Conexión telefónica de AnyConnect VPN a un ejemplo de la configuración del router del Cisco IOS

Contenido

Introducción

Este documento describe cómo configurar los dispositivos del router del ® del Cisco IOS y del encargado de llamada de modo que los Teléfonos IP de Cisco puedan establecer las conexiones VPN al router del Cisco IOS. Estas conexiones VPN son necesarias para asegurar la comunicación con cualquiera de estos dos métodos de autenticación de cliente:

- Servidor o base de datos local del Authentication, Authorization, and Accounting (AAA)
- Certificado del teléfono

Prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

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

- Cisco IOS 15.1(2)T o más adelante
- Característica fijada/licencia: Universal (datos y Seguridad y UC) para el router del servicio integrado del Cisco IOS (ISR)-G2
- Característica fijada/licencia: Seguridad avanzada para el Cisco IOS ISR
- Versión 8.0.1.100000-4 del encargado de las Comunicaciones unificadas de Cisco (CUCM) o más adelante
- Versión 9.0(2)SR1S del teléfono IP - Skinny Call Control Protocol (SCCP) o más adelante

Para una lista completa de teléfonos utilizados en su versión CUCM, complete estos pasos:

1. Abra este URL: **https:// *<CUCM IP del servidor Address>:8443/cucreports/systemReports.do***
2. Elija la **lista unificada de la función del teléfono cm > generan un nuevos informe > característica: Virtual Private Network**.

Las versiones usadas en este ejemplo de la configuración incluyen:

- Versión 15.1(4)M4 del router del Cisco IOS
- Versión 8.5.1.10000-26 del encargado de llamada
- Versión 9.1(1)SR1S del teléfono IP

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

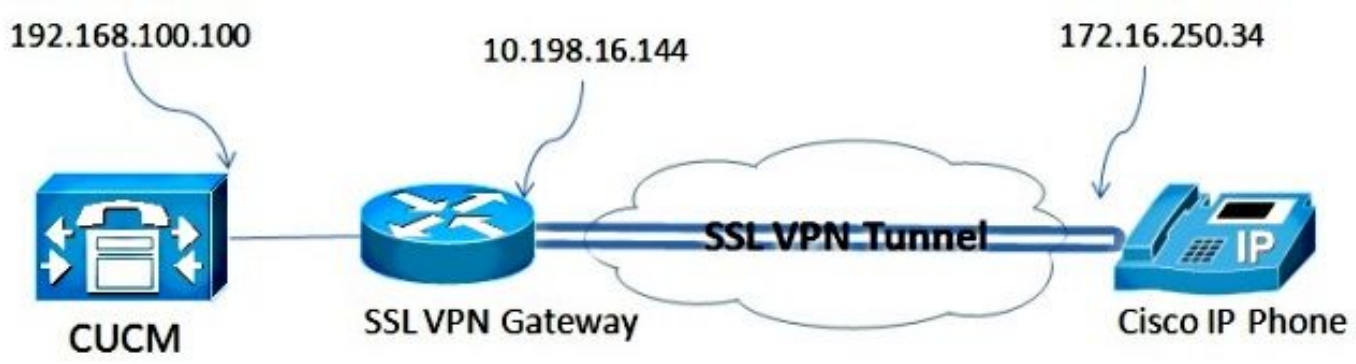
Configurar

Esta sección cubre la información necesaria para configurar las características descritas en este documento.

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

Topología de red

La topología usada en este documento incluye un teléfono IP de Cisco, el router del Cisco IOS como el gateway de VPN de Secure Sockets Layer (SSL), y CUCM como el gateway de la Voz.



Configuración de servidor VPN SSL

Esta sección describe cómo configurar el centro distribuidor del Cisco IOS para permitir las conexiones VPN entrantes SSL.

Pasos de la configuración común

1. Genere la clave del Rivest-Shamir-Adleman (RSA) con una longitud de 1024 bytes:

```
Router(config)#crypto key generate rsa general-keys label SSL modulus 1024
```

2. Cree el trustpoint para el certificado autofirmado, y asocie la clave SSL RSA:

```
Router(config)#crypto pki trustpoint server-certificate
enrollment selfsigned
usage ssl-server
serial-number
subject-name CN=10.198.16.144
revocation-check none
rsakeypair SSL
```

3. Una vez que se configura el trustpoint, aliste el certificado autofirmado con este comando:

```
Router(config)#crypto pki enroll server-certificate
% Include an IP address in the subject name? [no]: no
Generate Self Signed Router Certificate? [yes/no]: yes

Router Self Signed Certificate successfully created
```

4. Active el paquete correcto de AnyConnect en el centro distribuidor. El teléfono sí mismo no descarga este paquete. Pero, sin el paquete, el túnel VPN no establece. Se recomienda para utilizar la última versión del software cliente disponible en Cisco.com. Este ejemplo utiliza la versión 3.1.3103.

   En más viejas versiones del Cisco IOS, éste es el comando para activar el paquete:

```
Router(config)#webvpn install svc flash:anyconnect-win-3.1.03103-k9.pkg
```

   Sin embargo, en la última versión del Cisco IOS, éste es el comando:

```
Router(config)#crypto vpn anyconnect flash:/webvpn/anyconnect-win-
3.1.03103-k9.pkg sequence 1
```

5. Configure el gateway de VPN. El gateway de WebVPN se utiliza para terminar la conexión SSL del usuario.

```
Router(config)#crypto vpn anyconnect flash:/webvpn/anyconnect-win-
3.1.03103-k9.pkg sequence 1
```

   Note: Cualquier la dirección IP usada aquí necesita estar en la misma subred como el interfaz con el cual los teléfonos conectan, o el gateway necesita ser originario directamente de un interfaz en el router. El gateway también se utiliza para definir qué certificado es utilizado por el router para validar sí mismo al cliente.
6. Defina a la agrupación local que se utiliza para asignar los IP Addresses a los clientes cuando conectan:

```
Router(config)#crypto vpn anyconnect flash:/webvpn/anyconnect-win-
3.1.03103-k9.pkg sequence 1
```

Configuración con la autenticación AAA

Esta sección describe los comandos que usted necesita para configurar el servidor AAA o la base de datos local para autenticar sus teléfonos. Si usted planea utilizar la autenticación del certificado-solamente para los teléfonos, continúe a la siguiente sección.

Configure la base de datos de usuarios

La base de datos local del router o un servidor AAA del externo se puede utilizar para la autenticación:

- Para configurar la base de datos local, ingrese:

```
Router(config)#crypto vpn anyconnect flash:/webvpn/anyconnect-win-
3.1.03103-k9.pkg sequence 1
```

- Para configurar un servidor del telecontrol RADIUS AAA para la autenticación, ingrese:

```
Router(config)#crypto vpn anyconnect flash:/webvpn/anyconnect-win-
3.1.03103-k9.pkg sequence 1
```

Configure el contexto virtual y la Grupo-directiva

El contexto virtual se utiliza para definir los atributos que gobiernan la conexión VPN, por ejemplo:

- Qué URL a utilizar cuando usted conecta
- Qué pool a utilizar para asignar a las direcciones cliente
- Qué método de autenticación a utilizar

Estos comandos son un ejemplo de un contexto que utilice la autenticación AAA para el cliente:

```
Router(config)#crypto vpn anyconnect flash:/webvpn/anyconnect-win-
3.1.03103-k9.pkg sequence 1
```

Configuración con IP del teléfono el certificado significativo localmente - (LSC) para la autenticación de cliente

Esta sección describe los comandos que usted necesita para configurar la autenticación de

cliente certificado-basada para los teléfonos. Sin embargo, para hacer esto, el conocimiento de los diversos tipos de Certificados del teléfono se requiere:

- **Certificado instalado fabricante (MIC) -** MICs se incluye en 7941, 7961, y los Teléfonos IP de Cisco del nuevo-modelo. MICs es los Certificados dominantes 2,048-bit que son firmados por el Certificate Authority (CA) de Cisco. Para que el CUCM confíe en el certificado MIC, utiliza los Certificados CA instalados previamente CAP-RTP-001, CAP-RTP-002, y Cisco_Manufacturing_CA en su almacén de la confianza del certificado. Porque este certificado es proporcionado por el fabricante sí mismo, como se indica en el nombre, no se recomienda para utilizar este certificado para la autenticación de cliente.
- **LSC -** El LSC asegura la conexión entre CUCM y el teléfono después de que usted configure el modo de la seguridad del dispositivo para la autenticación o el cifrado. El LSC posee la clave pública para el teléfono IP de Cisco, que es firmado por la clave privada de la función del proxy de la autoridad de certificación CUCM (CAPF). Éste es el método más seguro (en comparación con el uso de MICs).
  Precaución: Debido al riesgo de seguridad mayor, Cisco recomienda el uso de MICs solamente para la instalación LSC y no para el uso continuo. Los clientes que configuran los Teléfonos IP de Cisco para utilizar MICs para la autenticación de Transport Layer Security (TLS), o para cualquier otro propósito, hacen tan por su cuenta y riesgo.

En este ejemplo de la configuración, el LSC se utiliza para autenticar los teléfonos.

> Consejo: La manera más segura de conectar su teléfono es utilizar la autenticación dual, que combina el certificado y la autenticación AAA. Usted puede configurar esto si usted combina los comandos usados para cada uno bajo un contexto virtual.

Configure el Trustpoint para validar el certificado del cliente

El router debe hacer el certificado CAPF instalar para validar el LSC del teléfono IP. Para conseguir ese certificado y instalarlo en el router, complete estos pasos:

1. Vaya a la página Web de administración del sistema operativo CUCM (OS).
2. Elija el **Certificate Management (Administración de certificados) de la Seguridad**.
   Note: Esta ubicación pudo cambiar basado en la versión CUCM.
3. Encuentre el certificado etiquetado **CAPF**, y descargue el fichero **.pem**. Sálvelo como fichero de **.txt**
4. Una vez que se extrae el certifcate, cree un nuevo trustpoint en el router, y autentique el trustpoint con CAPF, como se muestra aquí. Cuando estaba incitado para el base 64 codificó el certificado CA, seleccionan y pegan el texto en el fichero descargado .pem junto con las líneas del COMENZAR y de EXTREMO.

```
Router(config)#crypto pki trustpoint CAPF
enrollment terminal
authorization username subjectname commonname
revocation-check none
Router(config)#crypto pki authenticate CAPF
Router(config)#

<base-64 encoded CA certificate>

quit
```

Cosas a observar:

- El método de la inscripción es terminal porque el certificado tiene que ser instalado manualmente en el router.
- Requieren al **comando username de la autorización** para decir al router qué utilizar como el username cuando el cliente hace la conexión. En este caso, utiliza el nombre común (NC).
- Un control de la revocación necesita ser inhabilitado porque los Certificados del teléfono no tienen un Listas de revocación de certificados (CRL) definido. Así pues, a menos que se inhabilite, la conexión falla y las depuraciones del Public Key Infrastructure (PKI) muestran esta salida:

```
Jun 17 21:49:46.695: CRYPTO_PKI: (A0076) Starting CRL revocation check
Jun 17 21:49:46.695: CRYPTO_PKI: Matching CRL not found
Jun 17 21:49:46.695: CRYPTO_PKI: (A0076) CDP does not exist. Use SCEP to
query CRL.
Jun 17 21:49:46.695: CRYPTO_PKI: pki request queued properly
Jun 17 21:49:46.695: CRYPTO_PKI: Revocation check is complete, 0
Jun 17 21:49:46.695: CRYPTO_PKI: Revocation status = 3
Jun 17 21:49:46.695: CRYPTO_PKI: status = 0: poll CRL
Jun 17 21:49:46.695: CRYPTO_PKI: Remove session revocation service providers
CRYPTO_PKI: Bypassing SCEP capabilies request 0
Jun 17 21:49:46.695: CRYPTO_PKI: status = 0: failed to create GetCRL
Jun 17 21:49:46.695: CRYPTO_PKI: enrollment url not configured
Jun 17 21:49:46.695: CRYPTO_PKI: transaction GetCRL completed
Jun 17 21:49:46.695: CRYPTO_PKI: status = 106: Blocking chain verification
callback received status
Jun 17 21:49:46.695: CRYPTO_PKI: (A0076) Certificate validation failed
```

Configure el contexto virtual y la Grupo-directiva

Esta parte de la configuración es similar a la configuración usada previamente, a excepción de dos puntas:

- El método de autenticación
- El trustpoint las aplicaciones del contexto para autenticar los teléfonos

Los comandos se muestran aquí:


```
Jun 17 21:49:46.695: CRYPTO_PKI: (A0076) Starting CRL revocation check
Jun 17 21:49:46.695: CRYPTO_PKI: Matching CRL not found
Jun 17 21:49:46.695: CRYPTO_PKI: (A0076) CDP does not exist. Use SCEP to
query CRL.
Jun 17 21:49:46.695: CRYPTO_PKI: pki request queued properly
Jun 17 21:49:46.695: CRYPTO_PKI: Revocation check is complete, 0
Jun 17 21:49:46.695: CRYPTO_PKI: Revocation status = 3
Jun 17 21:49:46.695: CRYPTO_PKI: status = 0: poll CRL
Jun 17 21:49:46.695: CRYPTO_PKI: Remove session revocation service providers
CRYPTO_PKI: Bypassing SCEP capabilies request 0
Jun 17 21:49:46.695: CRYPTO_PKI: status = 0: failed to create GetCRL
Jun 17 21:49:46.695: CRYPTO_PKI: enrollment url not configured
Jun 17 21:49:46.695: CRYPTO_PKI: transaction GetCRL completed
Jun 17 21:49:46.695: CRYPTO_PKI: status = 106: Blocking chain verification
callback received status
Jun 17 21:49:46.695: CRYPTO_PKI: (A0076) Certificate validation failed
```


Configuración de administrador de la llamada

Esta sección describe los pasos de la configuración de administrador de la llamada.

Exporte Uno mismo-haber firmado o el certificado de identidad del router al CUCM

Para exportar el certificado del router e importar el certificado en el encargado de llamada como certificado de la Teléfono-VPN-confianza, complete estos pasos:

1. Controle el certificado usado para el SSL.

```
Router#show webvpn gateway SSL
SSL Trustpoint: server-certificate
```

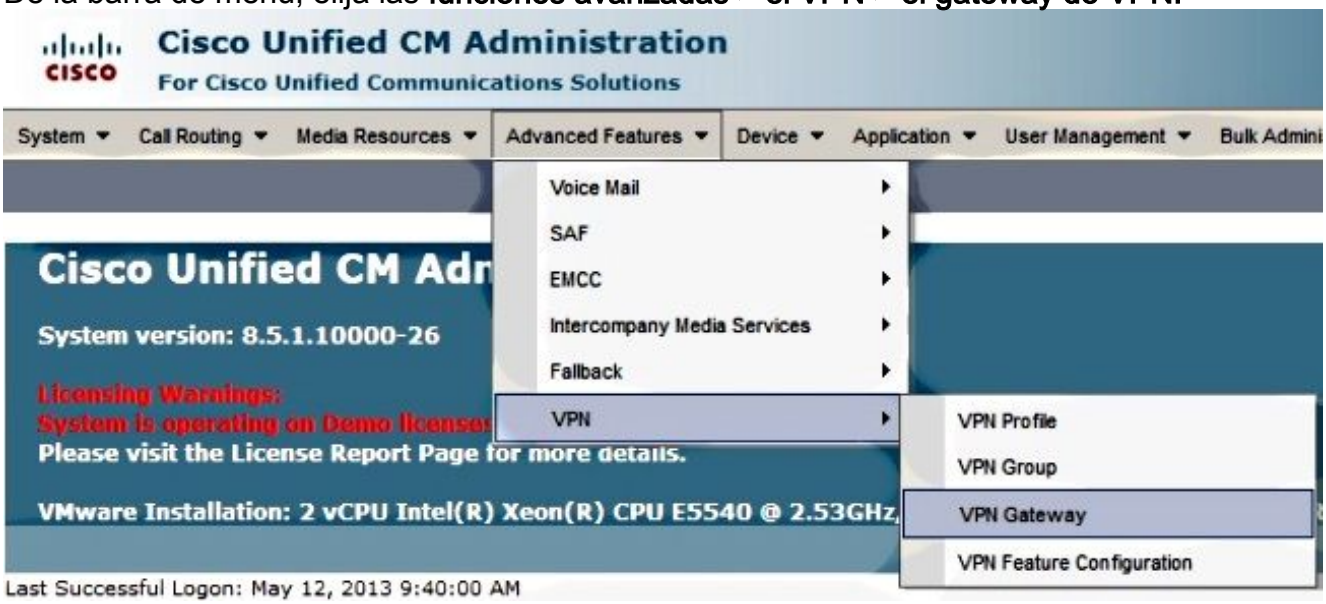
2. Exporte el certificado.

```
Router(config)#crypto pki export server-certificate pem terminal
The Privacy Enhanced Mail (PEM) encoded identity certificate follows:
-----BEGIN CERTIFICATE-----

<output removed>

-----END CERTIFICATE-----
```

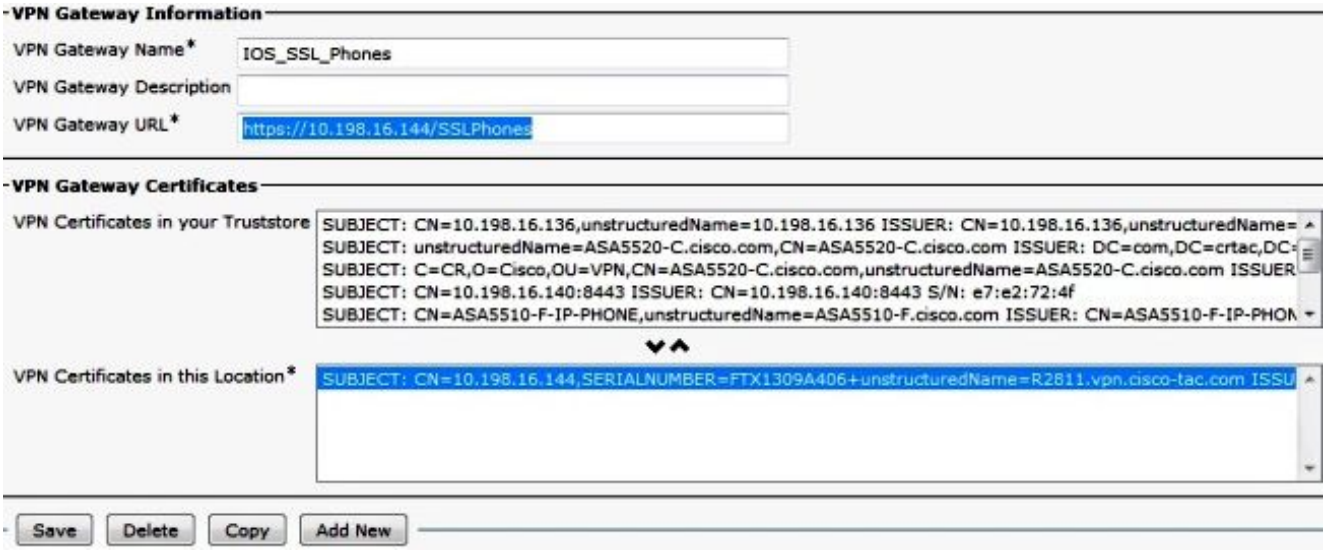
3. Copie el texto de la terminal y sálvelo como un fichero **.pem**.
4. Ábrase una sesión al encargado de llamada, y elija el **Certificate Management (Administración de certificados) del > Security (Seguridad) de la administración OS > el certificado unificados de la carga por teletratamiento > Teléfono-VPN-confianza selecta** para cargar por teletratamiento el archivo de certificado guardado en el paso anterior.

Configure el gateway de VPN, el grupo, y el perfil en el CUCM

1. Navegue a **Cisco unificó la administración cm**.
2. De la barra de menú, elija las **funciones avanzadas > el VPN > el gateway de VPN.**

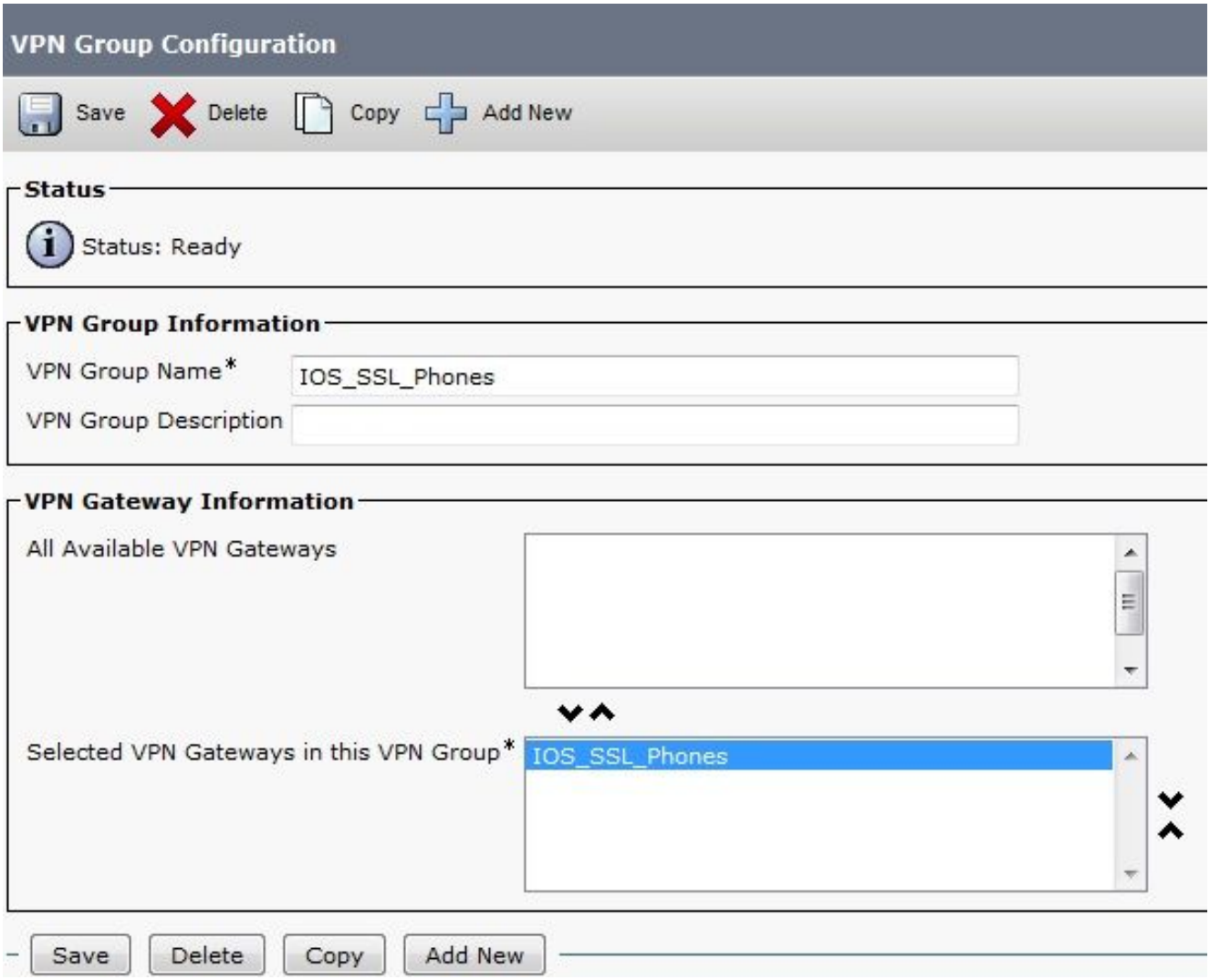


3. En la ventana de configuración del gateway de VPN, complete estos pasos:
   En el campo de nombre del gateway de VPN, ingrese un nombre. Éste puede ser cualquier nombre.En el campo Description (Descripción) del gateway de VPN, ingrese una descripción (opcional).En el campo URL del gateway de VPN, ingrese el grupo-URL definido en el ranurador.En los Certificados VPN en este campo de la ubicación, elija el certificado que fue cargado por teletratamiento al encargado de llamada previamente para moverlo desde el almacén de la confianza a esta
   ubicación.

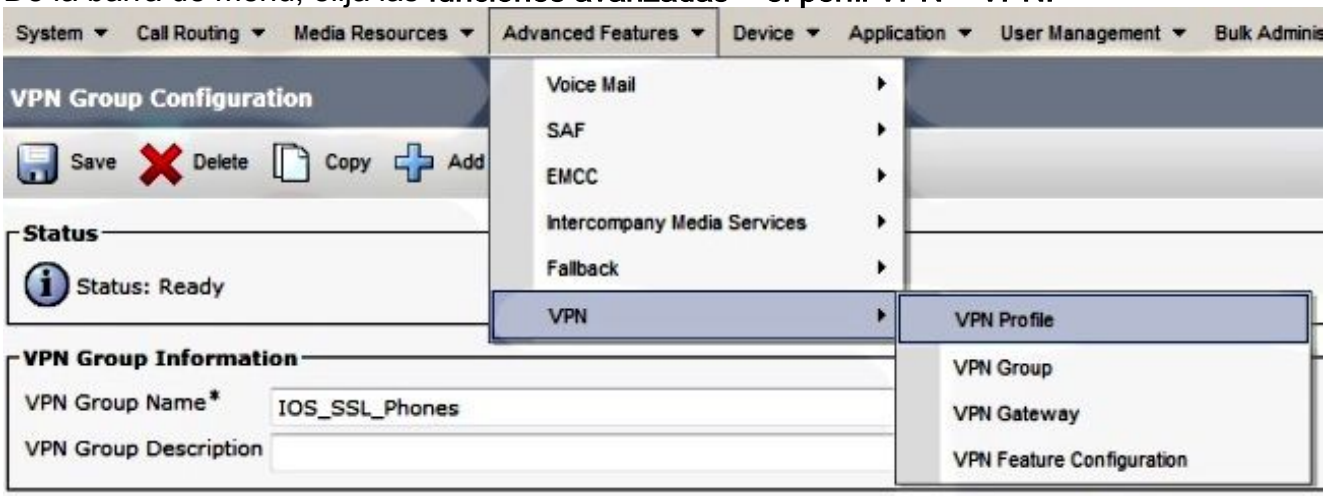


4. De la barra de menú, elija las **funciones avanzadas > al grupo VPN > VPN.**

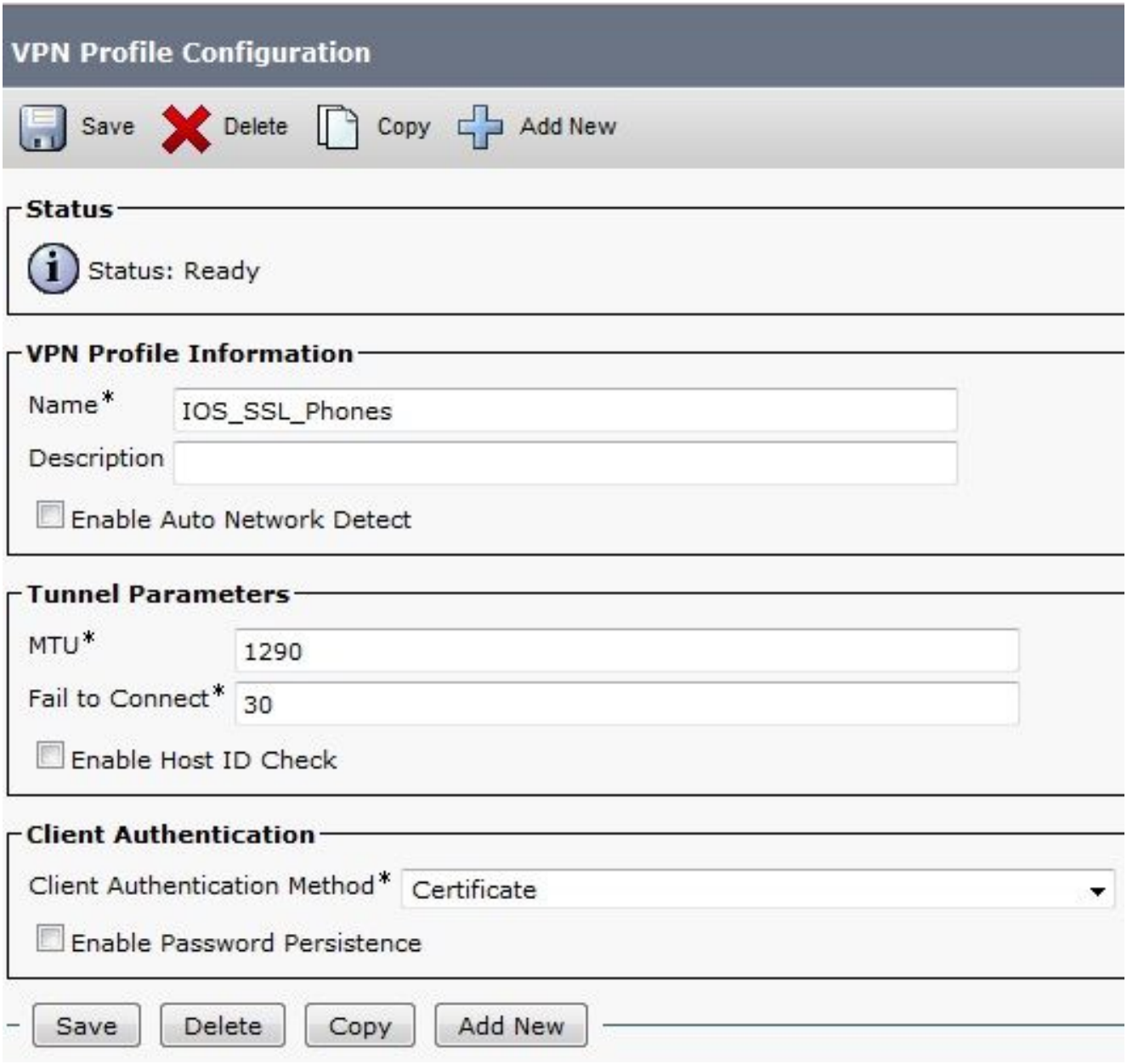
5. En todos los gateways de VPN disponibles coloque, elija el **gateway de VPN** definido previamente. Haga clic la flecha hacia abajo para mover el gateway seleccionado a los gateways de VPN seleccionados en este campo del grupo VPN.



6. De la barra de menú, elija las **funciones avanzadas > el perfil VPN > VPN.**



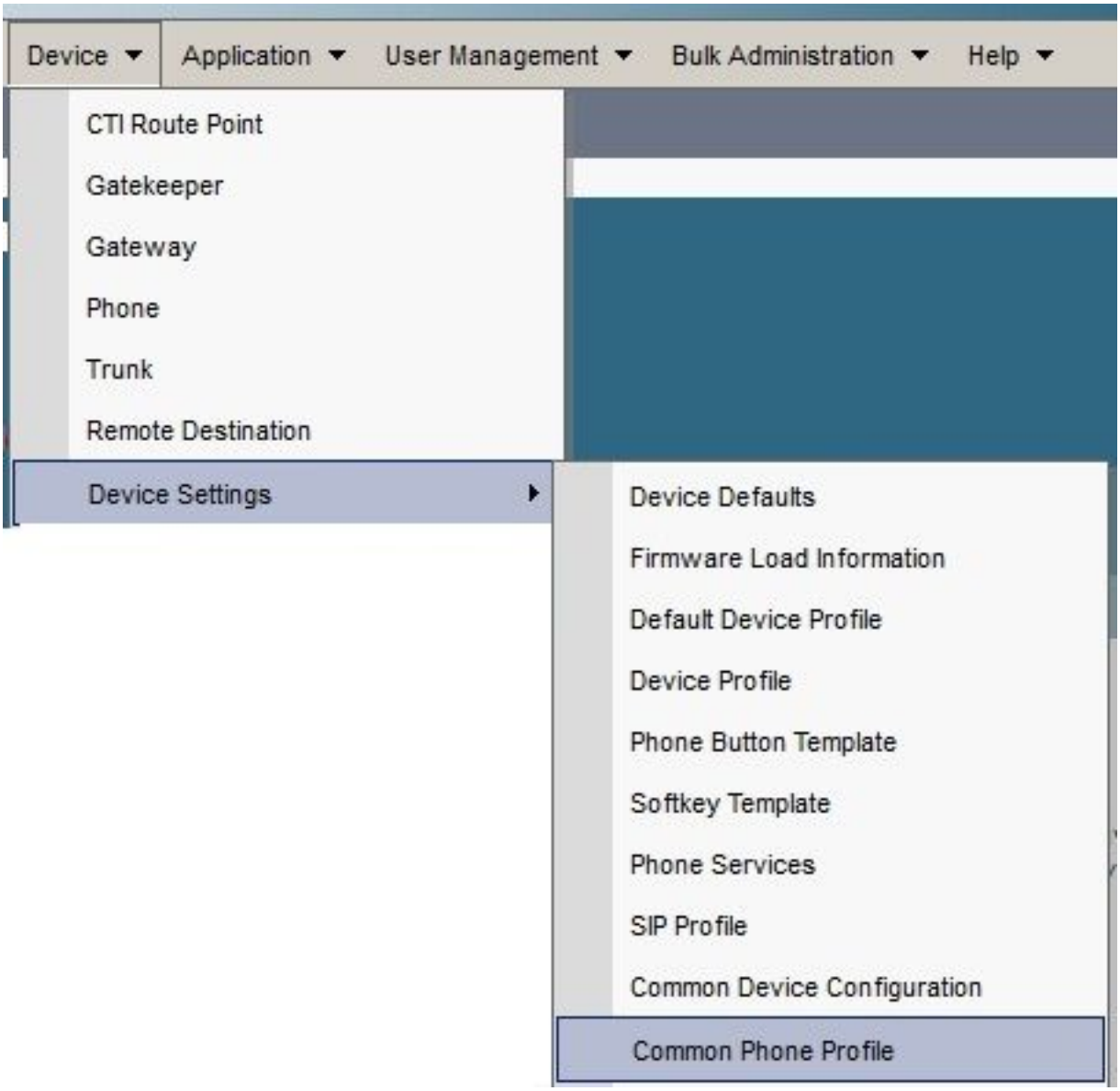
7. Para configurar el perfil VPN, complete todos los campos que se marquen con un asterisco (*).

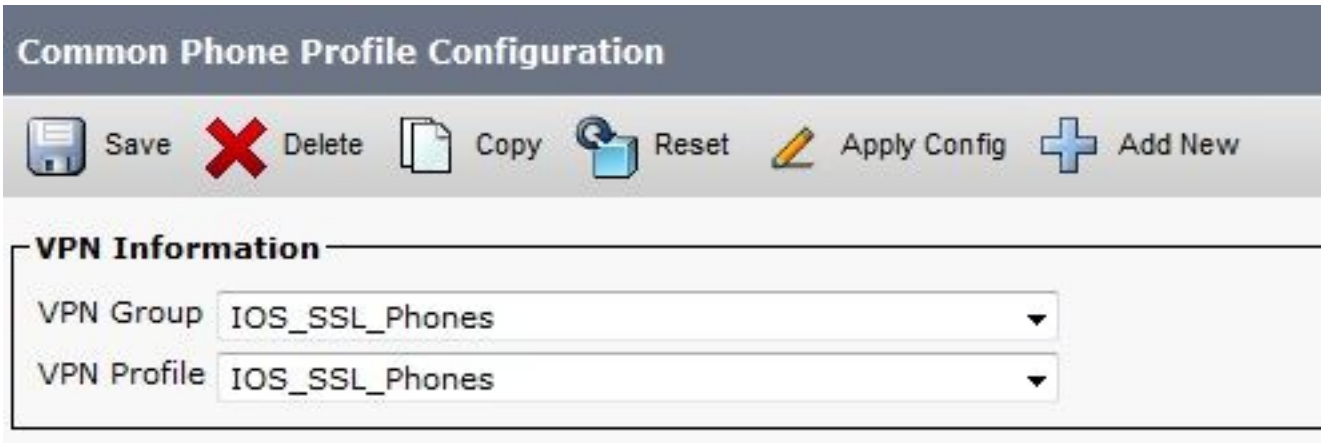


La red auto del permiso detecta: Si está activado, el teléfono VPN hace ping el servidor TFTP. Si no se recibe ninguna respuesta, él los auto-iniciados una conexión VPN.**Control del ID del host del permiso:** Si está activado, el teléfono VPN compara el nombre de dominio completo (FQDN) del gateway de VPN URL contra la red de área CN/Storage (SAN) del certificado. El cliente no puede conectar si estos items no hacen juego o si un certificado del comodín con un asterisco (*) se utiliza.**Persistencia de la contraseña del permiso:** Esto permite que el teléfono VPN oculte el nombre de usuario y contraseña para la tentativa siguiente VPN.

Aplique el grupo y el perfil al teléfono IP con el perfil común del teléfono

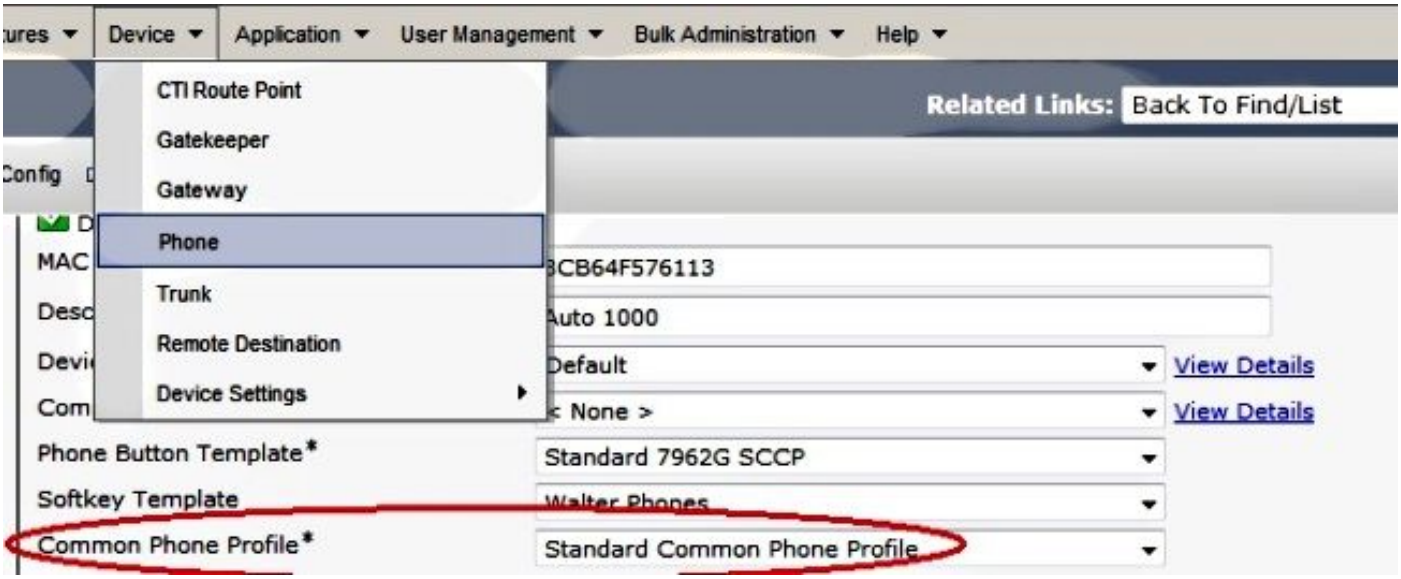
En la ventana común de la configuración del perfil del teléfono, el tecleo **aplica los Config** para aplicar la nueva configuración VPN. Usted puede utilizar el **perfil común** estándar del **teléfono** o crear un nuevo perfil.





Aplique el perfil común del teléfono al teléfono IP

Si usted creó un nuevo perfil para los teléfonos/los usuarios específicos, navegue a la ventana de la **Configuración del teléfono**. En el campo común del perfil del teléfono, elija el perfil **común estándar del teléfono**.



Instale localmente - los Certificados significativos (LSC) en los Teléfonos IP de Cisco

La guía siguiente se puede utilizar para instalar localmente - los Certificados significativos en los Teléfonos IP de Cisco. Este paso es solamente necesario si la autenticación usando el LSC se utiliza. La autenticación usando el Manufacterer instaló el certificado (MIC) o el nombre de usuario y contraseña no requiere un LSC ser instalado.

Instale un LSC en un teléfono con el modo seguro del racimo CUCM fijado No-seguro.

Registre el teléfono al encargado de llamada otra vez para descargar la nueva configuración

Éste es el último paso en el proceso de configuración.

Verificación

Verificación del router

Para controlar las estadísticas de la sesión de VPN en el router, usted puede utilizar estos comandos, y controla las diferencias entre las salidas (destacadas) para saber si hay username y certifica la autenticación:

Para el username/la autenticación de contraseña:

```
Router#show webvpn session user phones context SSL
Session Type : Full Tunnel
Client User-Agent : Cisco SVC IPPhone Client v1.0 (1.0)

Username : phones                Num Connection : 1
Public IP : 172.16.250.34 VRF Name : None
Context : SSL Policy Group : SSLPhones
Last-Used : 00:00:29 Created : 15:40:21.503 GMT
Fri Mar 1 2013
Session Timeout : Disabled Idle Timeout : 2100
DPD GW Timeout : 300 DPD CL Timeout : 300
Address Pool : SSL MTU Size : 1290
Rekey Time : 3600 Rekey Method :
```

```
Lease Duration : 43200
Tunnel IP : 10.10.10.1 Netmask : 255.255.255.0
Rx IP Packets : 106 Tx IP Packets : 145
CSTP Started : 00:11:15 Last-Received : 00:00:29
CSTP DPD-Req sent : 0 Virtual Access : 1
Msie-ProxyServer : None Msie-PxyPolicy : Disabled
Msie-Exception :
Client Ports : 51534
DTLS Port : 52768
Router#

Router#show webvpn session context all
WebVPN context name: SSL
Client_Login_Name  Client_IP_Address  No_of_Connections  Created  Last_Used
phones             172.16.250.34              1         00:30:38  00:00:20
```

Para la autenticación del certificado:

```
Router#show webvpn session user SEP8CB64F578B2C context all
Session Type : Full Tunnel
Client User-Agent : Cisco SVC IPPhone Client v1.0 (1.0)

Username : SEP8CB64F578B2C      Num Connection : 1
Public IP : 172.16.250.34 VRF Name : None
CA Trustpoint  : CAPF
Context : SSL Policy Group :
Last-Used : 00:00:08 Created : 13:09:49.302 GMT
Sat Mar 2 2013
Session Timeout : Disabled Idle Timeout : 2100
DPD GW Timeout : 300 DPD CL Timeout : 300
Address Pool : SSL MTU Size : 1290
Rekey Time : 3600 Rekey Method :
Lease Duration : 43200
Tunnel IP : 10.10.10.2 Netmask : 255.255.255.0
Rx IP Packets : 152 Tx IP Packets : 156
CSTP Started : 00:06:44 Last-Received : 00:00:08
CSTP DPD-Req sent : 0 Virtual Access : 1
Msie-ProxyServer : None Msie-PxyPolicy : Disabled
Msie-Exception :
Client Ports : 50122
DTLS Port : 52932


Router#show webvpn session context all
WebVPN context name: SSL
Client_Login_Name  Client_IP_Address  No_of_Connections  Created  Last_Used
SEP8CB64F578B2C    172.16.250.34              1         3d04h     00:00:16
```

Verificación CUCM

Confirme que el teléfono IP está registrado con el encargado de llamada con el direccionamiento asignado el router proporcionado a la conexión SSL.

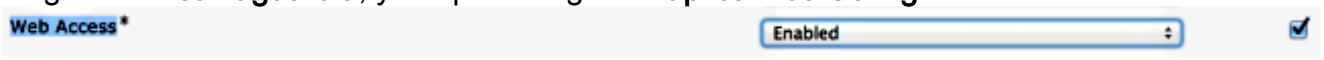
Troubleshooting

Depuraciones en el servidor VPN SSL

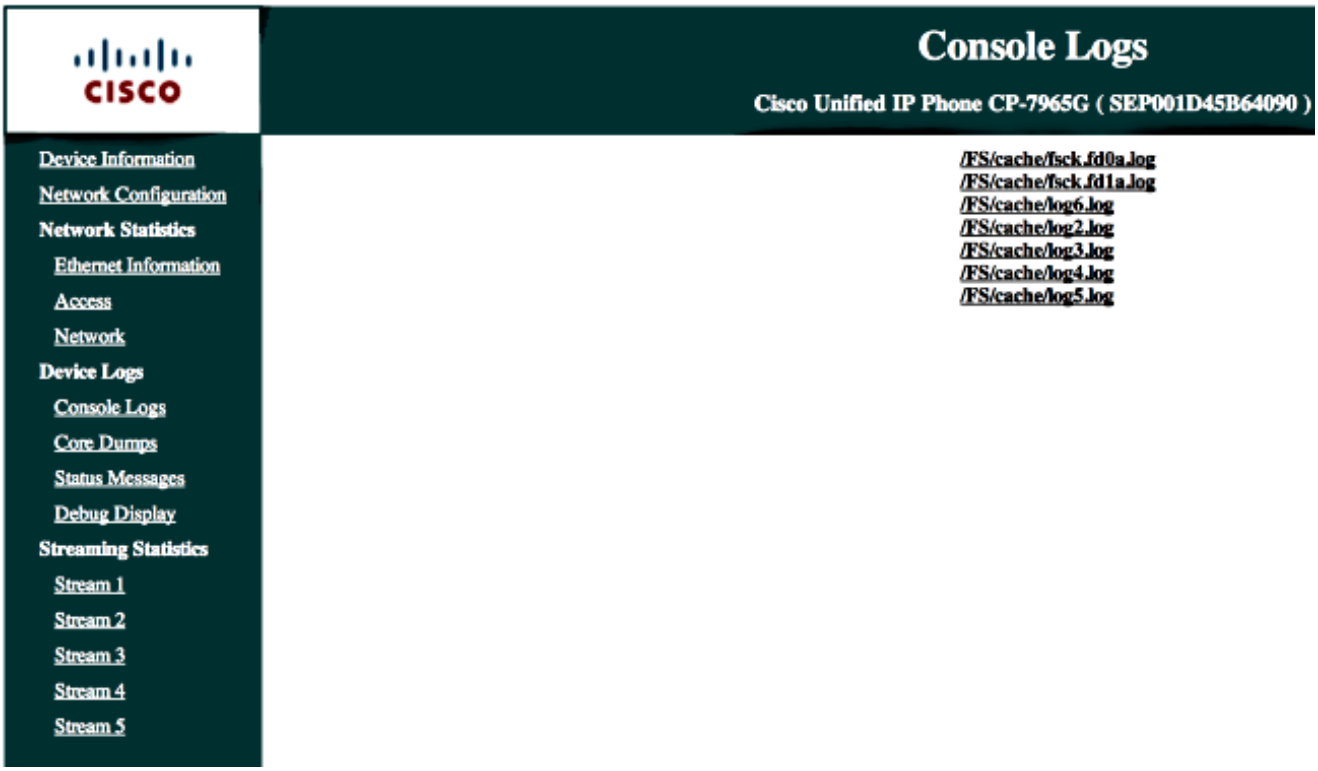
```
Router#show debug

WebVPN Subsystem:
WebVPN (verbose) debugging is on
WebVPN HTTP debugging is on
WebVPN AAA debugging is on
WebVPN tunnel debugging is on
WebVPN Tunnel Events debugging is on
WebVPN Tunnel Errors debugging is on
Webvpn Tunnel Packets debugging is on


PKI:
Crypto PKI Msg debugging is on
Crypto PKI Trans debugging is on
Crypto PKI Validation Path debugging is on
```

Depuraciones del teléfono

1. Navegue al **Device (Dispositivo) > Phone (Teléfono) de** CUCM.
2. En la página de la configuración del dispositivo, fije el Acceso Web a **activado**.
3. Haga clic la **salvaguardia**, y después haga clic **aplican los Config**.



4. De un hojeador, ingrese el IP address del teléfono, y elija los **registros de la consola del** menú a la izquierda.



5. Descargue todos los ficheros del ***.log de /FS/cache/log**. Los archivos del registro de la consola contienen la información sobre porqué el teléfono no puede conectar con el VPN.

Bug relacionados

ID de bug CSCty46387 de Cisco, IOS SSLVPN: Mejora para hacer que un contexto sea un valor por defecto
ID de bug CSCty46436 de Cisco, IOS SSLVPN: Mejora al comportamiento de la validación del certificado del cliente