Configure Secure Sockets Layer Virtual Private Network (SSL VPN) en el router RV340 o RV345

Aviso especial: Estructura de la autorización - Versiones de firmware 1.0.3.15 y más adelante. Moviéndose adelante, AnyConnect incurrirá en una carga para las licencias del cliente solamente.

Para más información sobre AnyConnect que autoriza en el Routers de las RV340 Series, controle hacia fuera el artículo AnyConnect autorizando para saber si hay el Routers de las RV340 Series.

Objetivo

El gateway de Secure Sockets Layer Virtual Private Network (SSL VPN) permite que los usuarios remotos establezcan un túnel del VPN seguro usando un buscador Web. Esta característica permite de fácil acceso a una amplia gama de recursos Web y de aplicaciones red-activadas usando el Hypertext Transfer Protocol (HTTP) nativo sobre la ayuda segura del navegador del Protocolo de transporte de hipertexto SSL (HTTPS).

El SSL VPN permite que los usuarios tengan acceso remotamente a las redes restrictas, usando un camino seguro y autenticado cifrando el tráfico de la red.

El Routers RV340 y RV345 apoya al Cliente Cisco AnyConnect VPN, o también conocido como cliente seguro de la movilidad de Anyconnect. Este Routers utiliza dos túneles SSL VPN por abandono, y el usuario puede registrar una licencia de utilizar hasta 50 túneles. Una vez que está instalado y activado, el SSL VPN establece un seguro, túnel del VPN de acceso remoto.

Este artículo apunta mostrarle cómo configurar SSL VPN en el RV340 o el router RV345.

Dispositivos aplicables

- RV340
- RV345
- Cliente seguro de la movilidad de Cisco

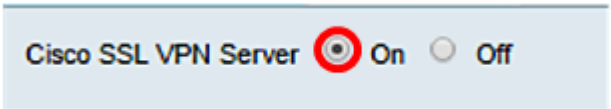
Versión de software

- 1.0.03.15 — RV340, RV345
- 4.4.01054 — Cliente seguro de la movilidad de AnyConnect

Configure SSL VPN

Paso 1. Tenga acceso a la utilidad en Internet del router y elija **VPN > SSL VPN**.

Paso 2. Haga clic **encendido el** botón de radio para activar al servidor VPN de Cisco SSL.

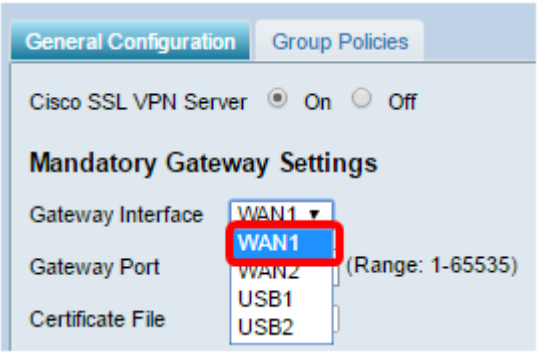


Configuraciones obligatorias del gateway

Las configuraciones siguientes son obligatorias:

Paso 3. Elija el interfaz del gateway de la lista desplegable. Éste será el puerto que será utilizado para pasar el tráfico a través de los túneles SSL VPN. Las opciones son:

- WAN1
- WAN2
- USB1
- USB2

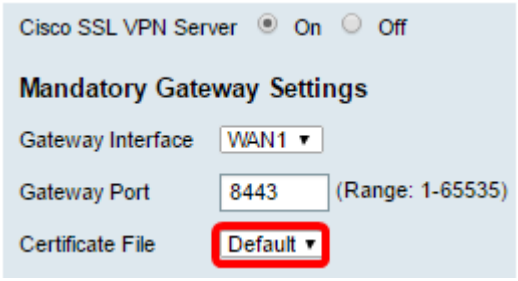


Nota: En este ejemplo, se elige el WAN1.

Paso 4. Ingrese el número del puerto que se utiliza para el gateway de VPN SSL en el campo de *puerto de gateway* que se extiende a partir de la 1 a 65535.

Nota: En este ejemplo, 8443 se utiliza como el número del puerto.

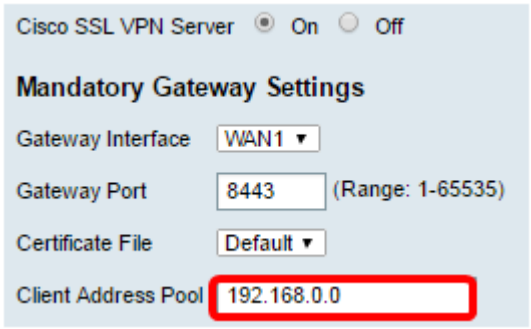
Paso 5. Elija el archivo de certificado de la lista desplegable. Este certificado autentica a los usuarios que intentan tener acceso al recurso de red a través de los túneles SSL VPN. La lista desplegable contiene un certificado del valor por defecto y los Certificados se importen que.



Nota: En este ejemplo, se elige el valor por defecto.

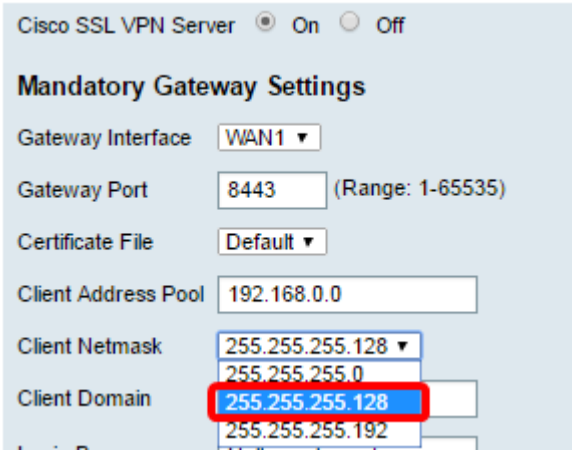
Paso 6. Ingrese el IP address del pool de la dirección cliente en el campo del *pool de la dirección cliente*. Este pool será el rango de los IP Addresses que será afectado un aparato a los clientes remotos VPN.

Nota: Asegúrese de que el rango de dirección IP no solape con los IP Addresses uces de los en la red local.



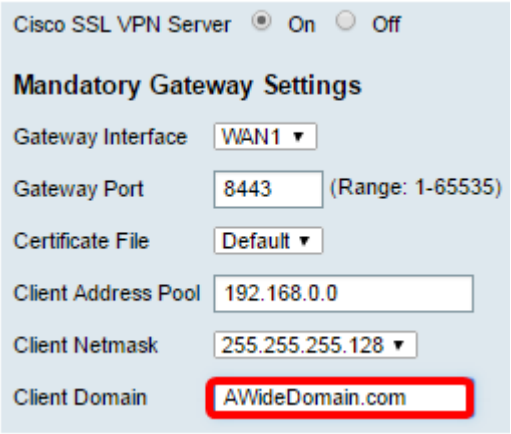
Nota: En este ejemplo, se utiliza 192.168.0.0.

Paso 7. Elija la máscara de red del cliente de la lista desplegable.



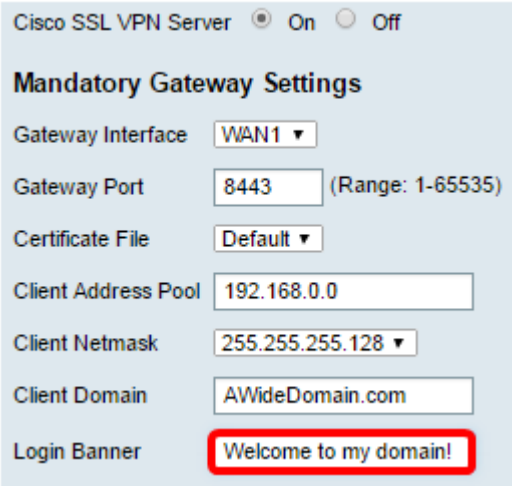
Nota: En este ejemplo, se elige 255.255.255.128.

Paso 8. Ingrese el Domain Name del cliente en el campo del *dominio del cliente*. Éste será el Domain Name que se debe empujar a los clientes SSL VPN.



Nota: En este ejemplo, AWideDomain se utiliza como el Domain Name del cliente.

Paso 9. Ingrese el texto que aparecería como anuncio de inicio de sesión en el campo del *anuncio de inicio de sesión*. Éste será el banner que será visualizado cada vez un cliente abre una sesión.



Nota: ¡En este ejemplo, recepción a mi dominio! se utiliza como el anuncio de inicio de sesión.

Configuraciones opcionales del gateway

Las configuraciones siguientes son opcionales:

Paso 1. Ingrese un valor en los segundos para el descanso ocioso que se extiende a partir del 60 a 86400. Ésta será la duración del tiempo que la sesión de VPN SSL puede seguir siendo ociosa.

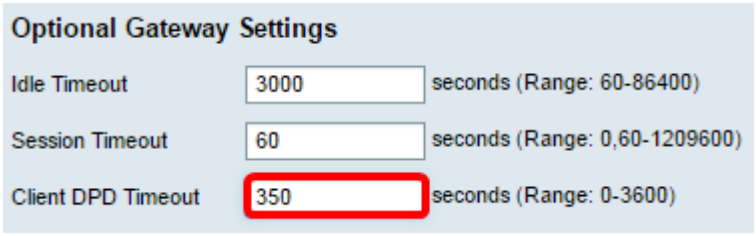
Nota: En este ejemplo, se utiliza 3000.

Paso 2. Ingrese un valor en los segundos en el campo del *tiempo de espera de la sesión*. Éste es el tiempo que toma para que la sesión del Transmission Control Protocol (TCP) o del User Datagram Protocol (UDP) mida el tiempo hacia fuera después del tiempo de inactividad especificado. El rango es a partir el 60 a 1209600.

Nota: En este ejemplo, se utiliza 60.

Paso 3. Ingrese un valor en los segundos en el campo del *descanso de ClientDPD* que se extiende a partir de la 0 a 3600. Este valor especifica el envío periódico de los mensajes HELLO/ACK para controlar el estatus del túnel VPN.

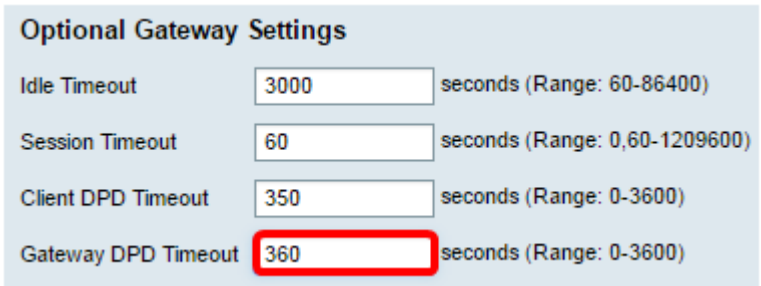
Nota: Esta característica se debe activar en los ambos extremos del túnel VPN.



Nota: En este ejemplo, se utiliza 350.

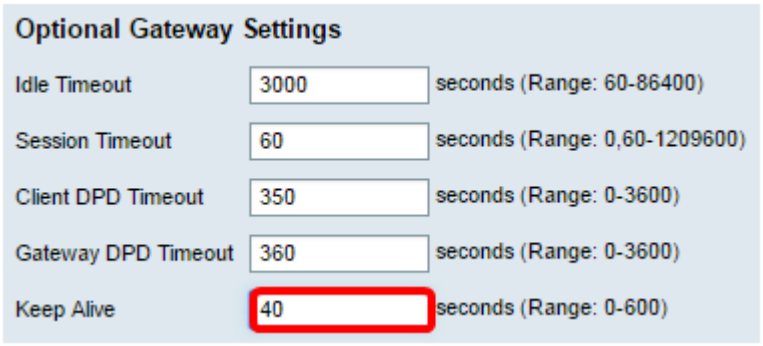
Paso 4. Ingrese un valor en los segundos en el campo del *descanso de GatewayDPD* que se extiende a partir de la 0 a 3600. Este valor especifica el envío periódico de los mensajes HELLO/ACK para controlar el estatus del túnel VPN.

Nota: Esta característica se debe activar en los ambos extremos del túnel VPN.



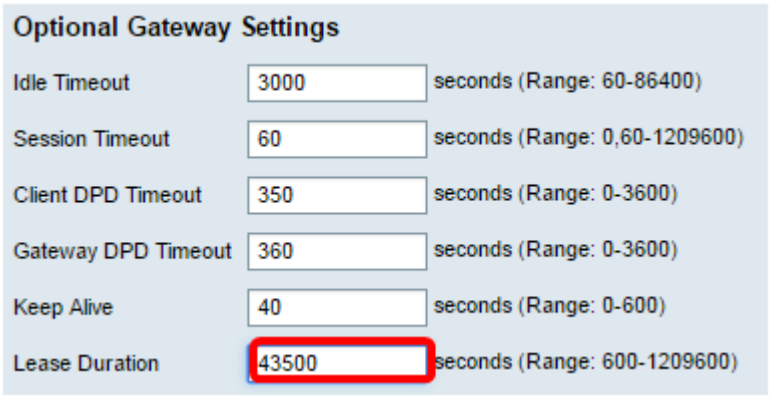
Nota: En este ejemplo, se utiliza 360.

Paso 5. Ingrese un valor en los segundos en el campo de la *señal de mantenimiento* que se extiende a partir de la 0 a 600. Esta característica se asegura de que su router esté conectado siempre con Internet. Intentará restablecer la conexión VPN si se cae.



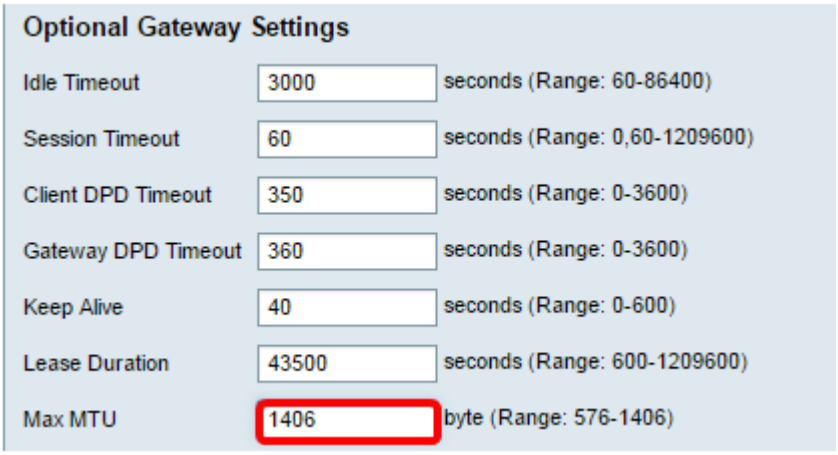
Nota: En este ejemplo, se utiliza 40.

Paso 6. Ingrese un valor en los segundos para la duración del túnel que se conectará en el campo del *tiempo de validez*. El rango es a partir el 600 a 1209600.



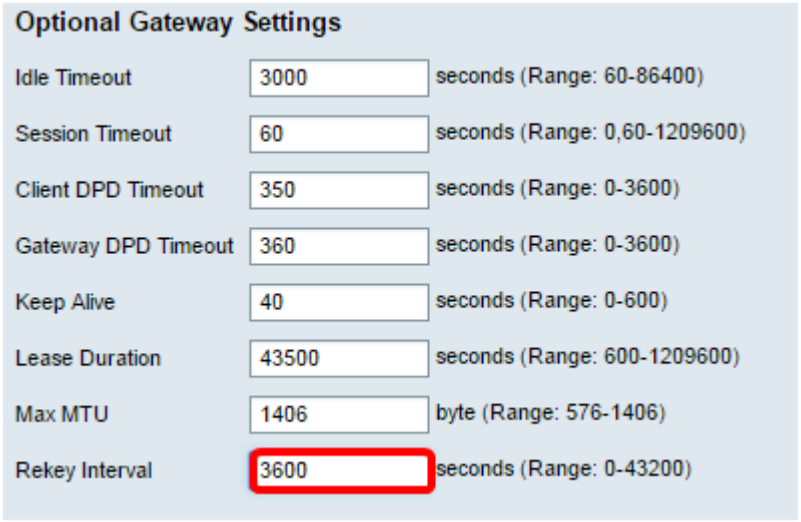
Nota: En este ejemplo, se utiliza 43500.

Paso 7. Ingrese el tamaño de paquetes en los bytes que se pueden enviar sobre la red. El rango es de es a partir el 576 a 1406.



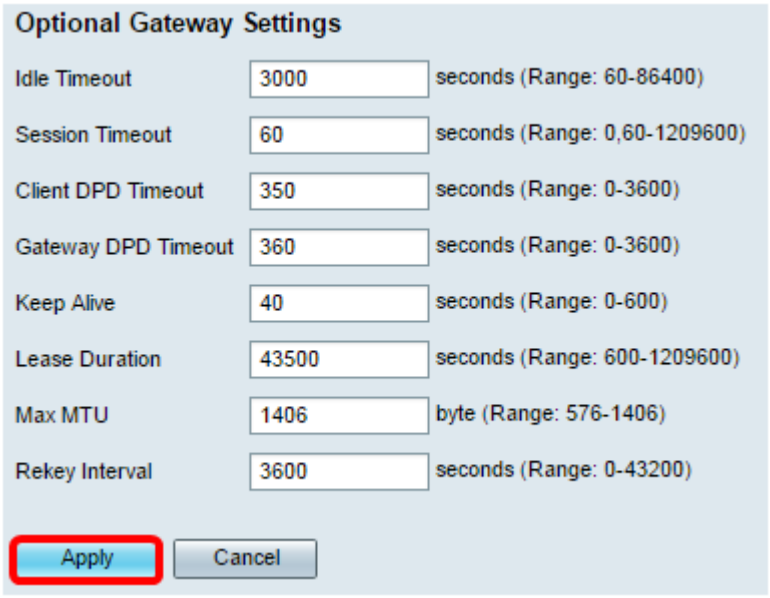
Nota: En este ejemplo, se utiliza 1406.

Paso 8. Ingrese la duración del intervalo del relevo en el campo del *intervalo de la reintroducción*. La característica de la reintroducción permite que las claves SSL renegocien después de que se haya establecido la sesión. El rango es a partir la 0 a 43200.



Nota: En este ejemplo, se utiliza 3600.

Paso 9. El tecleo **se aplica**.



El paso 10. (opcional) para salvar permanentemente la configuración, hace clic en el icono 

del centelleo.

Usted debe ahora haber configurado con éxito SSL VPN en su router RV34x.