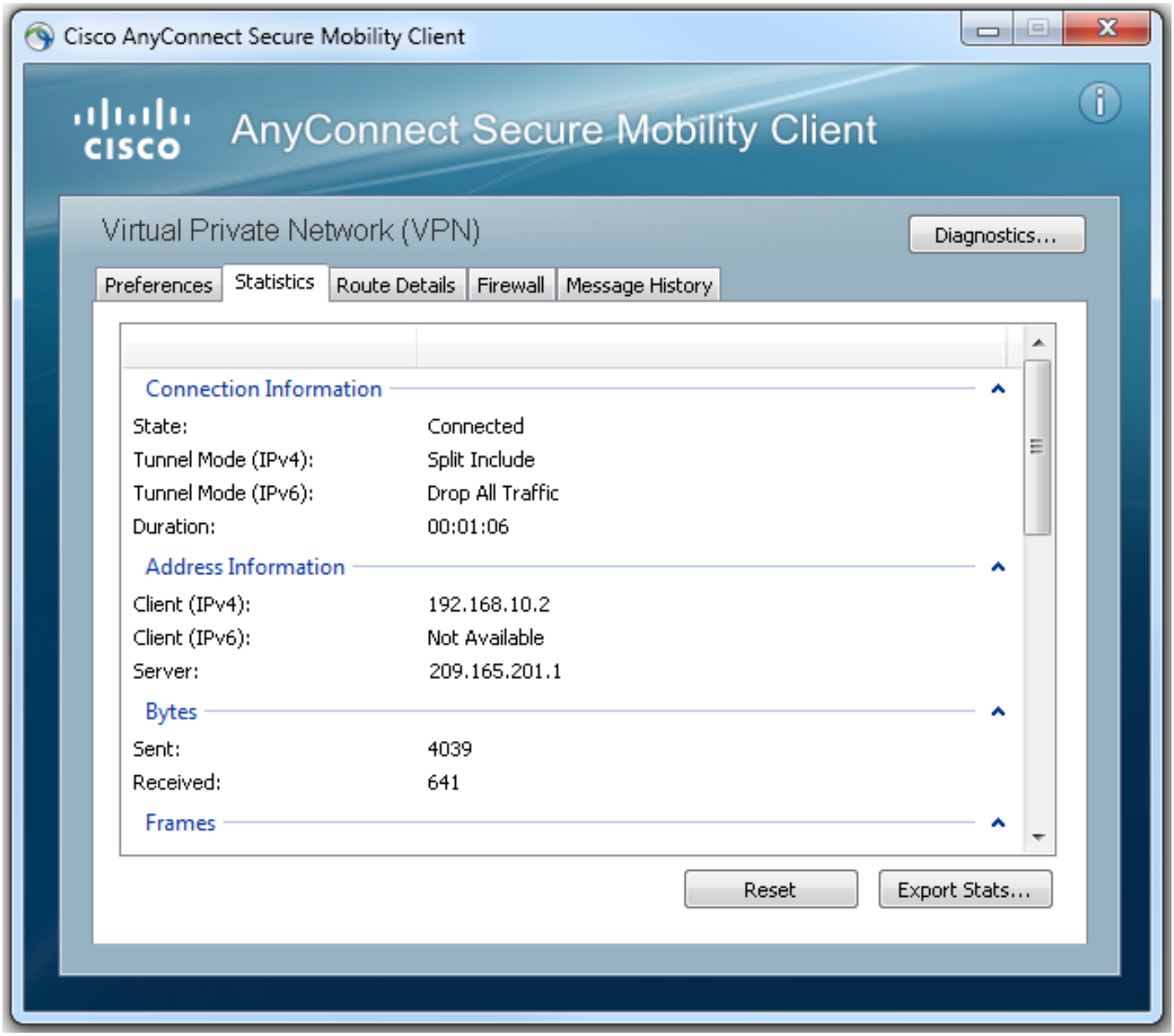


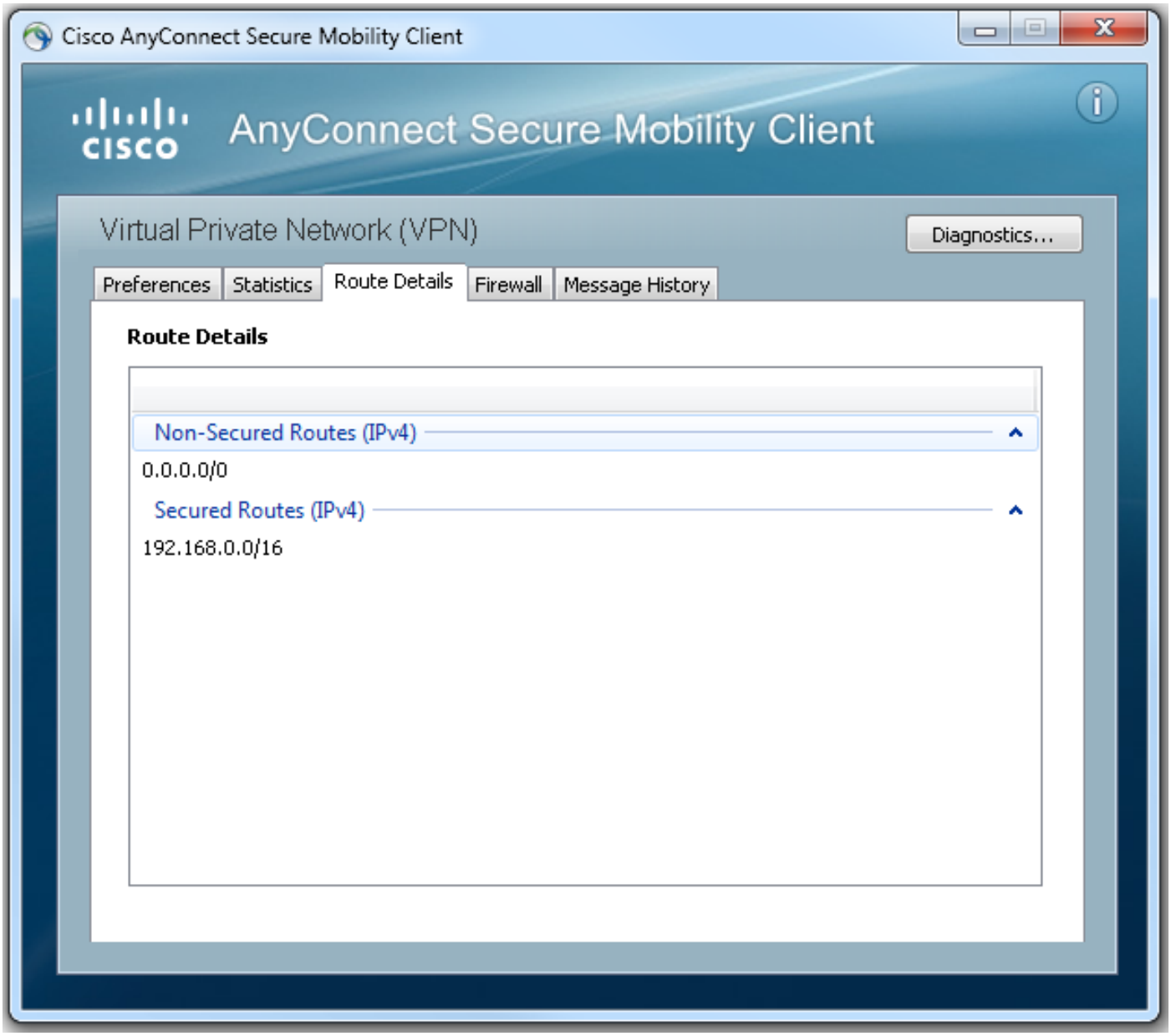


Una vez que se completa la instalación, AnyConnect intentará automáticamente conectar con el WebVPN el gateway. Pues un certificado autofirmado se está utilizando para que el gateway se

identifique, las advertencias del certificado múltiple aparecerán durante el intento de conexión. Éstos se esperan y se deben validar para que la conexión continúe. Para evitar estas advertencias del certificado, el certificado autofirmado que es presentado se debe instalar en el almacén del certificado confiable de la máquina del cliente, o si un certificado de tercera persona entonces se está utilizando el certificado del Certificate Authority debe estar en el almacén del certificado confiable.

Cuando la conexión completa la negociación, haga clic en el icono del **engranaje** en la izquierda inferior de AnyConnect visualizará una cierta información avanzada sobre la conexión. En esta página es posible ver algunos detalles de las estadísticas de conexión y de la ruta logrados del túnel dividido ACL en la configuración de la política del 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...



Aquí está el resultado final de la ejecutar-configuración de los pasos para la configuración:

```
webvpn context SSL_Context
 gateway SSLVPN_Gateway
 inservice
 policy group SSL_Policy
  aaa authentication list SSLVPN_AAA
  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
virtual-template 1
default-group-policy SSL_Policy
```

Troubleshooting

Hay algunos componentes comunes a marcar para cuando usted resuelve problemas los problemas de conexión de AnyConnect:

- Como el cliente debe presentar un certificado, es un requisito que el certificado especificó en el gateway del WebVPN sea válido. Para publicar un **certificado crypto del pki de la**

demostración mostrará la información que pertenece a todos los Certificados en el router.

- Siempre que un cambio se realice a la configuración del WebVPN, es una mejor práctica publicar un no en servicio y en servicio en el gateway y el contexto. Esto se asegurará que los cambios tomen el efecto correctamente.
- Según lo mencionado anterior, es un requisito tener un AnyConnect PKG para cada sistema operativo del cliente que conecte con este gateway. Por ejemplo, los clientes de Windows requieren Windows PKG, Linux que los clientes de 32 bits requieren Linux PKG de 32 bits, y así sucesivamente.
- Cuando usted considera al cliente de AnyConnect y el WebVPN basado en buscador utiliza el SSL, poder acceder la página del chapoteo del WebVPN indica generalmente que AnyConnect podrá conectar (asuma que la configuración pertinente de AnyConnect está correcta).

El Cisco IOS ofrece algunas diversas opciones del webvpn del debug que se puedan utilizar para resolver problemas las conexiones que fallan. Ésta es la salida generada del webvpn aaa del debug, del túnel del wevpn del debug, y de la sesión del webvpn de la demostración sobre una tentativa de la conexión satisfactoria:

```
webvpn context SSL_Context
 gateway SSLVPN_Gateway
 inservice
 policy group SSL_Policy
  aaa authentication list SSLVPN_AAA
  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
virtual-template 1
default-group-policy SSL_Policy
```

Información Relacionada

- Guía de configuración VPN SSL, Cisco IOS Release 15M&T
- Cliente de AnyConnect VPN (SSL) en el router IOS con el ejemplo de configuración CCP