GUÍA DE ADMINISTRACIÓN

Cisco RV215W Wireless-N VPN Firewall

Revisado en noviembre de 2013

78-20779-02

Contenido

1

Introducción

En este capítulo se proporciona información para ayudarlo con el proceso de instalación y para que comience a utilizar el Administrador de - dispositivos basado en el navegador.

- **Verificación de la instalación del hardware**
- **Uso del Asistente de instalación**
- **Cómo usar la página Introducción**
- **Cómo conectarse a la red inalámbrica**

Verificación de la instalación del hardware

Configure el dispositivo para conectarse a las redes alámbricas e inalámbricas mediante la Guía de inicio rápido de Cisco RV215W Wireless-N VPN Firewall.

PRECAUCIÓN Utilice la fuente de energía de 12 V, 1,67 a que vino con el dispositivo. Si usa alguna otra fuente de energía, esto podría causar daños o un bajo rendimiento del dispositivo.

Para verificar la instalación del hardware y la conexión a Internet, realice las siguientes tareas:

PASO 1 Compruebe los estados de los indicadores LED. Para obtener más información, consulte la Guía de inicio rápido de Cisco RV215W Wireless-N VPN Firewall que viene con el dispositivo.

PASO 2 Conecte una computadora a un puerto LAN disponible y verifique que se pueda conectar a un sitio web en Internet, como www.cisco.com.

PASO 3 En una PC con función inalámbrica, conéctese a un sitio web en Internet, como www.cisco.com. Para configurar su radio, consulte **Cómo conectarse a la red inalámbrica**.

Uso del Asistente de instalación

El Asistente de instalación y el Administrador de dispositivos son compatibles con Microsoft Internet Explorer 6.0 o posterior, Mozilla Firefox 3.0 o posterior y Apple Safari 3.0 o posterior.

Para usar el Asistente de instalación:

PASO 1 Inicie la computadora que conectó al puerto LAN.

La computadora se convierte en un cliente DHCP del dispositivo y recibe una dirección IP en el rango 192.168.1.xxx.

PASO 2 Inicie un explorador web e introduzca **192.168.1.1** en la barra de direcciones. Esta es la dirección IP predeterminada del dispositivo.

Aparece un mensaje sobre el certificado de seguridad del sitio. El dispositivo utiliza un certificado de seguridad con firma automática y este mensaje aparece porque su computadora no conoce el dispositivo.

PASO 3 Haga clic en **Continuar a este sitio web** (o bien la opción que se muestra en su explorador web particular) para ir al sitio web. Aparece la página de inicio de sesión.

PASO 4 Ingrese el nombre de usuario y la contraseña.

El nombre de usuario predeterminado es **cisco**. La contraseña predeterminada es **cisco**. Las contraseñas distinguen mayúsculas y minúsculas.

PASO 5 Haga clic en **Iniciar sesión**. Se inicia el Asistente de instalación.

PASO 6 Siga las instrucciones que aparecen en la pantalla para configurar el dispositivo.

El Asistente de instalación intenta detectar y configurar automáticamente su conexión. Si no puede hacerlo, el Asistente de instalación puede pedirle la información sobre su conexión de Internet. Tal vez deba comunicarse con su proveedor de servicios de Internet (ISP) para obtener esa información.

Después de que el Asistente de instalación finaliza con la configuración del dispositivo, tiene que cambiar la contraseña predeterminada. Siga las instrucciones que aparecen en la pantalla. Después de cambiar la contraseña predeterminada, aparece la página **Introducción**.

Configuración de pasos siguientes

Si bien el Asistente de instalación configura automáticamente el dispositivo, le recomendamos que personalice algunos valores para brindar una mayor seguridad y un mejor rendimiento.

- Si ya tiene un servidor DHCP en la red y no desea que el dispositivo actúe como una red DHCP, desactive el servidor. Consulte **Configuración de opciones LAN**.
- Configure la red privada virtual (VPN) mediante QuickVPN. QuickVPN está incluido en el CD que se le envío con el firewall. Consulte **Ap?dice A, ?$paratext>.?Default Para Font>**.
- El dispositivo admite hasta cuatro redes inalámbricas. Solo puede configurar una red inalámbrica (o SSID) con el Asistente de instalación. Para configurar redes inalámbricas adicionales mediante el Administrador de dispositivos, consulte **Configuración de la red inalámbrica**.

Cómo usar la página Introducción

En la página **Introducción**, se muestran las tareas de configuración de dispositivo más comunes. Utilice los enlaces que aparecen en esta página para saltar a la página de configuración relevante.

Esta página aparecerá cada vez que inicie el Administrador de dispositivos. Para modificar esta opción, marque la opción **No mostrar al inicio**.

Configuración inicial

Cambiar contraseña de admin. predeterminada	Muestra la página **Usuarios**, donde puede modificar la contraseña de administrador y configurar una cuenta de invitado. Consulte **Configuración de cuentas de usuario**.
Iniciar Asistente de instalación	Inicia el Asistente de instalación. Siga las instrucciones que aparecen en la pantalla.

Configurar opciones WAN	Abre la página **Configuración de Internet** para cambiar los parámetros, como por ejemplo, el nombre de host para el router. Consulte **Configuración de las opciones WAN**.
Configure LAN Settings	Abre la página **LAN Configuration** para modificar los parámetros LAN, como por ejemplo, la dirección IP de administración. Consulte **Configuración de opciones LAN**.
Configurar opciones inalámbricas	Abre la página **Configuración básica** para administrar la radio. Consulte **Configuración de la red inalámbrica**.

Acceso rápido

Actualizar firmware del router	Abre la página **Actualización del firmware/idioma** para actualizar el firmware del router o el paquete de idioma. Consulte **Actualización del firmware o cambio de idioma**.
Agregar clientes VPN	Abre la página **Clientes VPN** para administrar redes virtuales privadas. Consulte **Clientes VPN**.
Configurar acceso a admin. remota	Abre la página **Configuración básica** para activar las funciones básicas del router. Consulte **Configuración de los parámetros básicos de firewall**.

Estado del dispositivo

Resumen del sistema	Muestra la página **Resumen del sistema**, la cual muestra el estado del router. Consulte **Visualización del resumen del sistema**.
Wireless Status	Muestra la página **Estadísticas inalámbricas**, la cual muestra el estado de la radio. Consulte **Visualización de estadísticas inalámbricas**.
Estado VPN	Muestra la página **Estado de VPN**, que proporciona una lista de las VPN administradas por este router. Consulte **Visualización del estado VPN**.

Otros recursos

Asistencia técnica	Haga clic en este vínculo para abrir la página de asistencia técnica de Cisco.
Foros	Haga clic en este vínculo para visitar los foros de asistencia técnica en línea de Cisco.

Guardar cambios

Cuando termine de realizar los cambios en una página de configuración, haga clic en **Save** (Guardar) para guardar los cambios en la memoria Flash o haga clic en **Cancel** (Cancelar) para deshacer los cambios.

Cómo conectarse a la red inalámbrica

Para conectar un dispositivo cliente (por ejemplo, una computadora) a la red inalámbrica, configure la conexión inalámbrica en el dispositivo con la información de seguridad inalámbrica que configuró para su dispositivo mediante el Asistente de instalación.

Los siguientes pasos se brindan como ejemplo; es posible que deba configurar el dispositivo cliente de manera diferente. Para obtener las instrucciones que son específicas del dispositivo cliente, consulte la documentación del dispositivo.

PASO 1 Abra la ventana o programa de configuración de conexiones inalámbricas del dispositivo.

Es posible que la computadora tenga instalado un software especial para administrar conexiones inalámbricas, o puede encontrar conexiones inalámbricas en el Panel de control en la ventana **Conexiones de red** o **Red e Internet**. (La ubicación depende del sistema operativo).

PASO 2 Escriba el nombre de la red (SSID) que eligió para su red en el Asistente de instalación.

PASO 3 Elija el tipo de cifrado y escriba la clave de seguridad que especificó en el Asistente de instalación.

Si no habilitó la seguridad (lo que no es recomendable), deje los campos de cifrado inalámbrico que se configuraron con el tipo de seguridad y la frase clave en blanco.

PASO 4 Verifique la conexión inalámbrica y guarde la configuración.

2

Visualización del estado del dispositivo

En este capítulo, se describe cómo ver estadísticas en tiempo real y otros datos sobre el dispositivo.

Visualización del panel de comando

La página **Panel de comando** brinda información importante sobre el router.

Para ver el Panel de comando, seleccione **Status** (Estado) > **Dashboard (Panel de comando)**.

Para modificar la velocidad de actualización de las estadísticas y los valores de parámetros que se muestran, seleccione la frecuencia desde el menú desplegable **Velocidad de actualización**.

Para obtener una vista interactiva del panel posterior del router, haga clic en **Mostrar vista de panel**.

La vista del panel posterior le muestra los puertos que están conectados a un dispositivo (en color verde).

- Para ver la información de conexión de un puerto, pase el mouse por el puerto.
- Para actualizar la información del puerto, haga clic en **Actualizar**.
- Para cerrar la hoja de información de la ventana, haga clic en **Cerrar**.

La página **Panel de comando** muestra lo siguiente:

Información del dispositivo

- **Nombre del sistema:** el nombre del dispositivo.
- **Versión del firmware:** la versión del firmware que ejecuta el dispositivo actualmente.
- **Número de serie:** el número de serie del dispositivo.

Uso de recursos

- **CPU:** uso de la CPU.
- **Memoria:** uso de la memoria.
- **Hora actual:** la hora del día.
- **Tiempo de act. del sist:** el tiempo de ejecución del sistema.

Resumen de Syslog

Indica si la función de registro está habilitada para estas categorías de eventos:

- **Emergencia**
- **Alerta**
- **Crítico**
- **Error**
- **Advertencia**

Para ver los registros, haga clic en **detalles**. Para obtener más información, consulte **Visualización de registros**.

Para administrar registros, haga clic en **administrar registro**. Para obtener más información, consulte **Configuración de los valores de registro**.

Interfaz LAN (red local)

- **Dirección MAC:** la dirección MAC del dispositivo.
- **Dirección IPv4:** la dirección IP de administración del dispositivo.
- **Dirección IPv6:** la dirección IP de administración del dispositivo (si se habilita IPv6).
- **Servidor DHCP:** estado del servidor DHCP para IPv4 del dispositivo (habilitado o deshabilitado).

- **Servidor DHCPv6:** estado del servidor DHCP para IPv6 del router (habilitado o deshabilitado).

Para ver la configuración de LAN, haga clic en **detalles**. Para obtener más información, consulte **Configuración de opciones LAN**.

Información sobre WAN (Red móvil)

- **Dirección IPv4:** la dirección IPv4 del puerto USB.
- **Estado:** el estado de la conexión a la red móvil WAN (activa o inactiva).

Para ver la configuración de WAN, haga clic en detalles. Para obtener más información, consulte **Configuración de conexiones WAN alámbricas**.

Información de WAN (Internet)

- **Dirección IPv4:** la dirección IPv4 del puerto WAN del router.
- **Dirección IPv6:** la dirección IPv6 del puerto WAN del router, si se habilita IPv6.
- **Estado:** el estado de la conexión a la red alámbrica WAN (activa o inactiva).

Para ver la configuración de WAN, haga clic en **detalles**. Para obtener más información, consulte **Configuración de conexiones WAN alámbricas**.

Redes inalámbricas

Se incluye el estado de los cuatro SSID de las redes inalámbricas.

Para ver la configuración inalámbrica del router, haga clic en **detalles**. Para obtener más información, consulte **Visualización de estadísticas inalámbricas**.

VPN

Usuarios QuickVPN: la cantidad de usuarios QuickVPN.

PPTP: la cantidad de usuarios de Protocolo de tunelización punto a punto (PPTP).

Visualización del resumen del sistema

La página **Resumen del sistema** muestra un resumen de los valores del dispositivo, como ser la versión de firmware y el número de serie.

Para ver un resumen de los valores del sistema, seleccione **Estado** > **Resumen del sistema**

Para ir a la ventana relacionada, haga clic sobre el parámetro subrayado. Por ejemplo, para modificar la dirección IP de LAN, haga clic en **LAN IP**. Aparece la ventana de configuración de LAN.

Haga clic en **Actualizar** para obtener la información más actualizada.

La página **Resumen del sistema** muestra la siguiente información:

Información del sistema

- **Versión del firmware:** la versión actual del software que ejecuta el dispositivo.
- **Suma de comprobación MD5 de Firmware:** el algoritmo del resumen de mensaje utilizado para verificar la integridad de los archivos.
- **Configuración regional:** el idioma instalado en el router.
- **Versión del idioma**: la versión del paquete de idiomas instalado. La versión del paquete de idiomas debe ser compatible con el firmware actualmente instalado. En algunos casos, se puede usar un paquete de idiomas anterior con una nueva imagen de firmware. El router verifica la versión del paquete de idiomas para ver si es compatible con la versión de firmware actual.
- **Suma de comprobación de idioma MD5**: suma de comprobación MD5 del paquete de idiomas.
- **Modelo CPU:** conjunto de chips de la CPU utilizada actualmente.
- **Número de serie:** el número de serie del dispositivo.
- **Tiempo de act. del sist:** el tiempo de ejecución del sistema.
- **Hora actual:** la hora del día.
- **PID VID:** el Id. del producto y el Id. de la versión del dispositivo.

Configuración IPv4

- **IP de LAN:** la dirección IP de LAN del dispositivo.
- **IP de WAN:** la dirección IP de WAN del dispositivo. Para liberar la dirección IP actual y obtener una nueva, haga clic en **Liberar** o **Renovar**.
- **Puerta de enlace**: dirección IP de la puerta de enlace a la que el dispositivo está conectado (por ejemplo, el módem alámbrico).
- **Modo:** se muestra **Puerta de enlace**, si NAT está habilitada, o **Router**.
- **DNS 1:** dirección IP del servidor DNS primario del puerto WAN.
- **DNS 2:** dirección IP del servidor DNS secundario del puerto WAN.
- **DDNS:** indica si el DNS dinámico está habilitado o deshabilitado.

Configuración IPv6

- **IP de LAN:** la dirección IP de LAN del dispositivo.
- **IP de WAN:** la dirección IP de WAN del dispositivo.
- **Puerta de enlace**: dirección IP de la puerta de enlace a la que el dispositivo está conectado (por ejemplo, el módem alámbrico).
- **NTP**: servidor del Protocolo de hora en la red (nombre de host o dirección IPv6).
- **Delegación de prefijo**: el prefijo IPv6 obtenido desde el dispositivo al ISP que se le otorga a las direcciones IP en el dispositivo.
- **DNS 1:** la dirección IP del servidor DNS primario.
- **DNS 2:** la dirección IP del servidor DNS secundario.

Resumen inalámbrico

- **SSID 1:** el nombre público de la primera red inalámbrica.
  - **Seguridad:** la configuración de seguridad para SSID 1.
- **SSID 2:** el nombre público de la segunda red inalámbrica.
  - **Seguridad:** la configuración de seguridad para SSID 2.
- **SSID 3:** el nombre público de la tercera red inalámbrica.
  - **Seguridad:** la configuración de seguridad para SSID 3.
- **SSID 4:** el nombre público de la cuarta red inalámbrica.
  - **Seguridad:** la configuración de seguridad para SSID 4.

Estado de configuración de firewall

- **Dos (denegación de servicio):** indica si la prevención de DoS está activada o desactivada.
- **Solicitud WAN de bloqueo**: indica si el bloqueo de la solicitud WAN está activado o desactivado.
- **Administración remota:** indica si se puede acceder de manera remota a Administrador de dispositivos.

Estado de configuración de VPN

- **Conexiones QuickVPN disponibles:** cantidad de conexiones QuickVPN disponibles.

- **Conexiones VPN PPTP disponibles:** cantidad de conexiones VPN PPTP disponibles.
- **Usuarios QuickVPN conectados:** cantidad de usuarios QuickVPN conectados.
- **Usuarios PPTP VPN conectados:** cantidad de usuarios PPTP VPN conectados.

Visualización de estadísticas inalámbricas

La página **Estadísticas inalámbricas** muestra las estadísticas inalámbricas para el radio del dispositivo.

Para ver las estadísticas, seleccione **Estado** > **Estadísticas inalámbricas**.

Para modificar la velocidad de actualización, escoja una velocidad de actualización del menú desplegable **Velocidad de actualización**.

Para mostrar los bytes en kilobytes (KB) y los datos numéricos en valores redondeados, marque **Show Simplified Statistic Data** (Mostrar datos estadísticos simplificados) y haga clic en **Save** (Guardar). De manera predeterminada, los datos de bytes se muestran en bytes y otros datos numéricos se muestran en versión larga.

Para restablecer los contadores de estadísticas inalámbricas, haga clic en **Borrar conteo**. Además, los contadores se restablecen cuando se reinicia el dispositivo.

La página **Estadísticas inalámbricas** muestra la siguiente información:

Nombre de SSID	Nombre de la red inalámbrica.
Paquete	Cantidad de paquetes inalámbricos recibidos y enviados informados al radio en todos los SSID configurados y activos.
Byte	Cantidad de bytes de información recibidos y enviados informados al radio en todos los SSID configurados.
Error	Cantidad de errores de paquetes recibidos y enviados informados a la radio en todos los SSID configurados.
Suprimidos	Cantidad de paquetes recibidos y enviados suprimidos por el radio en todos los SSID configurados.
Multidifusión	Cantidad de paquetes de multidifusión enviados por este radio.
Colisiones	Cantidad de colisiones de paquetes informadas al router.

Visualización del estado VPN

La página **VPN** muestra el estado de las conexiones VPN.

Para ver el estado de conexión del usuario VPN, elija **Estado** > **Estado VPN**.

La página **VPN** muestra la siguiente información:

Nombre de usuario	Nombre de usuario del usuario VPN asociado con el túnel QuickVPN PPTP.
IP remota	Se muestra la dirección IP del cliente QuickVPN remoto. Puede ser una dirección IP NAT/pública si el cliente se encuentra detrás del router NAT.
Estado	Se muestra el estado actual del cliente QuickVPN. OFFLINE (Desconectado) significa que el usuario VPN no ha iniciado ni establecido el túnel QuickVPN. ONLINE (En línea) significa que el túnel QuickVPN, iniciado o establecido por el usuario VPN, se encuentra activo.
Hora de inicio	Hora en que el usuario VPN estableció una conexión.
Hora de finalización	Hora en que el usuario VPN finalizó una conexión.
Duración (segundos)	Tiempo transcurrido entre el establecimiento y la finalización de una conexión por parte del usuario VPN.
Protocolo	Protocolo que usa el usuario.

Usted puede cambiar el estado de una conexión para establecer o desconectar el cliente VPN configurado.

Para finalizar una conexión VPN activa, haga clic en **Desconectar**.

Visualización del estado de la conexión IPSec

El estado de la conexión IPsec muestra el estado de las políticas VPN activas del dispositivo. (Estas políticas se configuran en la página **VPN** > **Configuración de VPN avanzada**). Para ver el estado de la conexión IPsec:

PASO 1 Elija **Estado** > **Estado de la conexión IPSec**. En la tabla, se muestra la siguiente información:

- **Velocidad de actualización**: seleccione la velocidad con la cual desea que se borre la pantalla de datos y que aparezcan los datos más nuevos.
- **Mostrar datos estadísticos simplificados**: de manera predeterminada, los datos de bytes se muestran en bytes y otros datos numéricos se muestran en versión larga. Para mostrar los bytes en kilobytes (KB) y los datos numéricos en forma redondeada, marque **Show Simplified Statistic Data** (Mostrar datos estadísticos simplificados).
- **Nombre de la política**: nombre de la política VPN cuyos datos se muestran.
- **Local o Remota:** muestra las direcciones IP local y remota.
- **Start Time and End Time** (Hora de inicio y hora de finalización): muestra las horas de inicio y finalización de las conexiones IPsec.
- **Duración**: muestra el tiempo transcurrido durante el cual la conexión estuvo activa.
- **Paquete**: muestra los paquetes recibidos (Rx) y transmitidos (Tx) en la conexión.
- **Byte**: muestra los bytes recibidos (Rx) y transmitidos (Tx) en la conexión.
- **Estado**: muestra el estado de la conexión (por ejemplo, activo o no conectado).
- **Acción**: muestra las acciones que puede realizar en la conexión (por ejemplo, desconectar).
- **Ext Action** (Acción ext.): muestra si puede conmutar entre las conexiones VPN primaria y secundaria. Si está marcada la casilla de verificación **Rollback enable** (Habilitar reversión) en la página **Advanced VPN Parameters** (Parámetros VPN avanzados), el botón **Switch** (Conmutar) está atenuado.

PASO 2 Si realizó algún cambio, haga clic en **Guardar**.

Visualización de registros

La página **Visualización de registros** muestra los registros de dispositivo.

Para ver los registros, seleccione **Estado** > **Visualización de registros**.

Haga clic en **Actualizar registros** para visualizar las últimas entradas de registro.

Para filtrar registros, o especificar la gravedad de los registros para mostrar, marque las casillas que están junto al tipo de registro y haga clic en **Ir**. Tenga en cuenta que todos los tipos de registro que están arriba de un tipo de registro seleccionado se incluyen automáticamente y no puede desactivarlos. Por ejemplo, al seleccionar registros de errores, se incluyen automáticamente los registros de emergencia, alerta y críticos, además de los registros de errores.

Los niveles de gravedad de los eventos se detallan de mayor gravedad a menor gravedad, de la siguiente manera:

- **Emergencia**: el sistema no se puede utilizar.
- **Alerta**: se necesita acción.
- **Crítico**: el sistema está en condición crítica.
- **Error**: el sistema está en condición de error.
- **Advertencia**: se presentó una advertencia del sistema.
- **Notificación**: el sistema está funcionando correctamente, pero se presentó un aviso del sistema.
- **Informativo**: información de dispositivos.
- **Depuración**: proporciona información detallada acerca de un evento.

Para eliminar todas las entradas en la ventana de registros, haga clic en **Borrar registros**.

Para guardar todos los mensajes de registro del firewall en el disco duro local, haga clic en **Guardar registros**.

Para guardar mensajes de registro en un dispositivo USB externo, haga clic en **Save Log to USB** (Guardar registro en USB).

Para especificar la cantidad de entradas que se debe mostrar por página, elija un número en el menú desplegable.

Utilice los botones de navegación de la página para desplazarse por páginas de registro.

Visualización de dispositivos conectados

La página **Dispositivos conectados** muestra información sobre los dispositivos activos conectados al dispositivo.

En la Tabla ARP IPv4, se muestra la información de los dispositivos que han respondido a la solicitud del Protocolo de resolución de direcciones (ARP, Address Resolution Protocol) del dispositivo. Si un dispositivo no responde a la solicitud, se elimina de la lista.

En la Tabla NDP IPv6, se muestran todos los dispositivos de Protocolo de detección de vecinos (NDP, Neighbor Discover Protocol) IPv6 conectados al enlace local del dispositivo.

Para ver los dispositivos conectados, seleccione **Estado** > **Dispositivos conectados**.

Para especificar los tipos de interfaz que desea visualizar, elija un valor en el menú desplegable **Filtro**:

Todos: todos los dispositivos conectados al router.

Inalámbricos: todos los dispositivos conectados mediante la interfaz inalámbrica.

Conectados: todos los dispositivos conectados al router a través de los puertos Ethernet.

WDS: todos los dispositivos con Sistema de distribución inalámbrica (WDS) conectados al router.

Visualización de estadísticas del puerto

La página **Estadísticas del puerto** muestra la actividad detallada del puerto.

Para ver las estadísticas, seleccione **Estado** > **Estadísticas del puerto**.

Para que la página vuelva a leer las estadísticas del router y poder actualizar la página, elija una velocidad de actualización en el menú desplegable **Velocidad de actualización**.

Para mostrar los bytes en kilobytes (KB) y los datos numéricos en forma redondeada, marque **Show Simplified Statistic Data** (Mostrar datos estadísticos simplificados) y haga clic en **Save** (Guardar). De manera predeterminada, los datos de bytes se muestran en bytes y otros datos numéricos se muestran en versión larga.

Para restablecer los contadores de estadísticas del puerto, haga clic en **Borrar conteo**.

La página **Estadísticas del puerto** muestra la siguiente información:

Interfaz	Nombre de la interfaz de red.
Paquete	Cantidad de paquetes recibidos/enviados.
Byte	Cantidad de bytes de información recibidos/enviados por segundo.
Error	Cantidad de errores de paquetes recibidos/enviados.
Suprimidos	Cantidad de paquetes recibidos/enviados que se suprimieron.
Multidifusión	Cantidad de paquetes de multidifusión enviados por este radio.
Colisiones	Cantidad de colisiones de señales que se produjeron en este puerto. Una colisión se produce cuando el puerto intenta enviar datos al mismo tiempo que un puerto en otro router u otra computadora conectado a este puerto.

Visualización del estado de la red de invitado

En las estadísticas de la red de invitado, se muestra información sobre la red de invitado inalámbrica configurada en el dispositivo.

Para ver el estado de la red de invitado, elija **Estado** > **Estado de red de invitado**. Aparece la siguiente información:

- **Nombre de host**: dispositivo conectado a la red de invitado.
- **Dirección IP**: la dirección IP asignada al dispositivo conectado.
- **Dirección MAC**: dirección MAC o dirección del hardware del dispositivo conectado.
- **Tiempo restante**: tiempo restante durante el cual el dispositivo puede conectarse a la red de invitado. (Estos límites se configuran en la página **Red inalámbrica** > **Configuración básica** > **Configuración de red de invitado**).
- **Acción**: muestra las acciones que puede realizar con el dispositivo conectado (por ejemplo, desconectar).

Visualización del estado de la red móvil

Las estadísticas de la red móvil sobre las redes 3G/4G y el dispositivo de configuración se configuran en el dispositivo.

Para ver el estado de la red móvil, elija **Estado** > **Red móvil**. Aparece la siguiente información:

- **Conexión**: dispositivo conectado a la red de invitado.
- **Dirección IP de Internet**: la dirección IP asignada al dispositivo USB.
- **Máscara de subred:** máscara de subred del dispositivo USB.
- **Puerta de enlace predeterminada:** dirección IP de la puerta de enlace predeterminada.
- **Tiempo de act. del conexión:** el tiempo de actividad.
- **Uso actual de la sesión:** volumen de datos que se reciben (Rx) y se transmiten (Tx) en el enlace móvil.
- **Nombre del fabricante**: nombre del fabricante de la tarjeta.
- **Modelo de tarjeta:** número del modelo de tarjeta.
- **Firmware de la tarjeta:** versión de firmware de la tarjeta.
- **Estado SIM**: estado del módulo de identificación del suscriptor (SIM)
- **IMS:** identificación única asociada con los usuarios de teléfonos móviles con redes GSM, UMTS o LTE.
- **Portadora:** portadora de la red móvil.
- **Tipo de servicio:** tipo de servicio al que se accede.
- **Intensidad de señal:** intensidad de la señal de la red móvil inalámbrica.

3

Configuración de red

En este capítulo, se describe cómo configurar las opciones de red del dispositivo.

- **Configuración de las opciones WAN**
- **Configuración de opciones LAN**
- **Clonación de la dirección MAC**
- **Configuración de enrutamiento**
- **Administración de puertos**
- **Configuración de DNS dinámico**
- **Configuración del modo IP**
- **Configuración IPv6**

Configuración de las opciones WAN

Se puede establecer una conexión a Internet mediante un puerto WAN o un módem inalámbrico instalados en el puerto USB. En esta sección se describe la configuración de WAN, la red móvil, y la recuperación tras fallas.

Configuración de conexiones WAN alámbricas

La configuración de las propiedades WAN para una red IPv4 difiere según el tipo de conexión a Internet que tenga.

Configuración de DHCP

Si su proveedor de servicios de Internet (ISP) usa el Protocolo de control de host dinámico (DHCP, Dynamic Host Control Protocol) para asignarle una dirección IP, usted recibe una dirección IP que se genera en forma dinámica cada vez que inicia sesión.

Para configurar las opciones WAN DHCP, siga estos pasos:

PASO 1 Seleccione **Redes** > **WAN**.

PASO 2 En el menú desplegable **Tipo de conexión a Internet**, seleccione **Configuración automática - DHCP**.

PASO 3 Haga clic en **Guardar**.

Configuración de IP estática

Si su ISP le asignó una dirección IP permanente, siga los pasos a continuación para configurar sus opciones WAN:

PASO 1 Seleccione **Redes** > **WAN**.

PASO 2 En el menú desplegable **Tipo de conexión a Internet**, seleccione **IP estática**.

PASO 3 Escriba esta información:

Dir. IP de Internet	Dirección IP del firewall del puerto WAN.
Máscara de subred	Máscara de subred del firewall del puerto WAN.

Puerta de enlace predet.	Dirección IP de la puerta de enlace predeterminada.
DNS estático 1	Dirección IP del servidor DNS primario.
DNS estático 2	Dirección IP del servidor DNS secundario.

PASO 4 Haga clic en **Guardar**.

Configuración de PPPoE

Para configurar los valores del protocolo punto a punto por Ethernet (PPPoE):

PASO 1 Seleccione **Redes** > **WAN**.

PASO 2 En el menú desplegable **Tipo de conexión a Internet**, seleccione **PPPoE**.

PASO 3 Escriba la siguiente información (quizá deba comunicarse con su ISP para obtener información de inicio de sesión de su PPPoE):

Nombre de usuario	El nombre de usuario asignado por el ISP.
Contraseña	La contraseña asignada por el ISP.
Conectar a petición	Seleccione esta opción si su ISP le cobra en función del tiempo que está conectado. Cuando selecciona esta opción, la conexión a Internet solo está activa si hay tráfico. Si no hay flujo de tráfico, la conexión está inactiva; es decir, está cerrada. Si hace clic en **Conectar a petición**, escriba los minutos que deben transcurrir para que se desactive la conexión en el campo **Tiempo máx. de inactividad**.
Mantener conexión	Cuando selecciona esta opción, la conexión a Internet está siempre activa. En el campo Período de repetición de marcación, escriba los segundos que deben transcurrir para que el dispositivo intente volver a conectarse una vez desconectado.

Tipo de autenticación	**Negociación automática**: el servidor envía una solicitud de configuración que especifica el algoritmo de seguridad establecido. Posteriormente, el dispositivo envía las credenciales de autenticación con el tipo de seguridad que envió el servidor. **PAP**: Protocolo de autenticación de contraseña (PAP); el protocolo de punto a punto lo utiliza para conectarse con el ISP. **CHAP**: Protocolo de confirmación de aceptación de la autenticación (CHAP) requiere que tanto el servidor como el cliente conozcan el texto simple de la clave para utilizar los servicios ISP. **MS-CHAP o MS-CHAPv2**: la versión de Microsoft de CHAP, utilizada para acceder a los servicios ISP.

PASO 4 Haga clic en **Guardar**.

Configuración de PPTP

Para configurar las opciones PPTP:

PASO 1 Seleccione **Redes** > **WAN**.

PASO 2 En el menú desplegable **Tipo de conexión a Internet**, seleccione **PPTP**.

PASO 3 Escriba esta información:

Dir. IP de Internet	Dirección IP del puerto WAN.
Máscara de subred	Máscara de subred del puerto WAN.
Puerta de enlace predet.	Dirección IP de la puerta de enlace predeterminada.
Servidor PPTP	Dirección IP del servidor del Protocolo de tunelización punto a punto (PPTP, Point-To-Point Tunneling Protocol).
Nombre de usuario	El nombre de usuario asignado a usted por el ISP.
Contraseña	La contraseña asignada a usted por el ISP.

Conectar a petición	Seleccione esta opción si su ISP le cobra en función del tiempo que está conectado. Cuando selecciona esta opción, la conexión a Internet solo está activa si hay tráfico. Si no hay flujo de tráfico, la conexión está inactiva; es decir, está cerrada. Si hace clic en **Conectar a petición**, escriba los minutos que deben transcurrir para que se desactive la conexión en el campo **Tiempo máx. de inactividad**.
Mantener conexión	Cuando selecciona esta opción, la conexión a Internet está siempre activa. En el campo Período de repetición de marcación, escriba los segundos que deben transcurrir para que el dispositivo intente volver a conectarse una vez desconectado.
Tipo de autenticación	Seleccione el tipo de autenticación: **Negociación automática**: el servidor envía una solicitud de configuración que especifica el algoritmo de seguridad establecido. Posteriormente, el dispositivo envía las credenciales de autenticación con el tipo de seguridad que envió anteriormente el servidor. **PAP**: el dispositivo usa el Protocolo de autenticación de contraseña (PAP) para realizar la conexión con el ISP. **CHAP**: el dispositivo usa el Protocolo de autenticación por desafío mutuo (CHAP) al realizar la conexión con el ISP. **MS-CHAP o MS-CHAPv2**: el dispositivo usa el Protocolo de autenticación por desafío mutuo de Microsoft (CHAP) al realizar la conexión con el ISP.

PASO 4 (Opcional) Para configurar los parámetros opcionales, consulte **Configuración de parámetros opcionales**.

PASO 5 Haga clic en **Save** (Guardar).

Configuración de L2TP

Para configurar las opciones L2TP:

PASO 1 Seleccione **Redes** > **WAN**.

PASO 2 En el menú desplegable **Tipo de conexión a Internet**, seleccione **L2TP**.

PASO 3 Escriba esta información:

Dir. IP de Internet	Escriba la dirección IP del puerto WAN.
Máscara de subred	Escriba la máscara de subred del puerto WAN.
Puerta de enlace predet.	Escriba la dirección IP de la puerta de enlace predeterminada.
Servidor L2TP	Escriba la dirección IP del servidor L2TP.
Nombre de usuario	Escriba el nombre de usuario que le asignó su ISP.
Contraseña	Escriba la contraseña que le asignó su ISP.
Conectar a petición	Seleccione esta opción si su ISP le cobra en función del tiempo que está conectado. Cuando selecciona esta opción, la conexión a Internet solo está activa si hay tráfico. Si no hay flujo de tráfico, la conexión está inactiva; es decir, está cerrada. Si hace clic en **Conectar a petición**, escriba los minutos que deben transcurrir para que se desactive la conexión en el campo **Tiempo máx. de inactividad**.
Mantener conexión	Cuando selecciona esta opción, la conexión a Internet está siempre activa. En el campo Período de repetición de marcación, escriba los segundos que deben transcurrir para que el dispositivo intente volver a conectarse una vez desconectado.
Tipo de autenticación	**Negociación automática**: el servidor envía una solicitud de configuración que especifica el algoritmo de seguridad establecido. Posteriormente, el dispositivo envía las credenciales de autenticación con el tipo de seguridad que envió el servidor. **PAP**: Protocolo de autenticación de contraseña (PAP); se utiliza para conectarse con el ISP. **CHAP**: Protocolo de confirmación de aceptación de la autenticación (CHAP); se utiliza para conectarse con el ISP. **MS-CHAP o MS-CHAPv2**: Protocolo de confirmación de aceptación de la autenticación de Microsoft (CHAP); se utiliza para conectarse con el ISP.

PASO 4 Haga clic en **Guardar**.

Configuración de parámetros opcionales

Para configurar los parámetros opcionales:

PASO 1 En la sección **Parámetros opcionales**, configure los siguientes parámetros:

Nombre del host	Nombre de host del dispositivo.
Nombre de dominio	Nombre de dominio para su red.
MTU	La unidad de transmisión máxima (MTU) es el tamaño del paquete más grande que puede enviarse a través de la red. El valor estándar de la MTU para las redes Ethernet en general es de 1500 bytes. Para las conexiones PPPoE, el valor es de 1492 bytes. A menos que su ISP exija algún cambio, le recomendamos que seleccione **Automática**. El tamaño predeterminado de MTU es de 1500 bytes. Si su ISP exige una configuración personalizada de MTU, seleccione **Manual** y escriba el tamaño de la MTU.
Tamaño	Tamaño de MTU.

PASO 2 Haga clic en **Guardar**.

Configuración de una red móvil

Use la página Red móvil para configurar el dispositivo para conectarlo a un módem USB de banda ancha móvil que esté conectado a la interfaz USB.

Para mostrar la ventana **Mobile Network** (Red móvil), elija **Networking** (Redes) > **WAN > Mobile Network (Red móvil)**.

Configuración global

Para instalar un módem USB:

PASO 1 Conecte el módem USB. Si el módem es compatible, se detectará automáticamente y aparecerá en la página Red móvil.

PASO 2 Seleccione el modo de conexión **Auto** (Automático) o **Manual** (Manual). La recuperación de conexión Ethernet solamente funciona si el modo de conexión se configura en automático.

- Para activar el módem y establecer una conexión automáticamente, seleccione modo **Automática**. Si selecciona este modo, también debe establecer un tiempo de Conexión a petición, o bien seleccionar Mantener conexión. La conexión a petición finaliza la conexión a Internet luego de que ha estado inactiva durante el período de tiempo especificado (Tiempo máx. de inactividad).

  Si su conexión a Internet finaliza debido a inactividad, el módem volverá a establecer una conexión en forma automática cuando un usuario intente acceder a Internet. En el campo **Max Idle Time** (Tiempo máx. de inactividad), ingrese la cantidad de minutos de tiempo de inactividad que puede transcurrir antes de que finalice la conexión a Internet. Si elije la opción **Keep Alive** (Mantener conexión), la conexión no finalizará en ningún momento.

- Para conectar o desconectar la conexión del módem manualmente, seleccione el modo **Manual**.

El dispositivo muestra el estado actual de la conexión del módem; incluye los estados de inicialización, conexión, desconexión o desconectado.

PASO 3 Verifique que el campo **Card Status** (Estado de tarjeta) muestre que su tarjeta móvil está **Connected** (Conectada).

También es posible que aparezcan los siguientes mensajes:

- Configure la APN manualmente (porque el dispositivo no puede determinar el nombre del punto de acceso)
- Buscando dispositivo...
- no hay tarjeta SIM
- SIM bloqueada
- SIM ocupada
- SIM lista
- Se necesita el código del PIN

- Error en el código del PIN
- La tarjeta está bloqueada
- La tarjeta no está activada
- Error de inicialización de la tarjeta
- error

Configuración de la red móvil

Si debe modificar alguno de los parámetros de la red móvil en el área **Mobile Network Setup** (Configuración de la red móvil), haga clic en el botón de radio **Manual** en el campo Configure Mode (Configurar modo). El dispositivo detecta automáticamente los módems compatibles y proporciona una lista de los parámetros de configuración adecuados. El PIN de la SIM puede modificarse tanto en el modo automático como manual.

El modelo de tarjeta le muestra el modelo del módem en el puerto USB. Las tarjetas no compatibles se informan como **no reconocidas**.

Para anular cualquiera de los otros parámetros, seleccione **Manual** y complete los siguientes campos:

Campo	Descripción
Nombre del punto de acceso (APN)	Red de Internet a la cual se conectará el dispositivo móvil. Ingrese el nombre de punto de acceso provisto por el proveedor de servicio de red móvil. Si no lo sabe, comuníquese con el proveedor del servicio.
Número de discado	Número de discado provisto por el proveedor del servicio de red móvil para la conexión a Internet.
Nombre de usuario Contraseña	Nombre de usuario y contraseña provistos por el proveedor del servicio de red móvil.
SIM verificada	Habilita y deshabilita la verificación de la tarjeta SIM.
SIM PIN	Código de PIN asociado a la tarjeta SIM. Este campo se muestra solamente para las tarjetas SIM GMS.
Nombre del servidor	Nombre del servidor para la conexión a Internet (en caso de que su proveedor de servicio se lo haya facilitado).

Campo	Descripción
Autenticación	Autenticación que utiliza el proveedor del servicio. El valor puede modificarse seleccionando el tipo de autenticación desde la lista desplegable. El modo predeterminado es Automática. Si no sabe qué tipo de autenticación usar, seleccione Automática.
Tipo de servicio	El tipo de servicio de conexión de datos móviles más común en función de la señal del área de servicio. Si la ubicación donde se encuentra admite únicamente servicio de datos móviles, puede limitar su opción preferida y reducir los tiempos configurados de conexión. La primera selección siempre busca el servicio HSPDA/3G/UMTS y cambia automáticamente a GPRS cuando está disponible.
Servicio LTE	Ajuste del servicio de evolución a largo plazo (LTE, Long Term Evolution). Seleccione **Auto** (Automático) para obtener una señal basada en la señal del área de servicio. Seleccione **4G only** (Solo 4G) para obtener únicamente señales 4G. Seleccione **3G only** (Solo 3G) para obtener únicamente señales 3G.

PASO 4 Haga clic en **Guardar** para guardar la configuración.

Configuración de la capacidad de banda ancha

El dispositivo controla la actividad de datos en el enlace de red móvil y cuando alcanza un umbral específico, envía una notificación.

Para activar o desactivar el seguimiento de la capacidad de banda ancha y configurar los límites:

PASO 1 Haga clic en **Activado** o **Desactivado**.

PASO 2 Seleccione **Monthly Renewal Date** (Fecha de renovación mensual) en la lista desplegable para indicar qué día del mes se reiniciará la capacidad de ancho de banda.

PASO 3 En el campo **Monthly Bandwidth Cap** (Capacidad de ancho de banda mensual), ingrese la cantidad máxima de datos en megabytes que tenga permitido transmitir antes de que el dispositivo realice una acción, como por ejemplo, enviar un correo electrónico a un administrador.

Config. de correo elec.

Cuando se alcanza el límite de datos, se puede enviar un mensaje de correo electrónico al administrador. Para configurar la dirección de correo electrónico del destinatario, marque la casilla de verificación **Email to** (Correo electrónico para) y haga clic en **Email Address** (Dirección de correo electrónico). Para obtener más información, consulte **Configuración de parámetros de correo electrónico**.

Si selecciona la casilla para activar esta opción, se enviará un correo electrónico:

- Cuando el uso de la red móvil haya excedido cierto porcentaje.
- Cuando el dispositivo falle por la ruta de respaldo y se recupere.
- En cada intervalo especificado mientras enlace de red móvil esté activa.

Configuración de recuperación tras fallas

Si bien puede ser que estén disponibles tanto Ethernet como un enlace de red móvil, solo se puede usar una conexión a la vez para establecer un enlace WAN. Cuando falle una conexión WAN, el dispositivo intentará establecer otra conexión en otra interfaz. Esta función se denomina Recuperación tras fallas. Cuando se restaure la conexión WAN primaria, se interrumpirá la conexión de respaldo. Esta función se denomina Recuperación.

PASO 1 Elija **Networking (Redes) > WAN > Failover & Recovery** (Conmutación por falla y recuperación).

PASO 2 Elija si su conexión de red primaria es una conexión WAN ethernet o una conexión de red móvil mediante un dispositivo de seguridad USB 3G.

PASO 3 Haga clic en el botón de radio **Failover to Secondary Enable** (Habilitar conmutación por falla a conexión secundaria) para permitir que el dispositivo conmute por falla de la conexión de red primaria y restaure la conectividad mediante la conexión secundaria.

Por ejemplo, su conexión primaria es una conexión WAN Ethernet y se interrumpe el enlace WAN. El dispositivo intenta restaurar la conexión mediante un enlace de red móvil 3G en la interfaz USB. Si no está activada la opción **Failover to Secondary Enable** (Habilitar conmutación por falla a conexión secundaria), la conexión secundaria está deshabilitada.

PASO 4 Haga clic en el botón de radio **Recovery back to Primary Enable** (Habilitar recuperación de conexión primaria) para permitir que el dispositivo revierta automáticamente a la conexión primaria e interrumpa la conexión secundaria. El modo de conexión de **WAN > Mobile Network** (Red móvil) debe estar establecido en Auto (Automático) para revertir automáticamente a una conexión primaria.

PASO 5 En el campo **Failover Check Interval** (Intervalo de verificación de conmutación por falla), ingrese el tiempo (en segundos) que debe transcurrir para que el dispositivo intente detectar la presencia de tráfico en la conexión secundaria.

PASO 6 En el campo **Recovery Check Interval** (Intervalo de verificación de recuperación), ingrese el tiempo (en segundos) que debe transcurrir para que el dispositivo intente detectar la presencia de tráfico en la conexión primaria. Si el enlace está inactivo, el dispositivo hace ping en un destino especificado en el intervalo especificado. Si hay una respuesta al paquete ping, el dispositivo asume que el enlace está activo e intenta revertir a la conexión de red primaria.

PASO 7 Haga clic en el botón de radio **Switch back to Primary immediately when Primary is available** (Volver de inmediato a conexión primaria cuando esté disponible) o establezca un tiempo en el campo **Switch back to Primary in a specific time range** (Volver a conexión primaria en un intervalo de tiempo específico). Si elige un intervalo de tiempo específico, determine las horas de inicio y finalización.

PASO 8 En el campo **Recovery Ping** (Ping de recuperación), ingrese la cantidad de veces que el dispositivo debe hacer ping en el sitio de validación de conexión después de la recuperación. Puede especificar hasta 5 pings de recuperación en el sitio. De manera predeterminada, el dispositivo hará ping una vez en el sitio de validación.

PASO 9 En el campo **Connection Validation Site** (Sitio de validación de conexión), elija la ubicación para hacer ping durante la validación de conmutación por falla y recuperación. Puede elegir la puerta de enlace del dispositivo, el DNS o una dirección IP personalizada como el sitio de validación. Si elige un sitio personalizado, ingrese la dirección IPv4 o IPv6. De manera predeterminada, el dispositivo hace ping en la puerta de enlace predeterminada para validar la conmutación por falla.

PASO 10 Para resolver los problemas de su conexión de red móvil 3G, haga clic en el botón de radio **3G Diagnostic Enable** (Habilitar diagnóstico 3G). Establezca el momento del día en que el dispositivo debe probar la conexión 3G.

PASO 11 Haga clic en **Guardar**.

La tabla de Interfaz WAN muestra el estado de WAN Ethernet y enlace de red móvil en Internet. Haga clic en el hipervínculo **Status** (Estado) para ver los detalles del puerto.

Actualización de dispositivo USB/WAN

Use esta página para cargar los archivos de módulo USB que admiten dispositivos de seguridad USB. Comuníquese con el soporte de Cisco para adquirir archivos de módulo USB. La Lista de módems USB de carga dinámica muestra los archivos de módulo de dispositivos de seguridad USB 3G y 4G compatibles con el dispositivo.

Para eliminar un archivo de módulo, seleccione el módulo de la Lista de módems USB de carga dinámica y haga clic en **Delete** (Eliminar).

Para cargar firmware de dispositivo USB (un módulo) de la PC:

PASO 1 Verifique que el dispositivo de seguridad USB no esté conectado al dispositivo.

PASO 2 Busque el archivo de módulo del dispositivo de seguridad USB y selecciónelo.

PASO 3 Haga clic en **Importar**.

PASO 4 Conecte el dispositivo de seguridad USB al dispositivo.

Configuración de opciones LAN

Las configuraciones DHCP y TCP/IP predeterminadas funcionan para la mayoría de las aplicaciones. Si desea que otra computadora de su red sea el servidor DHCP o si desea configurar manualmente las opciones de red de todos sus dispositivos, deshabilite el DHCP.

Además, en lugar de usar un servidor DNS, que asigna nombres de dominio de Internet (por ejemplo, www.cisco.com) a direcciones IP, puede usar un servidor de servicio de nombres de Internet de Windows (WINS). El servidor WINS es el servidor equivalente al servidor DNS, pero usa el protocolo NetBIOS para resolver los nombres de host. El dispositivo incluye la dirección IP del servidor WINS en la configuración DHCP que el dispositivo envía a los clientes de DHCP.

Si el dispositivo se conecta a un módem o un dispositivo que tiene una red configurada en la misma subred (192.168.1.x), el dispositivo modifica automáticamente la subred LAN a una subred aleatoria en función de 10.x.x.x, por lo que no hay un conflicto con la subred en la parte WAN del dispositivo.

Cambio de la dirección IP de administración de dispositivos

La dirección IP local de administración de dispositivos del dispositivo es estática y el valor predeterminado es 192.168.1.1.

Para modificar la dirección IP local de administración de dispositivos:

PASO 1 Seleccione **Redes** > **LAN** > **Configuración de LAN**.

PASO 2 En la sección **IPv4**, escriba esta información:

VLAN	El número de VLAN.
Dirección IP local	Dirección IP local de LAN del dispositivo. Asegúrese de que otro dispositivo no esté usando esta dirección IP.
Máscara de subred	Máscara de subred para la dirección IP local. La máscara de subred predeterminada es 255.255.255.0.

PASO 3 Haga clic en **Guardar**.

Una vez que modifique la dirección IP del dispositivo, su PC ya no podrá mostrar el Administrador de dispositivos.

Para mostrar el Administrador de dispositivos, siga uno de los siguientes pasos:

- Si el DHCP está configurado en dispositivo, libere y renueve la dirección IP de su computadora.
- Asigne manualmente una dirección IP a su computadora. La dirección debe estar en la misma subred que el dispositivo. Por ejemplo, si modifica la dirección IP del dispositivo a 10.0.0.1, asigne a su computadora una dirección IP en el rango de 10.0.0.2 a 10.0.0.255.

Abra una nueva ventana del explorador y escriba una nueva dirección IP del dispositivo para realizar nuevamente la conexión.

Configuración del servidor DHCP

Por opción predeterminada, dispositivo funciona como servidor DHCP para los hosts en la LAN inalámbrica (WLAN) o la LAN alámbrica. Asigna direcciones IP y brinda direcciones de servidor DNS.

Con DHCP activado, dispositivo asigna las direcciones IP a los dispositivos de red en la LAN de una agrupación de direcciones IPv4. El dispositivo prueba cada dirección antes de ser asignada para evitar direcciones duplicadas en la LAN.

La agrupación de direcciones IP predeterminadas abarca de 192.168.1.100 a 192.168.1.149. Para establecer una dirección IP estática en un dispositivo de red, utilice una dirección IP fuera de esta agrupación. Por ejemplo, suponiendo que la agrupación DHCP está configurada con los parámetros predeterminados, se pueden usar las direcciones IP estáticas de la agrupación de direcciones de 192.168.1.2 a 192.168.1.99. Lo anterior evita conflictos con la agrupación de direcciones IP DHCP.

Para configurar las opciones DHCP:

PASO 1 Seleccione **Redes** > **LAN** > **Configuración de LAN**.

PASO 2 (Opcional) Seleccione una VLAN que desee editar en la lista desplegable.

PASO 3 En el campo **Servidor DHCP**, seleccione una de las siguientes opciones:

Habilitar	Permite que dispositivo actúe como el servidor DHCP en la red.
Deshabilitar	Deshabilita DHCP en dispositivo cuando usted desea configurar manualmente las direcciones IP de todos los dispositivos de red.
Retransmisión DHCP	Retransmite las direcciones IP asignadas por otro servidor DHCP a los dispositivos de red.

Si usted habilitó el servidor DHCP dispositivo, ingrese esta información:

Dir. IP inicial	La primera dirección en la agrupación de direcciones IP. A cualquier cliente DHCP que se una a LAN se le asigna una dirección IP en este rango.
Cant. máx. de usuarios DHCP	La cantidad máxima de clientes DHCP.
Rango de dir. IP	(Sólo lectura) El rango de direcciones IP disponibles para los clientes DHCP.
Tiempo de concesión del cliente	Duración (en horas) que las direcciones IP se conceden a los clientes.
DNS estático 1	Dirección IP del servidor DNS primario.

DNS estático 2	Dirección IP del servidor DNS secundario.
DNS estático 3	Dirección IP del servidor DNS terciario.
WINS	Dirección IP del servidor WINS primario.

PASO 4 Si seleccionó **Retransmisión DHCP**, escriba la dirección de la puerta de enlace de retransmisión en el campo **Servidor DHCP remoto**. La puerta de enlace de retransmisión transmite mensajes DHCP al dispositivo de red, incluso a aquellos en otras subredes.

PASO 5 Haga clic en **Guardar**.

Configuración de VLAN

Una LAN virtual (VLAN) es un grupo de puntos finales en una red que se asocian según su función u otras características compartidas. A diferencia de las LAN que, en general, están basadas en zonas geográficas, las VLAN pueden agrupar puntos finales independientemente de la ubicación física del equipo o de los usuarios.

El dispositivo posee una VLAN predeterminada (VLAN 1) que no puede eliminarse. Puede crear hasta cuatro VLAN en el dispositivo.

Para crear una VLAN:

PASO 1 Seleccione **Redes** > **LAN** > **Afiliación a una VLAN**.

PASO 2 Haga clic en **Agregar fila**.

PASO 3 Escriba esta información:

ID de VLAN	ID numérica de VLAN para asignar los puntos finales en la afiliación VLAN. Debe escribir un número entre 3 y 4094. La ID de VLAN 1 está reservada para la VLAN predeterminada, que se usa para las tramas sin etiquetar recibidas en la interfaz.
Descripción	Descripción que identifica la VLAN.
Enrutamiento entre VLAN	Admite que una estación final en una VLAN se comunique con una estación final en otra VLAN.

Puerto 1 **Puerto 2** **Puerto 3** **Puerto 4**	Puede asociar las VLAN en el dispositivo a los puertos LAN en el dispositivo. De forma predeterminada, todos los puertos VLAN pertenecen a VLAN1. Puede editar estos puertos para asociarlos a otras VLAN. Elija el tipo de trama saliente para cada puerto: **Sin etiquetar**: la interfaz es un miembro sin etiquetar de la VLAN. Las tramas de la VLAN se envían sin etiqueta a la VLAN del puerto. **Etiquetado**: el puerto es un miembro etiquetado de la VLAN. Las tramas de la VLAN se envían con etiqueta a la VLAN del puerto. **Excluido**: actualmente el puerto no es miembro de la VLAN. Esta es la opción predeterminada para todos los puertos cuando se crea la VLAN.

PASO 4 Haga clic en **Guardar**.

Para editar las configuraciones de una VLAN, seleccione la VLAN y haga clic en **Editar**. Para eliminar una VLAN seleccionada, haga clic en **Eliminar**. Haga clic en **Guardar** para aplicar los cambios.

Configuración de DHCP estático

Puede configurar el dispositivo para asignar una dirección IP específica a un dispositivo con una dirección MAC específica.

Para configurar la DHCP estática:

PASO 1 Elija **Redes** > **LAN** > **DHCP estático**.

PASO 2 En el menú desplegable **VLAN**, seleccione un número de VLAN.

PASO 3 Haga clic en **Agregar fila**.

PASO 4 Escriba esta información:

Descripción	Descripción del cliente.
Dirección IP	Dirección IP del dispositivo. La dirección IP asignada no debe pertenecer a la agrupación de direcciones DHCP. La asignación DHCP estática significa que el servidor DHCP asigna la misma dirección IP a una dirección MAC definida cada vez que el dispositivo se conecta a la red. El servidor DHCP asigna la dirección IP reservada cuando el dispositivo que usa la dirección MAC correspondiente solicita una dirección IP.
Dirección MAC	Dirección MAC del dispositivo. El formato de una dirección MAC es XX:XX:XX:XX:XX:XX, donde X es un número de 0 a 9 (inclusive) o una letra entre la A y la F (inclusive).

Para editar las configuraciones de un cliente DHCP estático, seleccione el cliente y haga clic en **Editar**. Para eliminar un cliente DHCP seleccionado, haga clic en **Eliminar**. Haga clic en **Guardar** para aplicar los cambios.

Visualización de clientes DHCP alquilados

Puede ver una lista de puntos finales en la red (identificados por nombre de host, Dirección IP o Dirección MAC) y ver las direcciones IP que el servidor DHCP les asignó. También se muestra la VLAN de los puntos finales.

Para ver los clientes DHCP, elija **Redes** > **LAN** > **Clientes DHCP alquilados**.

Para cada VLAN definida en el dispositivo hay una tabla que muestra una lista de clientes asociados a la VLAN.

Para asignar una dirección IP estática a uno de los dispositivos conectados:

PASO 1 En la fila del dispositivo conectado, marque la casilla **Agregar al DHCP estático**.

PASO 2 Haga clic en **Guardar**.

El servidor DHCP del dispositivo siempre asignará la dirección IP que se muestra cuando el dispositivo solicita una dirección IP.

Configuración de un host DMZ

El dispositivo admite zonas desmilitarizadas (DMZ). La DMZ es una subred que está abierta al público pero que se encuentra detrás del firewall. La DMZ le permite redirigir los paquetes que se dirigen a su dirección IP del puerto WAN a una dirección IP determinada en su LAN.

Le recomendamos que use hosts que deban exponerse a la WAN (como servidores web o de correo electrónico) en la red DMZ. Puede configurar las reglas de firewall para permitir el acceso a servidores y puertos específicos en la DMZ desde la LAN o la WAN. En el caso de un ataque en cualquiera de los nodos DMZ, la LAN no necesariamente es vulnerable.

Debe configurar una dirección IP fija (estática) para el punto final que designe como host DMZ. Debe asignarle al host DMZ una dirección IP en la misma subred que la dirección IP LAN del dispositivo, pero no puede ser idéntica a la dirección IP otorgada a la interfaz LAN de esta puerta de enlace.

Para configurar la DMZ:

PASO 1 Seleccione **Redes** > **LAN** > **Host de DMZ**.

PASO 2 Marque **Habilitar** para habilitar la DMZ de la red.

PASO 3 En el menú desplegable VLAN, elija la ID de la VLAN donde se habilita la DMZ.

PASO 4 En el campo **Dir. IP del host**, escriba la dirección IP del host DMZ. El host de DMZ es el punto final que recibe los paquetes redirigidos.

PASO 5 Haga clic en **Guardar**.

Configuración de RSTP

El Protocolo de árbol de expansión rápida (RSTP, Rapid Spanning Tree Protocol) es un protocolo de red que impide la presencia de bucles en la red y reconfigura de manera dinámica qué enlaces físicos deben enviar tramas. Para configurar el protocolo de árbol de expansión rápida (RTSP):

PASO 1 Seleccione **Redes** > **LAN** > **RSTP**.

PASO 2 Configure los siguientes valores:

Prioridad del sistema	Seleccione la prioridad del sistema en el menú desplegable. Puede elegir de una prioridad de sistema de 0 a 61440 en incrementos de 4096. Los valores válidos son 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 40960, 45056, 49152, 53248, 57344 y 61440. Cuanto más baja sea la prioridad del sistema, mayores serán las probabilidades de que el dispositivo sea la raíz en el árbol de expansión. El valor predeterminado es **327688**.
Tiempo de saludo	El tiempo de saludo es el período de tiempo que la raíz del árbol de expansión espera antes de enviar mensajes de saludo o hello. Escriba un número de 1 a 10. El número predeterminado es **2**.
Tiempo máximo	La edad máxima es el período de tiempo que el router espera para recibir un mensaje de saludo o hello. Si se alcanza la edad máxima, el router intenta modificar el árbol de expansión. Escriba un número de 6 a 40. El número predeterminado es **20**.
Retraso de reenvío	El retraso de reenvío es el intervalo después del cual una interfaz cambia de estado de bloqueo a estado de reenvío. Escriba un número de 4 a 30. El número predeterminado es **15**.
Forzar versión	Seleccione la versión de protocolo predeterminado que desea usar. Seleccione **Normal** (use RSTP) o **Compatible** (compatible con el STP anterior). El valor predeterminado es **Normal**.

PASO 3 En la **Tabla de config.**, configure los siguientes parámetros:

Protocolo habilitado	Marque la casilla para habilitar el RSTP en el puerto asociado. El protocolo RSTP está deshabilitado de manera predeterminada.
Borde	Marque esta casilla para especificar que el puerto asociado es un puerto de borde (estación final). Desmarque esta casilla para especificar que el puerto asociado es un enlace (puente) a otro dispositivo STP. El puerto de borde está habilitado de forma predeterminada.
Costo de trayecto	Introduzca el costo de trayecto del RSTP para los puertos designados. Use 0 para el valor predeterminado (el dispositivo determina automáticamente el valor de la ruta). También puede ingresar un número del 2 al 200000000.

PASO 4 Haga clic en **Guardar**.

Administración de puertos

Puede configurar las opciones de velocidad y control de flujo de los cuatro puertos LAN del dispositivo.

Para configurar las velocidades del puerto y el control del flujo:

PASO 1 Elija **Redes** > **Administración de puertos**.

PASO 2 Configure esta información:

Puerto	El número del puerto.
Enlace	La velocidad del puerto. Si no hay un dispositivo conectado al puerto, este campo muestra **Inactivo**.

Modo	Seleccione en el menú desplegable una de las siguientes velocidades de puerto: • **Negociación automática**: el dispositivo y el dispositivo conectado seleccionan una velocidad común. • **Semi de 10 Mbps**: 10 Mbps en ambas direcciones, pero solo una dirección a la vez. • **Completo de 10 Mbps**: 10 Mbps en ambas direcciones de forma simultánea. • **Semi de 100 Mbps**: 100 Mbps en ambas direcciones, pero solo una dirección a la vez. • **Completo de 100 Mbps**: 100 Mbps en ambas direcciones de forma simultánea.
Control de flujo	Marque la casilla para habilitar el control de flujo para este puerto. El control de flujo es el proceso de administración de la velocidad de transmisión de datos entre dos nodos para evitar que un remitente rápido exceda la velocidad de un receptor lento. Ofrece un mecanismo para que el receptor controle la velocidad de transmisión, de manera que el nodo de recepción no se sature con datos del nodo de transmisión.

PASO 3 Haga clic en **Guardar**.

Clonación de la dirección MAC

Algunas veces, quizá necesite configurar la dirección MAC del puerto WAN del dispositivo para que sea igual a la dirección MAC de su computadora o a otra dirección MAC. Esto se denomina clonación de dirección MAC.

Por ejemplo, algunos ISP registran la dirección MAC de la tarjeta NIC de su computadora cuando se instala el servicio. Cuando coloca un router detrás del módem por cable o el módem DSL, el ISP no reconoce la dirección MAC del puerto WAN del dispositivo.

En este caso, para configurar su dispositivo de manera que el ISP lo reconozca, clone la dirección MAC del puerto WAN para que sea igual a la dirección MAC de su computadora.

Para configurar el clon de una dirección MAC:

PASO 1 Seleccione **Redes** > **Clon de dir. MAC**.

PASO 2 En el campo **Clon de dir. MAC**, marque **Habilitar** para habilitar la clonación de la dirección MAC.

PASO 3 Para configurar la dirección MAC del puerto WAN del dispositivo, seleccione una de las siguientes opciones:

- Para configurar la dirección MAC del puerto WAN de manera que sea igual a la dirección MAC de su computadora, haga clic en **Clonar MAC de Mi PC**.
- Para especificar una dirección MAC diferente, escríbala en el campo **Dirección MAC**.

PASO 4 Haga clic en **Guardar**.

Configuración de enrutamiento

Configure las opciones de enrutamiento.

Configuración del modo operativo

Para configurar el modo operativo de dispositivo:

PASO 1 Seleccione **Redes** > **Enrutamiento**.

PASO 2 En el campo **Modo operativo**, seleccione una de las siguientes opciones:

Puerta de enlace	(Recomendado) Haga clic en este botón para configurar el dispositivo de tal manera que funcione como la puerta de enlace. Mantenga esta configuración predeterminada si el dispositivo es el host de la conexión de su red a Internet y desempeña las funciones de enrutamiento.

Router	(Solo para usuarios avanzados) Haga clic en este botón para configurar el dispositivo de tal manera que funcione como router. Seleccione esta opción si el dispositivo se encuentra en una red con otros routers. Al habilitar el modo Router, se deshabilita la NAT (Traducción de direcciones de red) en el dispositivo.

PASO 3 Haga clic en **Guardar**.

Configuración de enrutamiento dinámico

El protocolo de información de enrutamiento (RIP) es un protocolo de puerta de enlace interior (IGP) que se usa con frecuencia en las redes internas. Le permite al router intercambiar su información de enrutamiento de forma automática con otros routers y le permite ajustar de forma dinámica sus tablas de enrutamiento y adaptarla a los cambios en la red.

El enrutamiento dinámico (RIP) permite que el dispositivo se adapte de forma automática a los cambios físicos en el diseño de la red e intercambiar las tablas de enrutamiento con otros routers.

El router determina la ruta de los paquetes de red en función de la menor cantidad de saltos entre el origen y el destino. El protocolo RIP está deshabilitado de manera predeterminada.

NOTA El protocolo RIP está deshabilitado de manera predeterminada en el dispositivo.

Para configurar el enrutamiento dinámico:

PASO 1 Seleccione **Redes** > **Enrutamiento**.

PASO 2 Configure los siguientes valores:

RIP	Marque la casilla **Habilitar** para habilitar RIP. Esto permite que el dispositivo use el RIP para dirigir el tráfico.

Versión de envío de paquetes por RIP	Seleccione la versión de envío de paquetes por RIP (**RIPv1** o **RIPv2**). La versión de RIP que se usa para enviar las actualizaciones a otros routers en la red depende de los parámetros de configuración de los otros routers. RIPv2 tiene compatibilidad descendente con RIPv1.
Versión de recepción de paquetes por RIP	Seleccione la versión de recepción de paquetes por RIP.

PASO 3 Haga clic en **Guardar**.

Configuración de enrutamiento estático

Puede configurar las rutas estáticas para dirigir los paquetes a la red de destino. Una ruta estática es el trayecto predeterminado que el paquete debe recorrer para alcanzar un host o red específicos.

Algunos ISP necesitan rutas estáticas para crear su tabla de enrutamiento en lugar de usar protocolos de enrutamiento dinámicos. Las rutas estáticas no necesitan recursos de CPU para intercambiar información de enrutamiento con un router de par.

También puede usar rutas estáticas para alcanzar routers de par que no admiten protocolos de enrutamiento dinámico. Las rutas estáticas se pueden usar junto con las rutas dinámicas. El dispositivo admite hasta 30 rutas estáticas.

Asegúrese de no introducir bucles de enrutamiento en su red.

Para configurar el enrutamiento estático:

PASO 1 Seleccione **Redes** > **Enrutamiento**.

PASO 2 En el menú desplegable **Entradas de ruta**, elija una entrada de ruta.

Para eliminar la entrada de ruta, haga clic en **Eliminar esta entrada**.

PASO 3 Configure los siguientes parámetros para la entrada de ruta seleccionada:

Escribir nombre de ruta	Escriba el nombre de la ruta.
IP de LAN de destino	Escriba la dirección IP de la LAN de destino.

Máscara de subred	Escriba la máscara de subred de la red de destino.
Puerta de enlace	Escriba la dirección IP de la puerta de enlace usada para esta ruta.
Interfaz	Seleccione la interfaz a la que se envían los paquetes para esta ruta: • **LAN e inalámbrica**: haga clic en este botón para dirigir los paquetes a la LAN y la red inalámbrica. • **Internet (WAN)**: haga clic en este botón para dirigir los paquetes a Internet (WAN).

PASO 4 Haga clic en **Guardar**.

Visualización de la tabla de enrutamiento

En la tabla de enrutamiento, hay información acerca de la topología de la red que lo rodea de forma directa.

Para ver la información de enrutamiento de su red, seleccione **Redes** > **Tabla de enrutamiento** y elija una de las siguientes opciones:

- **Mostrar tabla de enrutamiento IPv4**: la tabla de enrutamiento se muestra con los campos configurados en las páginas **Redes** > **Enrutamiento**.
- **Mostrar tabla de enrutamiento IPv6**: la tabla de enrutamiento se muestra con los campos configurados en las páginas **Redes** > **IPv6**.

Configuración de DNS dinámico

El DNS dinámico (DDNS) es un servicio de Internet que permite localizar los routers con diferentes direcciones IP a través de nombres de dominio de Internet. Para usar el DDNS, debe configurar una cuenta con un proveedor DDNS como DynDNS.com, TZO.com, 3322.org, o noip.com.

El router notifica a los servidores DNS dinámicos los cambios en la dirección IP WAN, de manera que se pueda obtener acceso a cualquier servicio público en su red a través del nombre de dominio.

Para configurar el DDNS, haga lo siguiente:

PASO 1 Seleccione **Redes** > **DNS dinámico**.

PASO 2 En el menú desplegable **Servicio DDNS**, elija **Deshabilitar** para deshabilitar este servicio o elija el servicio DDNS que desea usar.

PASO 3 Si no tiene una cuenta DDNS, haga clic en la URL del servicio para visitar el sitio web del servicio DDNS seleccionado, de manera que pueda crear una cuenta.

PASO 4 Configure esta información:

Dir. de correo electrónico	(TZO.com y noip.com) Dirección de correo electrónico que usó para crear la cuenta DDNS.
Nombre de usuario	(DynDNS.com y 3322.org) Nombre de usuario de la cuenta DDNS.
Contraseña	Contraseña de la cuenta DDNS.
Verificar contraseña	(TZO.com, DynDNS.com y noip.com) Confirmación de la contraseña de la cuenta DDNS.
Nombre del host	(DynDNS.com, 3322.org y noip.com) Nombre de host del servidor DDNS.
Nombre de dominio	(TZO.com) Nombre del dominio que se usa para acceder a la red.

Intervalo de actualización	Elija una de las siguientes opciones para establecer la frecuencia con la que desea actualizar la dirección IP y el nombre de dominio al servidor DDNS: **Never** (Nunca): no actualizar nunca. **Weekly** (Por semana): actualizar todas las semanas a las 00:MM del lunes, donde MM es un número elegido aleatoriamente entre 0 y 59. Esta opción se selecciona de manera predeterminada. **Semi-monthly** (Por quincena): actualizar el día 1.º y día 15 del mes a las 00:MM, donde MM es un número elegido aleatoriamente entre 0 y 59. **Monthly** (Por mes): actualizar el día 1.º del mes a las 00:MM, donde MM es un número elegido aleatoriamente entre 0 y 59.
Dir. IP de Internet	(Solo lectura) La dirección IP de Internet del dispositivo.
Estado	(Solo lectura) Indica si la actualización del DDNS se completó correctamente o si la información de la actualización de la cuenta enviada al servidor DDNS no llegó a destino.

PASO 5 Para realizar una prueba de la configuración DDNS, haga clic en **Configuración de prueba**.

PASO 6 Haga clic en **Guardar**.

Configuración del modo IP

Las propiedades de configuración de red de área ancha son configurables para las redes IPv4 e IPv6. Puede escribir información acerca de su tipo de conexión a Internet y otros parámetros en estas páginas.

Para seleccionar un modo de IP:

PASO 1 Seleccione **Redes** > **Modo IP**.

PASO 2 En el menú desplegable **Modo IP**, seleccione una de las siguientes opciones:

LAN:IPv4, WAN:IPv4	Utiliza IPv4 en los puertos LAN y WAN.
LAN:IPv6, WAN:IPv4	Utiliza IPv6 en los puertos LAN e IPv4 en los puertos WAN.
LAN:IPv6, WAN:IPv6	Utiliza IPv6 en los puertos LAN y WAN.
LAN:IPv4+IPv6, WAN:IPv4	Utiliza IPv4 e IPv6 en los puertos LAN e IPv4 en los puertos WAN.
LAN:IPv4+IPV6, WAN:IPv4+IPv6	Utiliza IPv4 e IPv6 en los puertos LAN y WAN.
LAN:IPv4, WAN:IPv6	Utiliza IPv4 en los puertos LAN e IPv6 en los puertos WAN.

PASO 3 (Opcional) Si usa tunelización 6to4, que permite que los paquetes IPv6 se transmitan en una red IPv4, haga lo siguiente:

a. Haga clic en **Mostrar entrada estática DNS 6to4**.

b. En los campos **Dominio** e **IP**, escriba hasta cinco asignaciones de dominio a IP.

La función de tunelización 6to4 se usa habitualmente cuando un sitio o usuario final desea conectarse a IPv6 Internet a través de la red IPv4 existente.

PASO 4 Haga clic en **Guardar**.

Configuración IPv6

La versión 6 del protocolo de Internet (IPv6) es una versión del protocolo de Internet (IP) que tiene como objetivo reemplazar la versión 4 del protocolo de Internet (IPv4). La configuración de las propiedades WAN para una red IPv6 depende del tipo de conexión a Internet que tenga.

Configuración de conexiones IPv6 WAN

Puede configurar el dispositivo para que sea un cliente DHCPv6 del ISP para esta WAN o usar una dirección IPv6 estática provista por el ISP.

Para configurar las opciones IPv6 WAN en su dispositivo, primero debe configurar el modo IP a uno de los siguientes modos:

- LAN:IPv6, WAN:IPv6
- LAN:IPv4+IPv6, WAN:IPv4
- LAN:IPv4+IPv6, WAN:IPv4+IPv6

Consulte **Configuración del modo IP** para obtener instrucciones sobre cómo configurar el modo IP.

Configuración de DHCPv6

Si su ISP le suministra una dirección asignada dinámicamente, configure el dispositivo como un cliente DHCPv6.

Para configurar el dispositivo como cliente DHCPv6:

PASO 1 Elija **Redes** > **IPv6** > **Configuración IPv6 WAN**.

PASO 2 En el campo **Tipo de conexión WAN**, seleccione **Config. automática - DHCPv6**.

PASO 3 Haga clic en **Guardar**.

Configuración de una dirección IPv6 estática de WAN

Si su ISP le asigna una dirección fija para obtener acceso a WAN, configure el dispositivo para usar una dirección IPv6 estática.

Para configurar una dirección IPv6 WAN estática:

PASO 1 Elija **Redes** > **IPv6** > **Configuración IPv6 WAN**.

PASO 2 En el campo **Tipo de conexión WAN**, seleccione **IPv6 estática**.

PASO 3 Escriba esta información:

Dirección IPv6	Dirección IPv6 del puerto WAN.

Longitud de prefijo IPv6	Longitud del prefijo IPv6 (generalmente definida por el ISP). La red IPv6 (subred) se identifica a través de los bits iniciales de la dirección denominados prefijo. Todos los hosts en la subred poseen un prefijo idéntico. Por ejemplo, en la dirección IPv6 `2001:0DB8:AC10:FE01::` el prefijo es `2001`.
Puerta de enlace IPv6 predeterminada	Dirección IPv6 de la puerta de enlace predeterminada. Generalmente se trata de la dirección IP del servidor en el ISP.
DNS estático 1	Dirección IP del servidor IPv6 DNS primario.
DNS estático 2	Dirección IP del servidor IPv6 DNS secundario.

PASO 4 Haga clic en **Guardar**.

Configuración de opciones PPPoE IPv6

Puede ejecutar IPv4 PPPoE, IPv6 PPPoE, o ambos. Si ejecuta ambos, la configuración de su IPv6 WAN PPPoE debe coincidir con la configuración de su IPv4 WAN PPPoE. Si no coinciden, aparecerá un mensaje que le preguntará si desea establecer el protocolo IPv6 para que coincida con el protocolo IPv4 . Para obtener más información, consulte **Configuración de PPPoE**.

Para configurar las opciones PPPoE IPv6, siga estos pasos:

PASO 1 Elija **Redes** > **IPv6** > **Configuración IPv6 WAN**.

PASO 2 En el campo **Tipo de conexión WAN**, seleccione **PPPoE IPv6**.

PASO 3 Escriba la siguiente información (quizá deba comunicarse con su ISP para obtener información de inicio de sesión de su PPPoE):

Nombre de usuario	El nombre de usuario asignado a usted por el ISP.
Contraseña	La contraseña asignada a usted por el ISP.

Conectar a petición	Si el ISP le cobra en función de la cantidad de tiempo que estuvo conectado, seleccione el botón de radio. Cuando lo seleccione, la conexión a Internet estará activa solamente cuando haya tráfico. Si no hay flujo de tráfico, la conexión está inactiva; es decir, está cerrada. En el campo **Tiempo máx. de inact.**, ingrese la cantidad de minutos que deben transcurrir sin que se detecte tráfico para que el enlace se torne inactivo.
Mantener conexión	Mantiene el enlace WAN activo, ya que envía un mensaje de conexión activa mediante el puerto. En el campo Período de repetición de marcación, escriba los segundos que deben transcurrir para que el dispositivo intente volver a conectarse una vez desconectado.
Tipo de autenticación	Tipos de autenticación: **Negociación automática**: el servidor envía una solicitud de configuración que especifica el algoritmo de seguridad establecido en el servidor. dispositivo responde con sus credenciales de autenticación, incluido el tipo de seguridad enviado por el servidor. **PAP**: usa el Protocolo de autenticación de contraseña (PAP) para realizar la conexión con el ISP. **CHAP**: usa el Protocolo de confirmación de aceptación de la autenticación (CHAP) para conectarse al ISP. **MS-CHAP o MS-CHAPv2**: usa el Protocolo de confirmación de aceptación de la autenticación de Microsoft (CHAP) para conectarse con el ISP.
Nombre del servicio	Nombre que puede necesitar el ISP para iniciar sesión en el servidor PPPoE.

MTU	La unidad de transmisión máxima (MTU) o el tamaño del paquete más grande que puede enviarse a través de la red. A menos que su ISP exija algún cambio, le recomendamos que seleccione **Automática**. El valor estándar de la MTU para las redes Ethernet es de 1500 bytes. Para las conexiones PPPoE, el valor es de 1492 bytes. Si su ISP requiere una configuración personalizada para la MTU, escoja **Manual**.
Tamaño	Tamaño de MTU. Si su ISP exige una configuración personalizada de MTU, ingrese el tamaño de la MTU.
Modo de dirección	Modo de dirección dinámico o estático. Si selecciona estático, introduzca la dirección IPv6 en el campo que se encuentra a continuación.
Longitud de prefijo IPv6	Longitud del prefijo IPv6.
Puerta de enlace IPv6 predeterminada	Dirección IP de la puerta de enlace IPv6 predeterminada.
DNS estático 1	Dirección IP del servidor DNS primario.
DNS estático 2	Dirección IP del servidor DNS secundario.

PASO 4 Haga clic en **Guardar**.

Configuración de conexiones IPv6 LAN

En el modo IPv6, el servidor LAN DHCP se habilita de forma predeterminada (similar al modo IPv4). El servidor DHCPv6 asigna direcciones IPv6 de las agrupaciones de direcciones configuradas que usan la longitud de prefijo IPv6 asignada a la LAN.

Para configurar las opciones IPv6 LAN en su dispositivo, primero debe configurar el modo IP a uno de los siguientes modos:

- LAN:IPv6, WAN:IPv4
- LAN:IPv6, WAN:IPv6

- LAN:IPv4+IPv6, WAN:IPv4
- LAN:IPv4+IPv6, WAN:IPv4+IPv6

Consulte **Configuración del modo IP** para obtener más información sobre cómo configurar el modo IP.

Para configurar las opciones IPv6 LAN:

PASO 1 Elija **Redes** > **IPv6** > **Configuración IPv6 LAN**.

PASO 2 Escriba la siguiente información para configurar la dirección IPv6 LAN:

Dirección IPv6	Escriba la dirección IPv6 del dispositivo. La dirección IPv6 predeterminada para la puerta de enlace es fec0::1 (o FEC0:0000:0000:0000:0000:0000:0000:0001). Puede cambiar esta dirección IPv6 de 128 bits según los requisitos de la red.
Longitud de prefijo IPv6	Escriba la longitud de prefijo IPv6. La red IPv6 (subred) se identifica a través de los bits iniciales de la dirección denominados prefijo. De forma predeterminada, el prefijo tiene una longitud de 64 bits. Todos los hosts de la red tienen bits iniciales idénticos para su dirección IPv6; en este campo se establece la cantidad de bits iniciales comunes a las direcciones de red.

PASO 3 Haga clic en **Guardar** o continúe con la configuración de los valores de IPv6 DHCP LAN.

PASO 4 Escriba la siguiente información para configurar la dirección DHCPv6:

Estado DHCP	Marque la casilla para habilitar el servidor DHCPv6. Cuando se habilita, el dispositivo asigna una dirección IP dentro del rango especificado y brinda información adicional a cualquier punto final LAN que solicite las direcciones DHCP.
Nombre de dominio	(Opcional) Nombre de dominio del servidor DHCPv6.
Preferencia de servidor	Nivel de preferencia del servidor en este servidor DHCP. Los mensajes de anuncios con el valor de preferencia de servidor más alto a un host LAN se prefieren a otros mensajes de anuncios de servidor DHCP. El valor predeterminado es 255.
DNS estático 1	Dirección IPv6 del servidor DNS primario en la red IPv6 del ISP.
DNS estático 2	Dirección IPv6 del servidor DNS secundario en la red IPv6 del ISP.
Tiempo de concesión del cliente	Duración del tiempo de concesión al cliente (en segundos) durante el cual las direcciones IPv6 se conceden a los puntos finales de la LAN.

PASO 5 Elija **Redes** > **IPv6** > **Configuración IPv6 LAN**.

PASO 6 En la **Tabla de agrupación de dir. IPv6**, haga clic en **Agregar fila**.

PASO 7 Escriba esta información:

Dirección inicial	Dirección IPv6 inicial de la agrupación.
Dirección final	Dirección IPv6 final de la agrupación.
Longitud de prefijo IPv6	Longitud del prefijo que determina la cantidad de bits iniciales comunes en las direcciones de la red.

PASO 8 Haga clic en **Guardar**.

Para editar las configuraciones de una agrupación, seleccione la agrupación y haga clic en **Editar**. Para eliminar una agrupación seleccionada, haga clic en **Eliminar**. Haga clic en **Guardar** para aplicar los cambios.

Configuración de enrutamiento estático IPv6

Puede configurar las rutas estáticas para dirigir los paquetes a la red de destino. Una ruta estática es el trayecto predeterminado que el paquete debe recorrer para alcanzar un host o red específicos.

Algunos ISP necesitan rutas estáticas para crear su tabla de enrutamiento en lugar de usar protocolos de enrutamiento dinámicos. Las rutas estáticas no necesitan recursos de CPU para intercambiar información de enrutamiento con un router de par.

También puede usar rutas estáticas para alcanzar routers de par que no admiten protocolos de enrutamiento dinámico. Las rutas estáticas se pueden usar junto con las rutas dinámicas. Asegúrese de no introducir bucles de enrutamiento en su red.

Para crear una ruta estática:

PASO 1 Seleccione **Redes** > **IPv6** > **Enrutamiento estático IPv6**.

PASO 2 En la lista de rutas estáticas, haga clic en **Agregar fila**.

PASO 3 Escriba esta información:

Nombre	Nombre de la ruta.
Destino	Dirección IPv6 del host o la red de destino para esta ruta.
Longitud del prefijo	Cantidad de bits del prefijo en la dirección IPv6 que define la subred de destino.
Puerta de enlace	Dirección IPv6 de la puerta de enlace a través de la cual puede alcanzarse el host o la red de destino.
Interfaz	Interfaz para la ruta: **LAN**, **WAN** o **6to4**.
Métrico	Prioridad de la ruta. Escoja un valor entre 2 y 15. Si existen diversas rutas para el mismo destino, se utilizará la ruta con la métrica más baja.

Activo	Marque la casilla para activar la ruta. Cuando agrega una ruta en el estado inactivo, se incluye en la lista de enrutamiento, pero el dispositivo no la utiliza. La incorporación de una ruta inactiva sirve si la ruta no está disponible cuando usted la incorpora. Cuando la red esté disponible, podrá habilitarla.

PASO 4 Haga clic en **Guardar**.

Para editar las configuraciones de una ruta, seleccione la ruta y haga clic en **Editar**. Para eliminar una ruta seleccionada, haga clic en **Eliminar**. Haga clic en **Guardar** para aplicar los cambios.

Configuración de enrutamiento (RIPng)

RIP Nueva generación (RIPng) es un protocolo de enrutamiento basado en el algoritmo de vector de distancia (D-V). RIPng usa los paquetes UDP para intercambiar la información de enrutamiento a través del puerto 521.

RIPng usa un conteo de saltos para medir la distancia a un destino. El conteo de saltos se denomina métrica o costo. El conteo de saltos de un router a una red conectada directamente es 0. El conteo de saltos entre dos routers conectados directamente es 1. Cuando el conteo de saltos es superior o igual a 16, la red o el host de destino no puede alcanzarse.

De forma predeterminada, la actualización del enrutamiento se envía cada 30 segundos. Si el router no recibe actualizaciones de un vecino después de 180 segundos, las rutas adquiridas del vecino se consideran inalcanzables. Después de otros 240 segundos, si no se recibe actualización de enrutamiento, el router elimina estas rutas de la tabla de enrutamiento.

En el dispositivo, el RIPng se deshabilita de forma predeterminada.

Para configurar el RIPng:

PASO 1 Seleccione **Redes** > **IPv6** > **Enrutamiento (RIPng)**.

PASO 2 Haga clic en **Habilitar**.

PASO 3 Haga clic en **Guardar**.

Configuración de la tunelización

La tunelización IPv6 a IPv4 (tunelización 6to4) permite que los paquetes IPv6 sean transmitidos a través de una red IPv4. La tunelización IPv4 a IPv6 (tunelización 4to6) permite que los paquetes IPv4 sean transmitidos a través de una red IPv6.

Tunelización 6to4

6to4, como característica de tunelización, se usa habitualmente cuando un sitio o usuario final desea conectarse a IPv6 Internet a través de la red IPv4 existente.

Pasos para configurar la tunelización 6to4:

PASO 1 Seleccione **Redes** > **IPv6** > **Tunelización**.

PASO 2 En el campo **Tunelización 6to4**, marque **Habilitar**.

PASO 3 Seleccione el tipo de tunelización (**6to4** o **6RD** [Implementación rápida]).

PASO 4 Para la tunelización 6RD, seleccione **automática** o **manual**.

PASO 5 Introduzca la siguiente información:

- **Prefijo IPv6**
- **Longitud de prefijo IPv6**
- **Retransmisión de borde**
- **Longitud de la máscara IPv4**

PASO 6 Haga clic en **Guardar**.

Tunelización 4to6

Pasos para configurar la tunelización 4to6:

PASO 1 Seleccione **Redes** > **IPv6** > **Tunelización**.

PASO 2 En el campo **Tunelización 4to6**, marque **Habilitar**.

PASO 3 Escriba la dirección IPv6 local del puerto WAN en el dispositivo.

PASO 4 Escriba la dirección IPv6 remota o la dirección IP del punto final remoto.

PASO 5 Haga clic en **Guardar**.

Visualización del estado de túnel IPv6

Para ver el estado de túnel IPv6, haga lo siguiente:

PASO 1 Seleccione **Redes** > **IPv6** > **Estado de túneles IPv6**.

PASO 2 Haga clic en **Actualizar** para visualizar la información más actualizada.

Esta página muestra información acerca de la configuración automática del túnel a través de la interfaz WAN dedicada. La tabla muestra el nombre del túnel y la dirección IPv6 que se crea en el dispositivo.

Configuración de aviso de router

El Daemon de aviso de router (RADVD) en el dispositivo escucha las solicitudes de router en la LAN IPv6 y responde con avisos de router, según corresponda. Esta es la configuración automática IPv6 sin estado y el dispositivo distribuye los prefijos IPv6 a todos los nodos en la red.

Para configurar el RADVD:

PASO 1 Seleccione **Redes** > **IPv6** > **Aviso de router**.

PASO 2 Escriba esta información:

Estado de RADVD	Marque la casilla **Habilitar** para habilitar el RADVD.
Modo de anuncios	Seleccione uno de los siguientes modos: **Multidifusión no solicitada**: envíe los avisos de router (RA) a todas las interfaces que pertenecen al grupo de multidifusión. **Solo unidifusión**: restrinja los avisos a las direcciones IPv6 conocidas solamente (las RA se envían a la interfaz que pertenece a la dirección conocida solamente).

Intervalo de anuncios	Intervalo de anuncios (4-1800) para la **Multidifusión no solicitada**. El valor predeterminado es 30. El intervalo de anuncios es un valor aleatorio entre el intervalo de aviso de router mínimo (MinRtrAdvInterval) y el intervalo de aviso de router máximo (MaxRtrAdvInterval). MinRtrAdvInterval = 0,33 * MaxRtrAdvInterval
Indicadores RA	Marque la casilla **Administrado** para usar el protocolo con estado/administrado para la configuración automática de la dirección. Marque la casilla **Otro** para usar el protocolo con estado/administrado para la configuración de la información no relacionada con la dirección.
Preferencia del router	Seleccione **baja**, **media** o **alta** en el menú desplegable. El valor predeterminado es medio. La preferencia del router ofrece una métrica de preferencia para los routers predeterminados. Los valores bajos, medios y altos están señalizados en los bits sin usar en los mensajes RA. Esta extensión tiene compatibilidad descendente para los routers (al configurar el valor de preferencia del router) y los hosts (al interpretar el valor de preferencia del router). Estos valores son ignorados por los hosts que no implementan la preferencia del router. Esta característica es útil si hay otros dispositivos habilitados por RADVD en LAN.
MTU	Tamaño de MTU (0 o 1280 a 1500). El valor predeterminado es 1500 bytes. La unidad de transmisión máxima (MTU) es el paquete más grande que puede enviarse a través de la red. La MTU se usa en las RA para garantizar que todos los nodos de la red usen el mismo valor de MTU cuando la MTU de la LAN no se conoce.
Tiempo de vida del router	Valor de tiempo de vida del router, o el tiempo en segundos que los mensajes de anuncios existen en la ruta. El valor predeterminado es 3600 segundos.

PASO 3 Haga clic en **Guardar**.

Configuración de los prefijos de anuncios

Para configurar los prefijos disponibles de RADVD:

PASO 1 Seleccione **Redes** > **IPv6** > **Prefijos de anuncios**.

PASO 2 Haga clic en **Agregar fila**.

PASO 3 Escriba esta información:

Tipo de prefijo IPv6	Seleccione uno de los siguientes tipos: **6to4**: admite la transmisión de paquetes IPv6 por una red IPv4. Se usa cuando un usuario final desea conectarse a Internet IPv6 con su conexión IPv4 existente. **Global/Local**: una dirección IPv6 localmente única que puede usar en las redes privadas IPv6 o una dirección de Internet IPv6 globalmente única.
ID de SLA	Si elige **6to4** como el tipo de prefijo IPv6, escriba el identificador de agrupación según el sitio (SLA ID). La SLA ID en el prefijo de la dirección 6to4 se determina en la ID de interfaz en la que se envían los anuncios.
Prefijo IPv6	Si elige **Global/Local** como el tipo de prefijo IPv6, escriba el prefijo IPv6. El prefijo IPv6 especifica la dirección de red IPv6.
Longitud de prefijo IPv6	Si elige **Global/Local** como el tipo de prefijo IPv6, escriba la longitud de prefijo. La variable de longitud de prefijo es un valor decimal que indica la cantidad de bits contiguos de orden superior de la dirección que conforma la parte de la red de la dirección.
Tiempo de vida del prefijo	Tiempo de vida del prefijo, o el tiempo total que el router que solicita autenticación puede usar el prefijo.

PASO 4 Haga clic en **Guardar**.

4

Configuración de la red inalámbrica

En este capítulo, se describe cómo configurar la red inalámbrica del dispositivo.

Seguridad inalámbrica

Las redes inalámbricas son prácticas y fáciles de instalar; por lo tanto, pequeñas empresas y hogares con acceso a Internet de alta velocidad las están adoptando cada vez más rápido.

Debido a que la red inalámbrica opera mediante el envío de información a través de ondas de radio, puede ser más vulnerable a intrusos que una red alámbrica tradicional.

Consejos para la seguridad inalámbrica

No puede evitar físicamente que alguien se conecte a la red inalámbrica, pero puede tomar las siguientes medidas para mantener la red segura:

- Cambie el nombre de la red inalámbrica predeterminado o el SSID.

  Los dispositivos inalámbricos tienen un nombre de red inalámbrica o un SSID predeterminados. Este es el nombre de la red inalámbrica y puede tener hasta 32 caracteres de longitud.

Para proteger la red, cambie el nombre de la red inalámbrica predeterminado a un nombre único para distinguir la red inalámbrica de otras redes inalámbricas que puedan existir alrededor suyo.

Cuando elija los nombres, no utilice información personal (por ejemplo, su número de seguro social), porque esta información puede ser vista por cualquier persona cuando está buscando redes inalámbricas.

- Cambie la contraseña predeterminada.

  Cuando desea cambiar la configuración de los productos inalámbricos, como puntos de acceso, routers y puertas de enlace, se le pide una contraseña. Estos dispositivos tienen una contraseña predeterminada. La contraseña predeterminada generalmente es **cisco**.

  Los hackers conocen estos valores predeterminados y es posible que intenten usarlos para acceder al dispositivo inalámbrico y cambiar las configuraciones de la red. Para impedir el acceso no autorizado, personalice la contraseña del dispositivo, de modo que sea difícil de adivinar.

- Habilite el filtrado de direcciones MAC.

  Las puertas de enlace y los routers Cisco le permiten habilitar el filtrado de direcciones MAC. La dirección MAC es una serie única de números y letras asignada a cada dispositivo de redes.

  Con el filtrado de direcciones MAC habilitado, el acceso a la red inalámbrica se proporciona únicamente para los dispositivos inalámbricos con direcciones MAC específicas. Por ejemplo, puede especificar la dirección MAC de cada computadora en la red, de modo que solo esas computadoras puedan acceder a la red inalámbrica.

- Habilite el cifrado.

  El cifrado protege los datos transmitidos por una red inalámbrica. El acceso Wi-Fi protegido (WPA/WPA2) y el protocolo de equivalencia de cableado (WEP) ofrecen distintos niveles de seguridad para la comunicación inalámbrica. Actualmente, se requiere que los dispositivos que poseen certificado Wi-Fi admitan WPA2, pero no se requiere que admitan WEP.

  Una red cifrada con WPA/WPA2 es más segura que una red cifrada con WEP, ya que WPA/WPA2 usa el cifrado de clave dinámica.

  Para proteger la información cuando se transmite a través de las ondas de transmisión, habilite el nivel más alto de cifrado que admite el equipo de la red.

  WEP es un cifrado estándar más antiguo y es posible que sea la única opción disponible en algunos dispositivos más antiguos que no admiten WPA.

- Mantenga los routers, los puntos de acceso o las puertas de enlace inalámbricos lejos de paredes exteriores y ventanas.
- Apague los routers, los puntos de acceso o las puertas de enlace inalámbricos cuando no estén en uso (a la noche, durante las vacaciones).
- Utilice frases clave sólidas que tengan, por lo menos, ocho caracteres de longitud. Combine letras y números para evitar utilizar palabras clásicas que pueden encontrarse en el diccionario.

Pautas generales para la seguridad de la red

La seguridad de la red inalámbrica no tiene utilidad si la red subyacente no está segura. Cisco recomienda que tome las siguientes precauciones:

- Proteja todas las computadoras de la red con contraseñas y, de forma individual, proteja con contraseña los archivos confidenciales.
- Cambie las contraseñas regularmente.
- Instale un software antivirus y un software de firewall personal.
- Deshabilite el uso compartido de archivos (entre entidades pares) para evitar que las aplicaciones utilicen el uso compartido de archivos sin su consentimiento.

Redes inalámbricas de Cisco RV215W

El dispositivo proporciona cuatro redes inalámbricas virtuales o cuatro SSID (identificador de conjunto de servicios): ciscosb1, ciscosb2, ciscosb3 y ciscosb4. Estos son los nombres o los SSID predeterminados de estas redes, pero puede cambiarlos a nombres más significativos. En esta tabla, se describen las configuraciones predeterminadas de estas redes:

Nombre de SSID	ciscosb1	ciscosb2	ciscosb3	ciscosb4
Habilitado	Sí	No	No	No
Difusión de SSID	Habilitado	Deshabilitado	Deshabilitado	Deshabilitado

Nombre de SSID	ciscosb1	ciscosb2	ciscosb3	ciscosb4
Modo de seguridad	Deshabilitado[1]	Deshabilitado	Deshabilitado	Deshabilitado
Filtro MAC	Deshabilitado	Deshabilitado	Deshabilitado	Deshabilitado
VLAN	1	1	1	1
Aislamiento inalámbrico con SSID	Deshabilitado	Deshabilitado	Deshabilitado	Deshabilitado
WMM	Habilitado	Habilitado	Habilitado	Habilitado
Botón de hardware WPS	Habilitado	Deshabilitado	Deshabilitado	Deshabilitado

1. Cuando use el Asistente de instalación, seleccione Seguridad óptima o Seguridad mejorada para proteger el dispositivo del acceso no autorizado.

Configuración de las opciones inalámbricas básicas

Puede utilizar la página **Configuración básica** (**Inalámbrica** > **Configuración básica**) para configurar las opciones inalámbricas básicas.

Para configurar las opciones inalámbricas básicas:

PASO 1 Elija **Inalámbrica** > **Configuración básica**.

PASO 2 En el campo **Radio**, marque **Habilitar** para encender la radio inalámbrica. De forma predeterminada, hay una sola red inalámbrica habilitada, **ciscosb1**.

PASO 3 En el campo **Modo de red inalámbrica**, elija una de estas opciones en el menú desplegable:

B/G/N-Combinado	Elija esta opción si tiene dispositivos inalámbricos N, B y G en la red. Este es el valor predeterminado (recomendado).

Solo B	Elija esta opción si tiene solo dispositivos inalámbricos B en la red.
Solo G	Elija esta opción si tiene solo dispositivos inalámbricos G en la red.
Solo N	Elija esta opción si tiene solo dispositivos inalámbricos N en la red.
B/G-Combinado	Elija esta opción si tiene dispositivos inalámbricos B y G en la red.
G/N-Combinado	Elija esta opción si tiene dispositivos inalámbricos G y N en la red.

PASO 4 Si elige **B/G/N-combinado**, **Solo N** o **G/N-combinado**, en el campo **Selección de banda inalámbrica**, seleccione el ancho de banda inalámbrica de la red (**20 MHz** o **20/40 MHz**). Si elige Solo N, debe usar seguridad WPA2 en la red. Consulte **Configuración del modo de seguridad**.

PASO 5 En el campo **Canal inalámbrico**, elija el canal inalámbrico en el menú desplegable.

PASO 6 En el campo **VLAN de administración AP**, elija **VLAN 1** si utiliza los valores predeterminados.

Si crea VLAN adicionales, elija un valor que corresponda con la VLAN configurada en otros switches de la red. Esto se realiza para propósitos de seguridad. Es posible que necesite cambiar la VLAN de administración para limitar el acceso al Administrador de dispositivos de dispositivo.

PASO 7 (Opcional) En el campo **U-APSD (ahorro de energía WMM)**, active la casilla **Habilitar** para habilitar la función de ahorro de energía automático no programado (U-APSD), también conocida como ahorro de energía WMM, que le permite a la radio conservar energía.

U-APSD es un esquema de ahorro de energía optimizado para aplicaciones en tiempo real, como VoIP, que transfieren datos de dúplex completo a través de WLAN. Al clasificar el tráfico IP saliente como datos de Voz, estos tipos de aplicación pueden aumentar la vida útil de la batería en un 25% aproximadamente y minimizar los retrasos de transmisión.

PASO 8 (Opcional) Configure las opciones de las cuatro redes inalámbricas (consulte **Edición de las opciones de las redes inalámbricas**).

PASO 9 Haga clic en **Guardar**.

Edición de las opciones de las redes inalámbricas

La **Tabla inalámbrica** en la página **Configuración básica** (**Inalámbrica** > **Configuración básica**) enumera las opciones de las cuatro redes inalámbricas que admite el dispositivo.

Para configurar las opciones de las redes inalámbricas:

PASO 1 Active la casilla de las redes que desea configurar.

PASO 2 Haga clic en el botón **Editar**.

PASO 3 Configure estas opciones:

Habilitar SSID	Haga clic en **Encendido** para habilitar la red.
Nombre de SSID	Escriba el nombre de la red.
Difusión de SSID	Active esta casilla para habilitar la difusión de SSID. Si la difusión SSID está habilitada, el router inalámbrico anuncia su disponibilidad a los dispositivos inalámbricos que se encuentran en el rango del router.
VLAN	Elija la VLAN asociada con la red.
Aislamiento inalámbrico con SSID	Active esta casilla para habilitar el aislamiento inalámbrico en la SSID.
WMM (Wi-Fi Multimedia)	Active esta casilla para habilitar WMM.
Botón de hardware WPS	Active esta casilla para asignar a la red el botón WPS del dispositivo que se encuentra en el panel frontal.

PASO 4 Haga clic en **Guardar**.

Configuración del modo de seguridad

Puede configurar uno de los siguientes modos de seguridad para las redes inalámbricas.

Configuración de WEP

El modo de seguridad WEP ofrece una seguridad débil con un método de cifrado básico que no es tan seguro como WPA. Es posible que se deba utilizar WEP en caso de que sus dispositivos de red no admitan WPA.

NOTA Si no debe utilizar WEP, le recomendamos que utilice WPA2. Si está usando el modo Solo N inalámbrico, debe usar WPA2.

Para configurar el modo de seguridad WEP:

PASO 1 En la **Tabla inalámbrica** (**Wireless** [Red inalámbrica] > **Basic Settings** [Configuración básica]), marque la casilla de la red que desea configurar.

PASO 2 Haga clic en **Editar modo de seguridad**.

Aparece la página **Configuración de seguridad**.

PASO 3 En el campo **Seleccionar SSID**, elija la SSID para la que se deben configurar las opciones de seguridad.

PASO 4 En el menú **Modo de seguridad**, elija **WEP**.

PASO 5 En el campo **Tipo de autenticación**, elija una de las siguientes opciones:

- **Sistema abierto**: esta es la opción predeterminada.
- **Clave compartida**: seleccione esta opción si el administrador de la red recomienda esta configuración. Si no está seguro, seleccione la opción predeterminada.

En ambos casos, el cliente inalámbrico debe proporcionar la clave compartida correcta (contraseña) para acceder a la red inalámbrica.

PASO 6 En el campo **Cifrado**, elija el tipo de cifrado:

- **10/64 bits (10 dígitos hexadecimales):** proporciona una clave de 40 bits.
- **26/128-bit(26 hex digits)** (26/128 bits [26 dígitos hexadecimales]): proporciona una clave de 104 bits, que ofrece un cifrado más sólido, de modo que se genera una clave más difícil de descodificar. Recomendamos un cifrado de 128 bits.

PASO 7 (Opcional) En el campo **Passphrase** (Frase clave), escriba una frase alfanumérica (que tenga más de ocho caracteres para lograr una seguridad óptima) y haga clic en **Generate Key** (Generar clave) para generar cuatro claves WEP únicas en los campos de claves WEP.

Si desea proporcionar su propia clave, ingrésela directamente en el campo **Clave 1** (recomendado). La longitud de la clave debe ser de 5 caracteres ASCII (o 10 caracteres hexadecimales) para una clave WEP de 64 bits y de 13 caracteres ASCII (o 26 caracteres hexadecimales) para una clave WEP de 128 bits. Los caracteres hexadecimales válidos son de 0 a 9 y de A a F.

PASO 8 En el campo **Clave TX**, elija qué clave utilizar como la clave compartida que deben utilizar los dispositivos para acceder a la red inalámbrica.

PASO 9 Haga clic en **Guardar** para guardar la configuración.

PASO 10 Haga clic en **Atrás** para volver a la página **Configuración básica**.

Configuración de WPA-Personal, WPA2-Personal y WPA2-Personal combinado

Los modos de seguridad de WPA Personal, WPA2 Personal y WPA2 Personal combinado ofrecen una seguridad fuerte para reemplazar a WEP.

- **WPA-Personal**: WPA es parte de la norma de seguridad inalámbrica (802.11i) estandarizada mediante Wi-Fi Alliance; estaba destinada como una medida intermedia para tomar el lugar de WEP mientras se preparaba el estándar 802.11i. WPA-Personal admite el protocolo de integridad de clave temporal (TKIP) y el cifrado de norma de cifrado avanzado (AES).
- **WPA2-Personal**: (recomendado) WPA2 es la implementación del estándar de seguridad especificado en el estándar 802.11i final. WPA2 admite el cifrado AES y esta opción utiliza la clave precompartida (PSK) para la autenticación.
- **WPA2-Personal combinado**: le permite utilizar los clientes WPA y WPA2 para conectarlos simultáneamente mediante la autenticación de PSK.

La autenticación personal es la PSK, una frase clave alfanumérica compartida con un par inalámbrico.

Para configurar el modo de seguridad de WPA Personal:

PASO 1 En la **Tabla inalámbrica** (**Inalámbrica** > **Configuración básica**), active la casilla de la red que desea configurar.

PASO 2 Haga clic en **Editar modo de seguridad**. Aparece la página **Configuración de seguridad**.

PASO 3 En el campo **Seleccionar SSID**, elija la SSID para la que se deben configurar las opciones de seguridad.

PASO 4 En el menú **Modo de seguridad**, elija una de las tres opciones de WPA Personal.

PASO 5 (Solo WPA-Personal) En el campo **Cifrado**, elija una de las siguientes opciones:

- **TKIP/AES**: elija **TKIP/AES** para garantizar la compatibilidad con dispositivos inalámbricos más antiguos que es posible que no admitan AES.
- **AES**: esta opción es más segura.

PASO 6 En el campo **Clave de seguridad**, escriba una frase alfanumérica (de 8 a 63 caracteres ASCII o de 64 dígitos hexadecimales). El medidor de seguridad de la contraseña muestra cuán segura es la clave: Por debajo del mínimo, débil, fuerte, muy fuerte o segura. Se recomienda el uso de una clave de seguridad que el medidor de seguridad registre como segura.

PASO 7 Para mostrar la clave de seguridad como la ingresa, marque la casilla **Exponer contraseña**.

PASO 8 En el campo **Renovación de clave**, escriba el período de tiempo (de 600 a 7200 segundos) entre las renovaciones de claves. El valor predeterminado es 3600.

PASO 9 Haga clic en **Guardar** para guardar la configuración.

PASO 10 Haga clic en **Atrás** para volver a la página **Configuración básica**.

Configuración de WPA-Enterprise, WPA2-Enterprise y WPA2-Enterprise combinado

Los modos de seguridad de WPA Enterprise, WPA2 Enterprise y WPA2 Enterprise combinado le permiten utilizar la autenticación del servidor RADIUS.

- **WPA-Enterprise**: le permite utilizar WPA con la autenticación del servidor RADIUS.
- **WPA2-Enterprise**: le permite utilizar WPA2 con la autenticación del servidor RADIUS.
- **WPA2-Enterprise combinado**: le permite utilizar los clientes WPA y WPA2 para conectarlos simultáneamente mediante la autenticación de RADIUS.

Para configurar el modo de seguridad de WPA Enterprise:

PASO 1 En la **Tabla inalámbrica** (**Inalámbrica** > **Configuración básica**), active la casilla de la red que desea configurar.

PASO 2 Haga clic en **Editar modo de seguridad**.

PASO 3 En el campo **Seleccionar SSID**, elija la SSID para la que se deben configurar las opciones de seguridad.

PASO 4 En el menú **Modo de seguridad**, elija una de las tres opciones de WPA Enterprise.

PASO 5 (Solo WPA-Enterprise) En el campo **Cifrado**, elija una de las siguientes opciones:

- **TKIP/AES**: elija **TKIP/AES** para garantizar la compatibilidad con dispositivos inalámbricos más antiguos que es posible que no admitan AES.
- **AES**: esta opción es más segura.

PASO 6 En el campo **Servidor RADIUS**, escriba la dirección IP del servidor RADIUS.

PASO 7 En el campo **Puerto RADIUS**, escriba el puerto que se utiliza para acceder al servidor RADIUS.

PASO 8 En el campo **Shared Key** (Clave compartida), escriba una frase alfanumérica.

PASO 9 En el campo **Renovación de clave**, escriba el período de tiempo (de 600 a 7200 segundos) entre las renovaciones de claves. El valor predeterminado es 3600.

PASO 10 Haga clic en **Guardar** para guardar la configuración.

PASO 11 Haga clic en **Atrás** para volver a la página **Configuración básica**.

Configuración del filtrado MAC

Puede utilizar el filtrado MAC para permitir o rechazar el acceso a la red inalámbrica con base en la dirección (hardware) MAC del dispositivo solicitante. Por ejemplo, puede escribir las direcciones MAC de un conjunto de computadoras y solo permitirles el acceso a la red a esas computadoras. Puede configurar el filtrado MAC para cada red o SSID.

Para configurar el filtrado MAC:

PASO 1 En la **Tabla inalámbrica** (**Inalámbrica** > **Configuración básica**), active la casilla de la red que desea configurar.

PASO 2 Haga clic en **Editar filtrado MAC**. Se abre la página **Filtrado MAC inalámbrico**.

PASO 3 En el campo **Editar filtrado MAC**, active la casilla **Habilitar** para habilitar el filtrado MAC para esta SSID.

PASO 4 En el campo **Control de conexión**, elija el tipo de acceso a la red inalámbrica:

- **Impedir**: seleccione esta opción para impedir que las direcciones MAC enumeradas en la **Tabla de direcciones MAC** accedan a la red inalámbrica. Esta opción se selecciona de forma predeterminada.
- **Permitir**: seleccione esta opción para permitir que las direcciones MAC enumeradas en la **Tabla de direcciones MAC** accedan a la red inalámbrica.

PASO 5 Para mostrar las computadoras y otros dispositivos de la red inalámbrica, haga clic en **Mostrar lista de clientes**.

PASO 6 En el campo **Save to MAC Address Filter List** (Guardar en lista de filtros de dir. MAC), marque la casilla para agregar el dispositivo a la lista de dispositivos que se agregarán a la **Tabla de direcciones MAC**.

PASO 7 Haga clic en **Agregar a MAC** para agregar los dispositivos seleccionados en la **Tabla de lista de clientes** a la **Tabla de direcciones MAC**.

PASO 8 Haga clic en **Guardar** para guardar la configuración.

PASO 9 Haga clic en **Atrás** para volver a la página **Configuración básica**.

Configuración del acceso de hora del día

Para proteger más la red, puede restringir su acceso al especificar cuándo los usuarios pueden acceder a la red.

Para configurar el acceso de hora del día:

PASO 1 En la **Tabla inalámbrica** (**Inalámbrica** > **Configuración básica**), active la casilla de la red que desea configurar.

PASO 2 Haga clic en **Acceso de hora del día**. Aparece la página Acceso de hora del día.

PASO 3 En el campo **Hora activa**, active la casilla **Habilitar** para habilitar el acceso de hora del día.

PASO 4 En los campos **Hora de inicio** y **Hora de finalización**, especifique el período durante el cual está permitido el acceso a la red.

PASO 5 Haga clic en **Guardar**.

Configuración de la red de invitados inalámbrica

El dispositivo admite una red de invitados inalámbrica que está separada de los otros SSID o redes inalámbricas del router. Este router brinda acceso seguro a los invitados que se encuentra aislado del resto de la red y se puede configurar para restringir el tiempo de acceso y el ancho de banda utilizado. Se aplican las siguientes restricciones y pautas de configuración:

- Se puede configurar una red de invitado para cada dispositivo.
- La red de invitado se configura como uno de los cuatro SSID disponibles en el dispositivo.
- La red de invitado no se puede configurar en la VLAN de administración AP (VLAN ID 1).

Para configurar la red de invitado, haga lo siguiente:

Cree una VLAN nueva.

PASO 1 En la Interfaz de administración, seleccione **Conexión de red** > **LAN** > **Afiliación VLAN.**

PASO 2 En la Tabla de config. de VLAN, agregue una VLAN nueva para la red de invitado. Por ejemplo, haga clic en **Agregar fila** e introduzca lo siguiente:

- **ID de VLAN**: introduzca un número para la VLAN (por ejemplo, **4**).
- **Descripción**: introduzca un nombre para la VLAN (por ejemplo, **red de invitado**).

PASO 3 Deje los puertos como **etiquetado** y haga clic en **Guardar**.

Configuración de la red de invitado

PASO 1 En la Interfaz de administración, seleccione **Red inalámbrica** > **Configuración básica**.

PASO 2 En la Tabla inalámbrica, seleccione el SSID o la red que desea designar como red de invitado.

PASO 3 Haga clic en **Editar**. Cambie el nombre del SSID para reflejar la designación de invitado (por ejemplo, *red de invitado*).

PASO 4 Haga clic en la casilla **Difusión de SSID** para que la red aparezca como una conexión inalámbrica disponible para los clientes que busquen redes.

PASO 5 Marque la casilla **Red de invitado** para configurar este SSID como red de invitado.

PASO 6 Seleccione la VLAN que creó para la red de invitado (o, si todavía no ha creado una red, seleccione **Agregar VLAN nueva**).

PASO 7 Haga clic en **Guardar**. El sistema le notifica que los puertos físicos Ethernet del dispositivo están excluidos de la VLAN que asignó a la red de invitado. Además, se activa automáticamente el aislamiento inalámbrico con SSID y WMM.

Configure la contraseña y demás opciones.

PASO 1 En la Interfaz de administración, seleccione **Red inalámbrica** > **Configuración básica**.

PASO 2 En la Tabla inalámbrica, haga clic en **Edit Guest Net** (Editar red de invitado).

PASO 3 Introduzca una contraseña; los usuarios introducirán esta contraseña para tener acceso a la red de invitado.

PASO 4 Escriba una vez más la contraseña para confirmarla.

PASO 5 Introduzca el tiempo, en minutos, durante el cual la conexión de invitado estará disponible para los invitados.

PASO 6 (Opcional) Para restringir el uso del ancho de banda según la red de invitado, marque **Enable Guest Bandwidth Restriction** (Habilitar restricción de ancho de banda de invitado). (Primero debe habilitarse la Qos; haga clic en el enlace hacia la página Administración del ancho de banda si debe configurar la Qos). En el campo **Available Bandwidth** (Ancho de banda disponible), ingrese el porcentaje de ancho de banda que asignará a la red de invitado.

PASO 7 Haga clic en **Guardar**.

Configuración de las opciones inalámbricas avanzadas

Las opciones inalámbricas avanzadas deben ajustarse únicamente por un administrador experto; las opciones incorrectas pueden reducir el rendimiento inalámbrico.

Para configurar las opciones inalámbricas avanzadas:

PASO 1 Elija **Inalámbrica** > **Configuración avanzada**. Aparece la página Configuración avanzada.

PASO 2 Configure estas opciones:

Ráfaga de trama	Habilite esta opción para que las redes inalámbricas tengan un mayor rendimiento, según el fabricante de los productos inalámbricos. Si no está seguro de cómo se utiliza esta opción, mantenga la opción predeterminada (habilitada).
Sin reconocimiento WMM	Haga clic para habilitar esta función. Al habilitar la opción Sin reconocimiento WMM, se puede obtener un rendimiento más eficiente, pero puede generar tasas de error más altas en un entorno de radiofrecuencia (RF). La configuración predeterminada es deshabilitada.
Velocidad básica	La configuración de la velocidad básica no es la velocidad de la transmisión, pero se trata de una serie de velocidades que Services Ready Platform puede transmitir. El dispositivo anuncia su velocidad básica a los dispositivos inalámbricos de la red para que sepan qué velocidades se utilizarán. La Services Ready Platform también anunciará que seleccionará de forma automática la mejor velocidad de transmisión. La configuración predeterminada es Predeterminada, en la cual el dispositivo puede transmitir a todas las velocidades inalámbricas estándar (1 Mbps, 2 Mbps, 5,5 Mbps, 11 Mbps, 18 Mbps, 24 Mbps, 36 Mbps, 48 Mbps y 54 Mbps). Además de las velocidades de B y G, el dispositivo admite la velocidad de N. Las otras opciones son de 1 a 2 Mbps cuando se lo utiliza con tecnología inalámbrica más antigua, y la opción Todo, cuando el dispositivo puede transmitir a todas las velocidades inalámbricas. La velocidad básica no es la velocidad real de la transmisión de datos. Si desea especificar la velocidad de la transmisión de datos del dispositivo, configure las opciones de la velocidad de transmisión.

Velocidad de transmisión	La velocidad de la transmisión de datos debe configurarse según la velocidad de la red inalámbrica. Puede seleccionar entre un rango de velocidades de transmisión o puede seleccionar **Automática** para que el dispositivo utilice de forma automática la velocidad de datos más rápida posible y para que habilite la función de repliegue automático. El repliegue automático negociará la mejor velocidad de conexión posible entre el dispositivo y un cliente inalámbrico. El modo predeterminado es Automática.
Velocidad de transmisión N	La velocidad de la transmisión de datos debe configurarse según la velocidad de las redes inalámbricas N. Puede seleccionar entre un rango de velocidades de transmisión o puede seleccionar **Automática** para que el dispositivo utilice de forma automática la velocidad de datos más rápida posible y para que habilite la función de repliegue automático. El repliegue automático negociará la mejor velocidad de conexión posible entre el dispositivo y un cliente inalámbrico. El modo predeterminado es Automática.
Modo de protección CTS	El dispositivo utilizará de forma automática el modo de protección CTS (Habilitar para enviar) cuando sus dispositivos inalámbricos N y G tengan problemas y no puedan transmitir al dispositivo en un entorno con tráfico de 802.11b pesado. Esta función aumenta la capacidad del dispositivo para capturar todas las transmisiones inalámbricas N y G, pero provocará una gran disminución en el rendimiento. El modo predeterminado es Automática.
Intervalo de señales	El valor de Intervalo de señales indica el intervalo de frecuencia de la baliza. Una baliza es un paquete que transmite el dispositivo para sincronizar la red inalámbrica. Escriba un valor entre 40 y 3500 milisegundos. El valor predeterminado es 100.

Intervalo DTIM	Este valor, entre 1 y 255, indica el intervalo del mensaje de indicación del tráfico de entrega (DTIM). Un campo DTIM es un campo de cuenta regresiva que informa a los clientes de la siguiente ventana para escuchar los mensajes de multidifusión y difusión. Cuando el dispositivo ha almacenado en el búfer mensajes de multidifusión y difusión para los clientes asociados, envía el siguiente DTIM con un valor de intervalo DTIM. Sus clientes escuchan las balizas y se activan para recibir los mensajes de multidifusión y difusión. El valor predeterminado es 1.
Umbral de fragmentación	Este valor especifica el tamaño máximo de un paquete antes de que se fragmenten los datos en varios paquetes. Si tiene una alta tasa de error de paquete, puede aumentar ligeramente el umbral de fragmentación. Habilitar el umbral de fragmentación a un nivel muy bajo puede provocar un mal rendimiento de la red. Se recomienda solo una ligera reducción del valor predeterminado. En la mayoría de los casos, debe permanecer en su valor predeterminado de 2346.
Umbral RTS	Si encuentra un flujo de datos incoherente, escriba solo reducciones mínimas. Se recomienda el valor predeterminado de 2347. Si un paquete de red es más chico que el tamaño del umbral de Petición para enviar (RTS) predefinido, no se habilitará el mecanismo de RTS/Habilitar para enviar (CTS). Services Ready Platform envía las tramas de RTS a una estación de recepción particular y negocia el envío de las tramas de datos. Después de recibir una RTS, la estación inalámbrica responde con una trama de CTS para reconocer el permiso de comenzar con la transmisión.

PASO 3 Haga clic en **Guardar**.

Configuración de WDS

Un sistema de distribución inalámbrica (WDS) es un sistema que habilita la interconexión inalámbrica de puntos de acceso en una red. Permite que una red inalámbrica se expanda mediante varios puntos de acceso sin la necesidad de utilizar la estructura básica de cableado para conectarlos.

Para establecer un enlace de WDS, se deben configurar el dispositivo y otros pares remotos de WDS en el mismo modo inalámbrico, canal inalámbrico, selección de banda inalámbrica y tipos de cifrado (Ninguno y WEP).

WDS solo se admite en un SSID.

Para configurar un WDS:

PASO 1 Elija **Inalámbrica** > **WDS**.

PASO 2 Active la casilla **Permitir que un repetidor repita la señal inalámbrica** para habilitar WDS.

PASO 3 Para ingresar manualmente la dirección MAC de un repetidor, haga clic en **Manual**, o elija **Automático** para que el router detecte automáticamente los puntos de acceso remoto.

Para seleccionar los repetidores desde la tabla de Redes disponibles, haga clic en **Show Site Survey** (Mostrar sondeo del sitio) para mostrar la **Tabla de redes disponibles**.

a. Haga clic en las casillas de verificación para seleccionar hasta tres puntos de acceso para usar como repetidores.

b. Haga clic en **Connect** (Conectar) para añadir direcciones MAC de los puntos de acceso seleccionados al campo MAC.

También puede ingresar las direcciones MAC hasta de tres puntos de acceso para usar como repetidores en los campos **MAC 1**, **MAC 2** y **MAC 3**.

PASO 4 Haga clic en **Guardar**.

Configuración de WPS

Configure WPS para permitir que los dispositivos compatibles con WPS puedan conectarse fácilmente y de manera segura a la red inalámbrica. Consulte el dispositivo cliente o su documentación para obtener más instrucciones sobre cómo configurar WPS en el dispositivo cliente.

Para configurar WPS:

PASO 1 Elija **Inalámbrica** > **WPS**. Aparece la página Wi-Fi Protected Setup (Configuración de Wi-Fi protegida).

PASO 2 En el menú desplegable de **SSID**, elija la red inalámbrica en la cual habilitará WPS.

PASO 3 Marque la casilla **Habilitar WPS** para habilitar el WPS. Para deshabilitar WPS, desactive la casilla.

PASO 4 Configure la WPS en los dispositivos cliente en una de las siguientes tres maneras:

a. Haga clic o presione el botón WPS en el dispositivo de cliente y luego haga clic sobre el ícono WPS en esta página.

b. Ingrese el número de PIN WPS del cliente y haga clic en **Registrar**.

c. Ingrese un número de PIN para el router; use el número de PIN indicado del router.

Device PIN Status (Estado del PIN del dispositivo): estado del número de identificación personal (PIN) del dispositivo WPA.

Device PIN (PIN de dispositivo): identifica el PIN de un dispositivo que intenta conectarse.

PIN Lifetime (Duración del PIN): duración de la clave. Si el tiempo caduca, se negociará una nueva red.

Después de configurar WPS, la siguiente información aparece en la parte inferior de la página **WPS**: Estado de Wi-Fi Protected Setup, nombre de la red (SSID) y seguridad.

5

Configuración del firewall

En este capítulo, se describe cómo configurar las propiedades del firewall del dispositivo

- **Características del firewall de Cisco RV215W**
- **Configuración de los parámetros básicos de firewall**
- **Administración de las programaciones de firewall**
- **Configuración de la administración de servicios**
- **Configuración de reglas de acceso**
- **Creación de la política de acceso a Internet**
- **Configuración de reenvío de puertos**

Características del firewall de Cisco RV215W

Puede asegurar su red mediante la creación y aplicación de las reglas que utiliza el dispositivo para bloquear y permitir de manera selectiva el tráfico de Internet entrante y saliente. A continuación, especifique cómo y a qué dispositivos se aplican las reglas. Para hacerlo, debe definir lo siguiente:

- Los servicios o tipos de tráfico (ejemplos: navegación web, VoIP, otros servicios estándares y también los servicios personalizados que usted defina) que el router debe permitir o bloquear.
- La dirección del tráfico al especificar el origen y el destino del tráfico; esto se realiza al especificar la Zona de origen (LAN/WAN/DMZ) y la Zona de destino (LAN/WAN/DMZ).
- Las programaciones cuando el router debe aplicar las reglas.
- Las palabras clave (en un nombre de dominio o en una URL de una página web) que el router debe permitir o bloquear.

- Las reglas para permitir o bloquear el tráfico de Internet entrante y saliente para los servicios especificados en las programaciones especificadas.
- Las direcciones MAC de los dispositivos cuyo acceso entrante a la red el router debe bloquear.
- El puerto activa esa señal para que el router permita o bloquee el acceso a determinados servicios definidos por el número de puerto.
- Los informes y las alertas que desea que el router le envíe.

Por ejemplo, puede establecer las políticas de acceso restringido de acuerdo con la hora del día, las direcciones web y las palabras clave de las direcciones web. Puede bloquear el acceso a Internet mediante las aplicaciones y los servicios en la red LAN, como salas de conversación o juegos. Puede bloquear el acceso desde la red DMZ pública o WAN solo a ciertos grupos de PC.

Las reglas (WAN a LAN/DMZ) entrantes restringen el acceso al tráfico que ingresa en la red, de modo que permiten, de manera selectiva, que solo determinados usuarios externos accedan a los recursos locales específicos. De forma predeterminada, se bloquea todo acceso desde la red WAN no segura a la red LAN segura, excepto en respuesta a solicitudes desde LAN o DMZ. Para permitir que los dispositivos externos accedan a servicios en la LAN segura, debe crear una regla de firewall para cada servicio.

Si desea permitir el tráfico entrante, debe dar a conocer al público la dirección IP del puerto WAN del router. Esto se denomina exposición de su host. La manera en que da a conocer su dirección depende de cómo están configurados los puertos WAN. Para su dispositivo, puede usar la dirección IP si existe una dirección estática asignada al puerto WAN; si su dirección WAN es dinámica, se puede usar un nombre DDNS (DNS dinámico).

Las reglas (LAN/DMZ a WAN) salientes restringen el acceso al tráfico que sale de la red, de modo que permiten, de manera selectiva, que solo determinados usuarios locales accedan a los recursos externos específicos. La regla saliente predeterminada permite el acceso de la zona segura (LAN) a la red DMZ pública o WAN no segura. Para bloquear el acceso de los hosts en la LAN segura a servicios desde el exterior (WAN no segura), debe crear una regla de firewall para cada servicio.

Configuración de los parámetros básicos de firewall

Para configurar los parámetros básicos de firewall:

PASO 1 Elija **Firewall** > **Configuración básica**.

PASO 2 Configure los siguientes parámetros de firewall:

Firewall	Active **Habilitar** para configurar los parámetros de firewall.
Protección contra DoS	Active **Habilitar** para habilitar la protección de denegación de servicio.
Bloquear solicitud WAN	Bloquea las solicitudes de ping al dispositivo desde la WAN.
Acceso web	Elija el tipo de acceso web que se puede utilizar para conectarse al firewall: HTTP o HTTPS (HTTP seguro).
Administración remota **Acceso remoto** **Actualización remota** **Dirección IP remota permitida** **Puerto de admin. remota**	Consulte **Configuración de la administración remota**.
Transmisión de multidifusión IPv4 (Proxy IGMP)	Active **Habilitar** para habilitar la transmisión de multidifusión para IPv4.
Transmisión de multidifusión IPv6 (Proxy IGMP)	Active **Habilitar** para habilitar la transmisión de multidifusión para IPv6.
UPnP **Permitir a usuarios configurar** **Permitir a usuarios deshabilitar acceso a Internet**	Consulte **Configuración de Universal Plug and Play**.

Bloquear Java	Active para bloquear los applets de Java. Los applets de Java son pequeños programas integrados en páginas web que habilitan la funcionalidad dinámica de la página. Se puede utilizar un applet malicioso para comprometer o infectar computadoras. La habilitación de este parámetro no permite que se descarguen los applets de Java. Haga clic en **Automático** para bloquear automáticamente Java o haga clic en **Manual** y escriba un puerto específico en el cual bloquear Java.
Bloquear cookies	Active para bloquear las cookies. Los sitios web que generalmente requieren inicio de sesión utilizan las cookies para guardar la información de la sesión. Sin embargo, muchos sitios web utilizan cookies para guardar la información de seguimiento y los hábitos de navegación. La habilitación de esta opción elimina las cookies que se creen mediante un sitio web. Muchos sitios web requieren que se acepten cookies para que se pueda acceder al sitio correctamente. El bloqueo de las cookies puede causar que muchos sitios web no funcionen correctamente. Haga clic en **Automático** para bloquear automáticamente las cookies o haga clic en **Manual** y escriba un puerto específico en el cual bloquear las cookies.
Bloquear ActiveX	Active para bloquear el contenido ActiveX. Similares a los applets de Java, los controles ActiveX se instalan en una computadora que ejecuta Windows mientras se ejecuta Internet Explorer. Se puede utilizar un control ActiveX malicioso para comprometer o infectar computadoras. La habilitación de este parámetro no permite que se descarguen los applets de ActiveX. Haga clic en **Automático** para bloquear automáticamente ActiveX o haga clic en **Manual** y escriba un puerto específico en el cual bloquear ActiveX.

Bloquear proxy	Active para bloquear los servidores proxy. Un servidor proxy (o proxy) permite que las computadoras enruten más conexiones a otras computadoras a través de proxy, eludiendo así ciertas reglas de firewall. Por ejemplo, si están bloqueadas las conexiones a una dirección IP específica mediante una regla de firewall, las solicitudes pueden enrutarse a través de un proxy que no está bloqueado por la regla, de modo que deja sin efecto la restricción. La habilitación de esta función bloquea los servidores proxy. Haga clic en **Automático** para bloquear automáticamente los servidores proxy o haga clic en **Manual** y escriba un puerto específico en el cual bloquear los servidores proxy.
ALG de FTP	Haga clic en **Auto** (Automático) para usar el puerto 21 predeterminado del FTP. Haga clic en **Manual** (Manual) para ingresar el número de puerto a través del cual desea dirigir el tráfico FTP en el dispositivo.

PASO 3 Haga clic en **Guardar**.

Configuración de la administración remota

Puede habilitar la administración remota para que pueda acceder al dispositivo desde una red WAN remota.

Para configurar la administración remota, configure estos parámetros en la página **Configuración básica**:

Administración remota	Marque **Habilitar** para habilitar la administración remota.
Acceso remoto	Elija el tipo de acceso web que se puede utilizar para conectarse al firewall: HTTP o HTTPS (HTTP seguro).
Actualización remota	Para permitir actualizaciones remotas del dispositivo, marque **Enable** (Habilitar).

Dirección IP remota permitida	Haga clic en el botón **Cualquier dir. IP** para permitir la administración remota desde cualquier dirección IP o escriba una dirección IP específica en el campo de direcciones.
Puerto de admin. remota	Escriba el puerto en el que está permitido el acceso remoto. El puerto predeterminado es 443. Al acceder remotamente al router, debe ingresar el puerto de admin. remota como parte de la dirección IP. Por ejemplo: **https://<ip-remota>:<puerto-remoto>**, o **https://168.10.1.11:443**

PRECAUCIÓN Cuando el acceso remoto está habilitado, cualquier persona que conozca la dirección IP puede acceder al router. Debido a que un usuario de WAN malintencionado puede volver a configurar el dispositivo y usarlo en forma incorrecta, se recomienda que cambie las contraseñas del administrador y de cualquier invitado antes de continuar.

Configuración de Universal Plug and Play

Universal Plug and Play (UPnP) permite la detección automática de dispositivos que se pueden comunicar con el dispositivo.

Para configurar UPnP, configure estos parámetros en la página **Configuración básica**:

UPnP	Marque la casilla **Habilitar** para habilitar UPnP.
Permitir a usuarios configurar	Active esta casilla para permitir que los usuarios que tienen el soporte de UPnP habilitado en las computadoras o en otros dispositivos habilitados para UPnP configuren las reglas de asignación de puerto para UPnP. Si está deshabilitada, el dispositivo no permite que la aplicación agregue la regla de reenvío.
Permitir a usuarios deshabilitar acceso a Internet	Active esta casilla para permitir que los usuarios deshabiliten el acceso a Internet.

Administración de las programaciones de firewall

Puede crear las programaciones de firewall para aplicar las reglas de firewall en días específicos o en horas específicas del día.

Incorporación o edición de una programación de firewall

Para crear o editar una programación:

PASO 1 Elija **Firewall** > **Programar administración**.

PASO 2 Haga clic en **Agregar fila**.

PASO 3 En el campo **Nombre**, escriba un nombre único para identificar la programación. Este nombre está disponible en la página Configuración de reglas de firewall en la lista **Seleccionar programación**. (Consulte **Configuración de reglas de acceso**).

PASO 4 En **Días programados**, seleccione si desea que la programación se aplique a todos los días o a días específicos. Si elige **Días específicos**, active la casilla que se encuentra al lado de los días que desea incluir en la programación.

PASO 5 En **Hora del día programada**, seleccione la hora del día en la cual desea que se aplique la programación. Puede elegir **A toda hora** o **A horas específicas**. Si elige **A horas específicas**, escriba las horas de inicio y finalización.

PASO 6 Haga clic en **Guardar**.

Configuración de la administración de servicios

Cuando crea una regla de firewall, puede especificar un servicio que está controlado por la regla. Los tipos comunes de servicio están disponibles para su selección, también puede crear sus propios servicios personalizados.

La página **Administración de servicio** le permite crear los servicios personalizados para los cuales se pueden definir las reglas de firewall. Una vez definido, el nuevo servicio aparece en la tabla **List of Available Custom Services** (Lista de servicios personalizados disponibles).

Para crear un servicio personalizado:

PASO 1 Elija **Firewall** > **Administración de servicio**.

PASO 2 Haga clic en **Agregar fila**.

PASO 3 En el campo **Nombre del servicio**, escriba el nombre del servicio para fines administrativos y de identificación.

PASO 4 En el campo **Protocolo**, elija el protocolo de capa 4 que utiliza el servicio en el siguiente menú desplegable:

- **TCP**
- **UDP**
- **TCP y UDP**
- **ICMP**

PASO 5 En el campo **Puerto de inicio**, escriba el primer puerto TCP o UDP del rango que utiliza el servicio.

PASO 6 En el campo **Puerto final**, escriba el último puerto TCP o UDP del rango que utiliza el servicio.

PASO 7 Haga clic en **Guardar**.

Para editar una entrada, seleccione la entrada y haga clic en **Editar**. Realice sus cambios y luego haga clic en **Guardar**.

Configuración de reglas de acceso

Configuración de política de salida predeterminada

La página **Reglas de acceso** le permite configurar la política de salida predeterminada del tráfico que se dirige de la red segura (LAN) a la red no segura (WAN dedicada/opcional).

La política de entrada predeterminada del tráfico que fluye de la zona no segura a la zona segura siempre está bloqueada y no se puede cambiar.

Para configurar la política de salida predeterminada:

PASO 1 Elija **Firewall** > **Reglas de acceso**.

PASO 2 Elija **Permitir** o **Rechazar**.

Nota: Asegúrese de que el soporte IPv6 esté habilitado en el dispositivo para configurar el firewall IPv6. Consulte **Configuración IPv6**.

PASO 3 Haga clic en **Guardar**.

Reorganización de las reglas de acceso

El orden en el que las reglas de acceso se muestran en la tabla de reglas de acceso indica el orden en el que se aplican. Es posible que desee reorganizar la tabla para que determinadas reglas se apliquen antes que otras. Por ejemplo, es posible que desee aplicar una regla que permita ciertos tipos de tráfico antes de bloquear otros tipos de tráfico.

Para reorganizar las reglas de acceso:

PASO 1 Elija **Firewall** > **Reglas de acceso**.

PASO 2 Haga clic en **Reorganizar**.

PASO 3 Marque la casilla que se encuentra en la fila de la regla que desea mover hacia arriba o hacia abajo y haga clic en la flecha arriba o en la flecha abajo para subir o bajar la regla una línea o seleccione la posición deseada para la regla en la lista desplegable y haga clic en **Mover a**.

PASO 4 Haga clic en **Guardar**.

Agregar reglas de acceso

Todas las reglas de firewall configuradas en el dispositivo se visualizan en la **Tabla de reglas de acceso**. Esta lista también indica si la regla está habilitada (activa) y proporciona un resumen de la zona de origen/destino, así como también los servicios y los usuarios a los que afecta la regla.

Para crear una regla de acceso:

PASO 1 Elija **Firewall** > **Reglas de acceso**.

PASO 2 Haga clic en **Agregar fila**.

PASO 3 En el campo **Tipo de conexión**, elija el origen del tráfico de origen:

- **Saliente (LAN > WAN)**: elija esta opción para crear una regla saliente.
- **Entrante (WAN > LAN)**: elija esta opción para crear una regla entrante.
- **Entrante (WAN > DMZ)**: elija esta opción para crear una regla entrante.

PASO 4 En el menú desplegable **Acción**, elija la acción:

- **Bloquear siempre**: siempre bloquea el tipo de tráfico seleccionado.
- **Permitir siempre**: nunca bloquea el tipo de tráfico seleccionado.
- **Bloquear por programación, permitir de otra forma**: bloquea el tipo de tráfico seleccionado de acuerdo con la programación.
- **Permitir por programación, bloquear de otra forma**: permite el tipo de tráfico seleccionado de acuerdo con la programación.

PASO 5 En el menú desplegable **Servicios**, elija el servicio a permitir o bloquear mediante esta regla. Elija **Todo el tráfico** para permitir que la regla se aplique a todas las aplicaciones y servicios, o elija una única aplicación para bloquear:

- Sistema de nombres de dominio (DNS), UDP o TCP
- Protocolo de transferencia de archivos (FTP)
- Protocolo de transferencia de hipertexto (HTTP)
- Protocolo de transferencia de hipertexto seguro (HTTPS)
- Protocolo trivial de transferencia de archivos (TFTP)
- Protocolo de acceso a mensajes por Internet (IMAP)
- Protocolo de transporte de noticias en red (NNTP)
- Protocolo de oficina de correos (POP3)
- Protocolo de administración de red simple (SNMP)
- Protocolo simple de transferencia de correo (SMTP)
- Telnet
- STRMWORKS
- Sistema de control de acceso al controlador de acceso al terminal (TACACS)
- Telnet (comando)
- Telnet secundario

- Telnet SSL
- Voz (SIP)

PASO 6 (Opcional) Haga clic en **Configurar servicios** para ir a la página **Administración de servicios** a fin de configurar los servicios antes de aplicarles las reglas de acceso.

Para obtener más información, consulte **Configuración de la administración de servicios**.

PASO 7 En el campo **IP de origen**, seleccione los usuarios a los que se les aplica la regla de firewall:

- **Cualquiera**: la regla se aplica al tráfico que se origina en cualquier host en la red local.
- **Dirección única**: la regla se aplica al tráfico que se origina en una dirección IP única en la red local. Escriba la dirección en el campo **Iniciar**.
- **Rango de direcciones**: la regla se aplica al tráfico que se origina en una dirección IP ubicada en un rango de direcciones. Escriba la dirección IP de inicio en el campo **Iniciar** y la dirección IP de finalización en el campo **Finalizar**.

PASO 8 En el campo **Registro**, especifique si deben registrarse los paquetes para esta regla.

Para registrar los detalles de todos los paquetes que coinciden con esta regla, elija **Siempre** en el menú desplegable. Por ejemplo, si una regla saliente para una programación está seleccionada como **Bloquear siempre**, para cada paquete que intente hacer una conexión saliente para ese servicio, se graba un mensaje en el registro con la dirección de origen y la dirección de destino del paquete (y más información).

La habilitación del registro puede generar un volumen significativo de mensajes de registro y se la recomienda para fines de depuración únicamente.

Elija **Nunca** para deshabilitar el registro.

NOTA Cuando el tráfico va desde LAN o DMZ a WAN, el sistema requiere que se vuelva a escribir la dirección IP de origen o destino de los paquetes IP entrantes a medida que pasan por el firewall.

PASO 9 En el campo **Prioridad de QoS**, asigne una prioridad a los paquetes IP de este servicio. Las prioridades se definen mediante el nivel de QoS: (**1 [más baja]**, **2**, **3** y **4 [más alta]**).

PASO 10 En el campo **Estado de la regla**, active la casilla para habilitar la nueva regla de acceso.

PASO 11 Haga clic en **Guardar**.

Creación de la política de acceso a Internet

El dispositivo admite varias opciones para bloquear el acceso a Internet. Puede bloquear todo el tráfico de Internet, bloquear el tráfico de Internet a ciertos equipos o puntos finales o bloquear el acceso a sitios de Internet al especificar palabras clave para bloquear. Si estas palabras clave se encuentran en el nombre del sitio (por ejemplo, el nombre del grupo de noticias o la dirección URL del sitio web), el sitio se bloquea.

Incorporación o edición de una política de acceso a Internet

Para crear una política de acceso a Internet:

PASO 1 Elija **Firewall** > **Política de acceso a Internet**.

PASO 2 Haga clic en **Agregar fila**.

PASO 3 En el campo **Estado**, marque **Habilitar**.

PASO 4 Escriba el nombre de una política para fines administrativos o de identificación.

PASO 5 En el menú desplegable **Acción**, elija el tipo de restricción de acceso que necesita:

- **Bloquear siempre**: bloquear siempre el tráfico de Internet. Esta opción bloquea el tráfico de Internet a puntos finales y de puntos finales. Si desea bloquear todo el tráfico pero permitir que ciertos puntos finales reciban tráfico de Internet, consulte el Paso 7.
- **Permitir siempre**: permitir siempre el tráfico de Internet. Puede redefinir esta opción para bloquear el tráfico de Internet de ciertos puntos finales; consulte el Paso 7. También puede permitir todo el tráfico de Internet excepto para ciertos sitios web; consulte el Paso 8.
- **Bloquear por programación**: bloquea el tráfico de Internet según una programación (por ejemplo, si desea bloquear el tráfico de Internet durante los días de semana en el horario de trabajo, pero permitirlo después del horario de trabajo y durante el fin de semana).
- **Permitir según programación**: permite tráfico de Internet según una programación.

Si elige **Bloquear por programación** o **Permitir por programación**, haga clic en **Configurar programaciones** para crear una programación. Consulte **Administración de las programaciones de firewall**.

PASO 6 Seleccione una programación en el menú desplegable.

PASO 7 (Opcional) Aplique la política de acceso a ciertos equipos para permitir o bloquear el tráfico proveniente de ciertos dispositivos:

a. En la tabla **Aplicar la política de acceso a los siguientes equipos**, haga clic en **Agregar fila**.

b. En el menú desplegable **Tipo**, elija cómo identificar la computadora (mediante una dirección MAC, una dirección IP o mediante la especificación de un rango de direcciones IP).

c. En el campo **Valor**, de acuerdo con lo que eligió en el paso anterior, escriba una de las siguientes opciones:

- Dirección MAC (xx:xx:xx:xx:xx:xx) de la computadora en la que se aplica la política.
- La dirección IP de la computadora en la que se aplica la política.
- Las direcciones IP de inicio y finalización del rango de direcciones que se deben bloquear (por ejemplo, 192.168.1.2-192.168.1.253).

PASO 8 Para bloquear el tráfico de sitios web específicos:

a. En la tabla **Bloqueo de sitios web**, haga clic en **Agregar fila**.

b. En el menú desplegable **Tipo**, elija cómo bloquear un sitio web (mediante la especificación de la URL o de una palabra clave que aparece en la URL).

c. En el campo **Valor**, escriba la URL o la palabra clave que se utiliza para bloquear el sitio web.

Por ejemplo, para bloquear la URL ejemplo.com, elija **Dirección URL** en el menú desplegable y escriba **ejemplo.com** en el campo **Valor**. Para bloquear una URL que tiene la palabra clave “ejemplo” en la URL, elija **Palabra clave** en el menú desplegable y escriba **ejemplo** en el campo **Valor**.

PASO 9 Haga clic en **Guardar**.

Configuración de reenvío de puertos

El reenvío de puertos se utiliza para redireccionar el tráfico de Internet de un puerto en WAN a otro puerto en LAN. Los servicios comunes están disponibles o puede definir un servicio personalizado y los puertos asociados que deben reenviarse.

Las páginas **Reglas de reenvío de un solo puerto** y **Reglas de reenvío de rango de puertos** enumeran todas las reglas de reenvío de puertos disponibles para este dispositivo y le permite configurar las reglas de reenvío de puertos.

NOTA El reenvío de puertos no es apropiado para los servidores en la LAN, ya que se depende de que el dispositivo LAN realice una conexión saliente para que se abran los puertos entrantes.

Algunas aplicaciones requieren que se reciban datos en un puerto o rango de puertos específicos para funcionar correctamente cuando se conecten dispositivos externos. El router debe enviar todos los datos entrantes para esa aplicación solamente en el puerto o rango de puertos requerido.

La puerta de enlace tiene una lista de los juegos y de las aplicaciones comunes con los puertos entrantes y salientes correspondientes que deben abrirse. También puede especificar una regla de reenvío de puertos mediante la definición del tipo de tráfico (TCP o UDP) y el rango de puertos entrantes y salientes que deben abrirse cuando están habilitados.

Configuración de reenvío de un solo puerto

Para agregar una regla de reenvío de un solo puerto:

PASO 1 Elija **Firewall** > **Reenvío de un solo puerto**. Se muestra una lista de las aplicaciones preexistentes.

PASO 2 En el campo **Aplicación**, escriba el nombre de la aplicación para la que debe configurarse el reenvío de puerto.

PASO 3 En el campo **Puerto externo**, escriba el número de puerto que activa esta regla cuando se realiza una solicitud de conexión desde el tráfico saliente.

PASO 4 En el campo **Puerto interno**, escriba el número de puerto que utiliza el sistema remoto para responder a la solicitud que recibe.

PASO 5 En el menú desplegable de Interfaz, elija **Ambos (Ehternet y 3G)**, **Ethernet** o **3G**.

PASO 6 En el menú desplegable **Protocolo**, elija un protocolo (**TCP**, **UDP** o **TCP** y **UDP**).

PASO 7 En el campo **Dirección IP**, escriba la dirección IP del host del lado de LAN a donde se reenviará el tráfico IP específico. Por ejemplo, puede enviar tráfico HTTP al puerto 80 de la dirección IP de un servidor web del lado de LAN.

PASO 8 En el campo **Habilitar**, active la casilla **Habilitar** para habilitar la regla.

PASO 9 Haga clic en **Guardar**.

Configuración de reenvío de rango de puertos

Para agregar una regla de reenvío de rango de puertos:

PASO 1 Elija **Firewall** > **Reenvío de rango de puertos**.

PASO 2 En el campo **Aplicación**, escriba el nombre de la aplicación para la que debe configurarse el reenvío de puerto.

PASO 3 En el campo **Puerto externo**, especifique el número de puerto que activará esta regla cuando se realice una solicitud de conexión desde el tráfico saliente.

PASO 4 En el campo **Iniciar**, especifique el número de puerto que comienza el rango de puertos que debe reenviarse.

PASO 5 En el campo **Finalizar**, especifique el número de puerto que finaliza el rango de puertos que debe reenviarse.

PASO 6 En el menú desplegable de Interfaz, elija **Ambos (Ehternet y 3G)**, **Ethernet** o **3G**.

PASO 7 En el menú desplegable **Protocolo**, elija un protocolo (**TCP**, **UDP** o **TCP** y **UDP**).

PASO 8 En el campo **Dirección IP**, escriba la dirección IP del host del lado de LAN a donde se reenviará el tráfico IP específico.

PASO 9 En el campo **Habilitar**, active la casilla **Habilitar** para habilitar la regla.

PASO 10 Haga clic en **Guardar**.

Configuración de la activación de rango de puertos

La activación de puertos permite que los dispositivos en LAN o DMZ soliciten uno o más puertos de reenvío. La activación de puertos espera una solicitud saliente de LAN/DMZ en uno de los puertos salientes definidos y, luego, abre un puerto entrante para ese tipo de tráfico determinado.

La activación de puertos es una forma de reenvío de puertos dinámica cuando una aplicación transmite datos a través de los puertos salientes o entrantes abiertos. La activación de puertos abre un puerto entrante para un tipo de tráfico específico en un puerto saliente definido. La activación de puertos es más flexible que el reenvío de puertos estático (disponible durante la configuración de las reglas de firewall), ya que una regla no debe referir a una IP de LAN o un rango de IP. Los puertos tampoco quedan abiertos cuando no estén en uso, lo que proporciona un nivel de seguridad que el reenvío de puertos no ofrece.

NOTA La activación de puertos no es apropiada para los servidores en LAN, ya que se depende de que el dispositivo LAN realice una conexión saliente antes de que se abran los puertos entrantes.

Algunas aplicaciones requieren que, cuando se conecten dispositivos externos, se reciban datos en un puerto o en un rango de puertos específicos para funcionar correctamente. El router debe enviar todos los datos entrantes para esa aplicación solamente en el puerto o rango de puertos requerido. La puerta de enlace tiene una lista de los juegos y de las aplicaciones comunes con los puertos entrantes y salientes correspondientes que deben abrirse. También puede especificar una regla de activación de puertos mediante la definición del tipo de tráfico (TCP o UDP) y del rango de puertos entrantes y salientes que deben abrirse cuando están habilitados.

Para agregar una regla de activación de puertos:

PASO 1 Elija **Firewall** > **Activación de rango de puertos**.

PASO 2 En el campo **Aplicación**, escriba el nombre de la aplicación para la que debe configurarse el reenvío de puerto.

PASO 3 En los campos **Rango activado**, escriba el número de puerto o el rango de número de puertos que activará esta regla cuando se realice una solicitud de conexión desde el tráfico saliente. Si la conexión saliente utiliza solamente un puerto, escriba el mismo número de puerto en los dos campos.

PASO 4 En los campos **Rango reenviado**, escriba el número de puerto o el rango de número de puertos que utiliza el sistema remoto para responder a la solicitud que recibe. Si la conexión entrante utiliza solamente un puerto, especifique el mismo número de puerto en los dos campos.

PASO 5 En el menú desplegable de Interfaz, elija **Ambos (Ehternet y 3G)**, **Ethernet** o **3G**.

PASO 6 En el campo **Habilitar**, active la casilla **Habilitar** para habilitar la regla.

PASO 7 Haga clic en **Guardar**.

6

Configuración de VPN

En este capítulo, se describe cómo configurar la VPN y la seguridad para el dispositivo.

Tipos de túnel VPN

Una red privada virtual (VPN) proporciona un canal (túnel) de comunicación segura entre dos routers de puerta de enlace o un trabajador remoto y un router de puerta de enlace. Puede crear distintos tipos de túneles de VPN, según las necesidades de su empresa. A continuación se describen varios escenarios. Lea estas descripciones para comprender las opciones y los pasos necesarios para configurar su VPN.

Acceso remoto con PPTP

En este escenario, un usuario remoto con un equipo de Microsoft se conecta a un servidor PPTP en su sitio para acceder a los recursos de red. Use esta opción para simplificar la configuración de la VPN. No es necesario configurar políticas de VPN. Los usuarios remotos se pueden conectar usando el cliente PPTP de un equipo de Microsoft. No hay necesidad de instalar un cliente VPN. Sin embargo, tenga en cuenta que se han detectado vulnerabilidades de seguridad en este protocolo.

Acceso remoto con QuickVPN de Cisco

Para una instalación rápida con configuración de seguridad VPN básica, distribuya el software QuickVPN de Cisco a sus usuarios, que pueden acceder a los recursos de su red de manera segura. Use esta opción si desea simplificar el proceso de configuración de VPN. No es necesario configurar políticas de VPN. Los usuarios remotos pueden conectarse de forma segura con el cliente QuickVPN de Cisco y una conexión a Internet.

VPN de sitio a sitio

El dispositivo es compatible con la VPN de sitio a sitio para un túnel VPN simple de puerta de enlace a puerta de enlace. Por ejemplo, puede configurar el dispositivo en una sucursal para conectar al router en el sitio corporativo, para que la sucursal pueda acceder de manera segura a la red corporativa. La VPN de sitio a sitio se configura en la página **VPN** > **Configuración básica de VPN**.

Clientes VPN

El software cliente de VPN se requiere para establecer un túnel VPN entre el router y el punto final remoto. Su dispositivo admite clientes Cisco QuickVPN y PPTP VPN.

Configuración de PPTP

El protocolo de tunelización punto a punto (PPTP) es un protocolo de red que permite la transferencia de datos segura desde un cliente remoto hasta una red comercial mediante la creación de una conexión VPN segura en redes públicas, como Internet.

NOTA Cuando se habilita la VPN en el dispositivo, la subred LAN en el dispositivo se cambia automáticamente para evitar que surjan problemas con la dirección IP entre la red remota y la red local.

Para configurar el servicio VPN PPTP:

PASO 1 Elija **VPN** > **Clientes VPN**.

PASO 2 Introduzca la siguiente información:

Servidor PPTP	Marque la casilla para habilitar el servidor PPTP.
Dirección IP para servidor PPTP	Escriba la dirección IP del servidor PPTP.

Dirección IP para clientes PPTP	Escriba el rango de direcciones IP de clientes PPTP.
Cifrado MPPE	Marque la casilla de verificación **Habilitar** para habilitar el cifrado MPPE. El Cifrado punto a punto de Microsoft (MPPE) se usa cuando los usuarios configuran y usan un cliente PPTP VPN para conectarse al dispositivo.

PASO 3 Haga clic en **Guardar**.

Configuración de QuickVPN

PASO 1 Agregue a los usuarios de QuickVPN en la página **VPN > VPN Clients (Clientes VPN)**. Consulte **Importación de configuración de clientes VPN** y **Creación y administración de usuarios QuickVPN**.

PASO 2 Enseñe a los usuarios a obtener el software QuickVPN gratuito de Cisco en Cisco.com, e instalarlo en sus equipos. Consulte **Utilización del software QuickVPN de Cisco**.

PASO 3 Para habilitar el acceso a través de Cisco QuickVPN en su dispositivo, debe habilitar la administración remota para abrir el puerto 443 para SSL. Consulte **Configuración de los parámetros básicos de firewall**.

Configuración de NetBIOS en VPN

Para habilitar NetBIOS en VPN:

PASO 1 En el campo **NetBIOS en VPN**, marque la casilla para permitir que las difusiones de NetBIOS viajen por el túnel VPN. De manera predeterminada, la función NetBIOS está disponible para las políticas de clientes.

PASO 2 Haga clic en **Guardar**.

Creación y administración de usuarios PPTP

Para crear usuarios PPTP:

PASO 1 En la **Tabla de config. de clientes VPN**, haga clic en **Agregar fila**.

PASO 2 Escriba esta información:

Habilitar	Marque esta casilla para habilitar al usuario.
Nombre de usuario	Escriba el nombre de usuario del usuario PPTP (de 4 a 32 caracteres).
Contraseña	Escriba la contraseña (de 4 a 32 caracteres).
Protocolo	Elija **PPTP** en el menú desplegable.

PASO 3 Haga clic en **Guardar**.

Para editar la configuración de un usuario PPTP, marque su casilla y haga clic en Edit (Editar). Cuando haya finalizado, haga clic en **Guardar**.

Para eliminar un usuario PPTP, marque su casilla y haga clic en **Eliminar**.

Creación y administración de usuarios QuickVPN

Para crear usuarios QuickVPN:

PASO 1 En la **Tabla de config. de clientes VPN**, haga clic en **Agregar fila**.

PASO 2 Escriba esta información:

PASO 3 Haga clic en **Guardar**.

Para editar la configuración de un usuario QuickVPN, marque su casilla y haga clic en **Edit** (Editar). Realice los cambios y haga clic en **Save** (Guardar).

Para eliminar un usuario QuickVPN, marque la casilla, haga clic en **Delete** (Eliminar) y luego en **Save** (Guardar).

Para obtener más información sobre QuickVPN, consulte **Ap?dice A, ?$paratext>.?Default Para Font>**

Importación de configuración de clientes VPN

Usted puede importar archivos de configuración de clientes VPN que contengan el nombre de usuario y la contraseña de clientes en un archivo de texto de valor separado por comas (CSV).

Puede usar un programa como Excel para crear un archivo CSV que contenga la configuración de clientes VPN. El archivo debe incluir una fila para los encabezados y una o más filas para los clientes VPN.

Por ejemplo, a continuación se especifican los parámetros de dos usuarios para importar:

PROTOCOLO	NOMBRE DE USUARIO	CONTRASEÑA
PPTP	pptp-user-1	12345678
QuickVPN	qv-user-1	12345678

PRECAUCIÓN Al importar la configuración de clientes VPN, se elimina la configuración existente.

Para importar la configuración de clientes VPN:

PASO 1 Haga clic en **Examinar** para ubicar el archivo.

PASO 2 Haga clic en **Importar** para cargar el archivo.

PASO 3 Cuando se lo solicite, para eliminar la configuración de usuarios VPN existentes e importar la configuración en el archivo CSV, haga clic en **Sí**.

Configuración de opciones básicas de VPN con IPsec de sitio a sitio

El dispositivo es compatible con la VPN de sitio a sitio para un túnel VPN simple de puerta de enlace a puerta de enlace. En esta configuración, el dispositivo crea una conexión segura con otro router habilitado para VPN. Por ejemplo, puede configurar el dispositivo en una sucursal para conectar al router en el sitio corporativo, para que la sucursal pueda acceder de manera segura a la red corporativa.

Pasos para configurar opciones de VPN básicas en una conexión de sitio a sitio:

PASO 1 Elija **VPN** > **Configuración de VPN básica**.

PASO 2 En el campo **Nombre de la conexión**, escriba un nombre para el túnel VPN.

PASO 3 En el campo **Clave previamente compartida**, introduzca la clave previamente compartida, o la contraseña, que será intercambiada entre los dos routers. Debe contener entre 8 y 49 caracteres.

PASO 4 En los campos **Información de punto final**, introduzca la siguiente información:

- **Remote Endpoint** (Punto final remoto): elija la manera en que se identifica el punto final remoto o el router al que se conectará el dispositivo. Por ejemplo, mediante una dirección IP, como 192.168.1.1, o mediante un nombre de dominio totalmente calificado (FQDN), como cisco.com.
- **Dirección IP remota de WAN (Internet)**: introduzca la dirección IP pública o el nombre de dominio del punto final remoto.
- **Redundancy Endpoint** (Punto final de redundancia): para permitir que el dispositivo conmute a una puerta de enlace alternativa cuando falle la conexión VPN primaria, marque la casilla de verificación **Enable** (Habilitar). Ingrese la dirección IP WAN o el FQDN para el punto final de redundancia.
- **Local WAN (Internet) IP Address** (Dirección IP local de WAN [Internet]): introduzca la dirección IP pública o el nombre de dominio del punto final local (dispositivo).

PASO 5 En los campos **Accesibilidad remota de conexión segura**, introduzca la siguiente información:

- **Dirección IP remota de LAN (red local)**: introduzca la dirección de la red privada (LAN) del punto final remoto. Esta es la dirección IP de la red interna en el sitio remoto.
- **Máscara de subred remota de LAN**: introduzca la máscara de subred de la red privada (LAN) del punto final remoto.
- **Dirección IP local de LAN (red local)**: introduzca la dirección de la red privada (LAN) de la red local. Esta es la dirección IP de la red interna del dispositivo.
- **Local LAN (Local Network) Subnet Mask** (Máscara de subred local de LAN [red local]): introduzca la máscara de subred de la red privada (LAN) de la red local (dispositivo).

Nota: Las direcciones IP de WAN y LAN remotas no pueden existir en la misma subred. Por ejemplo, una dirección IP de LAN de 192.168.1.100 y una dirección IP local de LAN de 192.168.1.115 ocasionarían un conflicto cuando el tráfico se enruta por medio de la VPN. El tercer octeto debe ser diferente para que las direcciones IP se encuentren en subredes diferentes. Por ejemplo, se aceptan una dirección IP de LAN remota de 192.168.1.100 y una dirección IP de LAN local de 192.168.2.100.

PASO 6 Haga clic en **Guardar**.

Visualización de valores predeterminados

Los valores predeterminados utilizados en las opciones de VPN básicas son los propuestos por el consorcio de la VPN y suponen que utiliza una clave previamente compartida o una contraseña, que es conocida tanto para el dispositivo como para el router del otro extremo (por ejemplo, Cisco RV220W). Pasos para visualizar los valores predeterminados:

PASO 1 Elija **VPN** > **Configuración de VPN básica**.

PASO 2 Haga clic en **Ver configuración predeterminada** para ver los valores predeterminados.

Para obtener más información sobre estos valores, consulte **Configuración de parámetros de VPN avanzados**.

Configuración de parámetros de VPN avanzados

La página Configuración de VPN avanzada le permite configurar parámetros de VPN avanzados, como las políticas IKE y otras políticas de VPN. Estas políticas controlan la manera en que el dispositivo inicia y recibe las conexiones de VPN con otros puntos finales.

Administración de políticas IKE

El protocolo de Intercambio de claves de Internet (IKE) intercambia las claves entre dos hosts IPsec de forma dinámica. Puede crear políticas IKE para definir los parámetros de seguridad, como la autenticación del par y los algoritmos de cifrado que se usarán en este proceso. Asegúrese de utilizar cifrado, autenticación y parámetros de grupo de claves compatibles en la política VPN.

PASO 1 Seleccione **VPN** > **IPsec** > **Configuración avanzada de VPN**.

PASO 2 En la **Tabla de políticas VPN**, si marca la casilla de la fila de conexión de la VPN, podrá realizar las siguientes tareas:

- **Add Row** (Agregar fila) o **Edit** (Editar): editar propiedades de la política IKE. Consulte **Agregar o editar políticas IKE**.
- **Habilitar**: habilitar la política.
- **Deshabilitar**: deshabilitar la política.
- **Eliminar**: eliminar la política.

NOTA No puede eliminar una política IKE si esta se está usando en una política VPN. Primero debe deshabilitar y eliminar la política VPN de la **Tabla de políticas VPN**.

- **Agregar fila**: agregar una política IKE. Consulte **Agregar o editar políticas IKE**.

NOTA Si ya tiene una conexión VPN configurada, no puede agregar otra sin eliminar la conexión de VPN existente.

PASO 3 Haga clic en **Guardar**.

Agregar o editar políticas IKE

PASO 1 Al agregar o editar políticas IKE, configure los siguientes parámetros:

- **Nombre de política:** escriba un nombre único de la política para fines de identificación y administración.
- **Modo intercambio:** elija una de las siguientes opciones:
  - **Main** (Principal): negocia el túnel con mayor seguridad, pero es más lento.
  - **Aggressive** (Agresivo): establece una conexión más rápida, pero con menos seguridad.
- **Local Identifier** (Identificador local): identificador IKE local.
- **Remote Identifier** (Identificador remoto): identificador IKE remoto.
- **Redundancy Identifier** (Identificador de redundancia): el identificador único para el punto final de respaldo alternativo usado para restaurar la conexión si falla la conexión VPN original.

PASO 2 En la sección **Parámetros de SA IKE**, los parámetros de asociación de seguridad (SA) definen la potencia y el modo para negociar la SA. Puede configurar las siguientes opciones:

- **Algoritmo de cifrado:** seleccione el algoritmo utilizado para negociar la SA:
  - **DES**
  - **3DES**
  - **AES-128**
  - **AES-192**
  - **AES-256**
- **Algoritmo de autenticación:** especifique el algoritmo de autenticación del encabezado de la VPN:
  - **MD5**
  - **SHA-1**
  - **SHA2-256**

    Asegúrese de que el algoritmo de autenticación esté configurado en forma idéntica en los dos lados del túnel de la VPN (por ejemplo, el dispositivo y el router al que se está conectando).
- **Clave previamente compartida:** introduzca la clave en el espacio provisto. Tenga en cuenta que no se admite el carácter comillas dobles (“) en la clave previamente compartida.
- **Grupo Diffie-Hellman (DH):** especifique el algoritmo del grupo DH, que se utiliza al intercambiar claves. El grupo DH establece la potencia del algoritmo en bits. Asegúrese de que el grupo DH esté configurado en forma idéntica en los dos lados de la política IKE.
- **Vida útil:** introduzca el intervalo, en segundos, después del cual la asociación de seguridad pierde validez.
- **Detección del par inactivo:** marque la casilla **Habilitar** para habilitar esta función o desmárquela para deshabilitarla. La detección del par inactivo (DPD) se utiliza para detectar si el par está activo o no. Si el par es detectado como inactivo, el router elimina la asociación de seguridad IKE e IPsec. Si habilita esta función, introduzca además los siguientes parámetros:
  - **Retraso de DPD:** introduzca el intervalo, en segundos, entre los mensajes DPD R-U-THERE consecutivos. Los mensajes DPD R-U-THERE

se envían solo cuando el tráfico IPsec es inactivo.

- **DPD Timeout** (Tiempo de espera de DPD): introduzca el tiempo máximo que el dispositivo debería esperar para recibir una respuesta al mensaje de DPD antes de considerar que el par está inactivo.

PASO 3 Marque la casilla de verificación **XAUTH Type Enable** (Habilitar tipo XAUTH) para configurar la autenticación extendida para su política VPN con IPsec. Proporcione el nombre de usuario y la contraseña de autenticación.

PASO 4 Haga clic en **Guardar**.

Administración de las políticas VPN

Para administrar las políticas VPN, haga lo siguiente:

PASO 1 Seleccione **VPN** > **IPsec** > **Configuración avanzada de VPN**.

PASO 2 En la **Tabla de política VPN**, si marca la casilla de la fila de conexión de la VPN, podrá realizar las siguientes tareas:

- **Add Row** (Agregar fila) o **Edit** (Editar): editar propiedades de la política VPN. Consulte **Agregar o editar políticas VPN**.
- **Habilitar**: habilitar la política.
- **Deshabilitar**: deshabilitar la política.
- **Eliminar**: eliminar la política.
- **Agregar fila**: agregar una política VPN. Consulte **Agregar o editar políticas VPN**.

NOTA Si ya tiene una conexión VPN configurada, no puede agregar otra sin eliminar la conexión de VPN existente.

PASO 3 Haga clic en **Guardar**.

Agregar o editar políticas VPN

Para crear una política VPN automática, primero debe crear una política IKE y, luego, agregar la política automática correspondiente para esa política IKE.

Al agregar o editar una política VPN, puede configurar los siguientes parámetros:

- **Nombre de la política:** escriba un nombre único para identificar la política.

- **Tipo de política:** elija una de las siguientes opciones:
  - **Política automática**: algunos parámetros del túnel VPN se generan de manera automática. Esto requiere utilizar el protocolo IKE (Intercambio de claves de Internet) para realizar negociaciones entre los dos puntos finales de la VPN.
  - **Política manual**: todas las configuraciones (incluidas las claves) del túnel de VPN se ingresan en forma manual para cada punto final. No se requiere ningún servidor de terceros ni ninguna organización.
- **Punto final remoto:** seleccione el tipo de identificador que desea proporcionar para la puerta de enlace que se encuentra en el punto final remoto: **Dirección IP** o **FQDN** (Nombre de dominio completamente calificado). Ingrese el identificador en el espacio provisto.
- **Redundancy Endpoint** (Punto final de redundancia): para permitir que el dispositivo conmute a una puerta de enlace alternativa cuando falle la conexión VPN primaria, marque la casilla de verificación **Enable** (Habilitar). Ingrese la dirección IP WAN o el FQDN para el punto final de redundancia.

  Para revertir automáticamente a la VPN primaria cuando se restaure la conexión, marque la casilla de verificación **Rollback enable** (Habilitar reversión).

En **Local Traffic Selection** (Selección de tráfico local) y **Remote Traffic Selection** (Sección de tráfico remoto), ingrese los siguientes parámetros:

- **IP local/remoto**: seleccione el tipo de identificador que desea proporcionar para el punto final:
  - **Simple**: limita la política a un host. Introduzca la dirección IP del host que formará parte de la VPN en el campo Dirección IP de inicio. Escriba la dirección IP en el campo **Start Address** (Dirección de inicio).
  - **Subred**: permite que una subred completa se conecte con la VPN. Introduzca la dirección de la red en el campo Dirección IP de inicio y la máscara de subred en el campo Máscara de subred. Escriba la dirección IP de la subred en el campo **Dirección de inicio**. Introduzca la máscara de la subred, como 255.255.255.0, en el campo **Máscara de subred**. El campo muestra automáticamente una dirección de subred predeterminada basada en la dirección IP.

    IMPORTANTE: Asegúrese de evitar el uso de redes que se superponen para los selectores de tráfico local o remoto. Para el uso de estas subredes, será necesario agregar rutas estáticas en el router y en los hosts que se utilizarán. Por ejemplo, una combinación que se debe evitar es la siguiente:

    Selector de tráfico local: 192.168.1.0/24

    Selector de tráfico remoto: 192.168.0.0/16

En el tipo de política **Manual**, introduzca los parámetros de la sección **Parámetros de política manual**:

- **SPI entrante, SPI saliente**: introduzca un valor hexadecimal que contenga entre 3 y 8 caracteres, por ejemplo, 0x1234.
- **Algoritmo de cifrado:** seleccione el algoritmo utilizado para cifrar los datos:
  - DES
  - 3DES
  - AES-128
  - AES-192
  - AES-256
- **Clave de entrada**: introduzca la clave de cifrado de la política de entrada. La longitud de la clave depende del algoritmo de cifrado elegido:
  - DES: 8 caracteres
  - 3DES: 24 caracteres
  - AES-128: 16 caracteres
  - AES-192: 24 caracteres
  - AES-256: 32 caracteres
- **Clave de salida**: introduzca la clave de cifrado de la política de salida. La longitud de la clave depende del algoritmo de cifrado elegido, como se muestra más arriba.
- **Algoritmo de integridad:** seleccione el algoritmo utilizado para verificar la integridad de los datos:
  - MD5
  - SHA-1
  - SHA2-256
- **Clave de entrada**: introduzca la clave de integridad (para ESP, con modo de integridad) para la política de entrada. La longitud de la clave depende del algoritmo elegido:
  - MD5: 16 caracteres
  - SHA-1: 20 caracteres
  - SHA2-256: 32 caracteres

- **Clave de salida**: introduzca la clave de integridad (para ESP, con modo de integridad) de la política de salida. La longitud de la clave depende del algoritmo elegido, como se muestra más arriba.

En el tipo de política **Automática**, introduzca los parámetros de la sección **Parámetros de política automática**.

- **Vida útil de SA**: introduzca la duración de la asociación de seguridad en segundos. Una vez que transcurra la cantidad de segundos, la asociación de seguridad se vuelve a negociar. El valor predeterminado es 3600 segundos. El valor mínimo es de 300 segundos.
- **Algoritmo de cifrado:** seleccione el algoritmo utilizado para cifrar los datos.
- **Algoritmo de integridad:** seleccione el algoritmo utilizado para verificar la integridad de los datos.
- **Grupo de claves PFS:** marque la casilla **Habilitar** para habilitar Confidencialidad directa perfecta (PFS) y mejorar la seguridad. Aunque es más lento, este protocolo ayuda a evitar curiosos al garantizar que se realice un intercambio Diffie-Hellman en todas las negociaciones de la fase 2.
- **Seleccionar política IKE:** seleccione la política IKE que definirá las características de la fase 1 de la negociación. Haga clic en **View** (Ver) para ver o editar la política IKE existente configurada en el dispositivo.

Configuración de administración de certificados

El dispositivo usa certificados digitales para autenticación VPN con IPsec y validación SSL (para HTTPS). Usted puede generar y firmar sus propios certificados con la funcionalidad disponible en el dispositivo.

Generación de un nuevo certificado

Usted puede generar un nuevo certificado para reemplazar el certificado existente en el dispositivo.

Para generar un certificado:

PASO 1 Elija **VPN** > **Certificate Management** (Administración de certificados).

PASO 2 Haga clic en el botón **Generar un nuevo certificado**.

PASO 3 Haga clic en **Generar certificado**.

Importación de certificados

Puede importar certificados previamente creados y guardados mediante el botón **Exportar para administrador**.

Para importar un certificado:

PASO 1 Elija **VPN** > **Certificate Management** (Administración de certificados).

PASO 2 Haga clic en el botón **Importar certificado desde un archivo**.

PASO 3 Haga clic en **Examinar** para ubicar el archivo del certificado.

PASO 4 Haga clic en **Instalar certificado**.

Exportación de certificados para administrador

Puede exportar el certificado para administrador a una carpeta en su computadora o a una ubicación externa en una unidad USB. El certificado para administrador contiene la clave privada y debería guardarse en un lugar seguro como copia de respaldo. Si se restablece la configuración del dispositivo para que vuelva a los valores predeterminados de fábrica, este certificado se puede importar y restaurar en el router.

Para exportar un certificado para administrador:

PASO 1 Elija **VPN** > **Certificate Management** (Administración de certificados).

PASO 2 Para exportar el certificado a su computadora, haga clic en **Export for Admin** (Exportar para administrador). El Administrador de dispositivos guarda el archivo admin.pem en C:\Documents and Settings\userid\Mis documentos\Descargas.

Para exportar el certificado a una unidad USB externa, haga clic en **Export to USB for Admin** (Exportar a USB para administrador).

Exportación de certificados para cliente

Puede exportar certificados para clientes a su computadora o a una ubicación externa en una unidad USB. El certificado para el cliente permite que usuarios QuickVPN se conecten al Cisco RV215W de manera segura. Los usuarios QuickVPN deben colocar el certificado en el directorio de instalación del cliente QuickVPN.

Para exportar un certificado para cliente:

PASO 1 Elija **VPN** > **Administración de certificados**.

PASO 2 Para exportar el certificado a su computadora, haga clic en **Export for Client** (Exportar para cliente). En una PC, el Administrador de dispositivos guarda el archivo client.pem en C:\Documents and Settings\userid\Mis documentos\Descargas.

Para exportar el certificado a una unidad USB externa, haga clic en **Export to USB for Client** (Exportar a USB para cliente).

Configuración de transmisión VPN

La transmisión VPN permite que el tráfico de VPN que se origina en clientes VPN pase por el dispositivo.

Para configurar la transmisión VPN:

PASO 1 Elija **VPN** > **Transmisión VPN**.

PASO 2 Elija el tipo de tráfico que desea dejar pasar por el firewall:

IPsec	Marque la casilla de verificación **Enable** (Habilitar) para dejar que los túneles de seguridad IP pasen por el dispositivo.
PPTP	Marque la casilla de verificación **Enable** (Habilitar) para dejar que los túneles PPTP pasen por el dispositivo.
L2TP	Marque la casilla de verificación **Enable** (Habilitar) para dejar que los túneles del Protocolo de tunelización de capa 2 (L2TP) pasen por el dispositivo.

PASO 3 Haga clic en **Guardar**.

7

Configuración de la calidad de servicio (QoS)

El router Cisco RV215W le permite configurar las siguientes funciones de la calidad de servicio (QoS):

- **Configuración de la administración del ancho de banda, p?ina 116**
- **Configuración de QoS basada en puertos, p?ina 119**
- **Configuración de valores de CoS, p?ina 120**
- **Configuración de los valores de DSCP, p?ina 121**

La Calidad de servicio (QoS) asigna prioridad a diversas aplicaciones, usuarios o flujos de datos, o garantiza cierto nivel de rendimiento para un flujo de datos. Esta garantía es importante cuando la capacidad de la red no es suficiente. En especial, para aplicaciones multimedia de flujo de datos en tiempo real, como Voz sobre IP, juegos en línea e IP-TV, que generalmente requieren tasas de bits fijas y son sensibles al retardo, y en redes donde la capacidad es un recurso limitado, por ejemplo, en comunicación de datos celulares.

Configuración de la administración del ancho de banda

Usted puede usar la función de administración del ancho de banda del dispositivo para administrar el ancho de banda del tráfico que fluye de la red segura (LAN) a la red insegura (WAN).

Configuración del ancho de banda

Usted puede limitar el ancho de banda para reducir la velocidad a la que el dispositivo transmite datos. Puede, además, usar un perfil de ancho de banda para limitar el tráfico saliente, lo que impide que los usuarios LAN consuman todo el ancho de banda del vínculo de Internet.

Para configurar el ancho de banda ascendente y descendente:

PASO 1 Seleccione **QoS** > **Administración del ancho de banda**.

PASO 2 En el campo **Administración del ancho de banda**, marque **Habilitar**. El ancho de banda máximo proporcionado por su ISP aparece en la sección **Ancho de banda**.

PASO 3 En la **Tabla de ancho de banda**, escriba la siguiente información para la interfaz WAN:

Flujo ascendente	Ancho de banda (Kbps) utilizado para enviar datos a Internet.
Flujo descendente	Ancho de banda (Kbps) utilizado para recibir datos de Internet.

PASO 4 Haga clic en **Guardar**.

Configuración de la prioridad de ancho de banda

En la **Tabla de prioridad de ancho de banda**, puede asignar prioridades a servicios para administrar el uso del ancho de banda.

Para configurar la prioridad de ancho de banda:

PASO 1 Elija **QoS** > **Administración del ancho de banda**.

PASO 2 En el campo **Administración del ancho de banda**, marque **Habilitar**. El ancho de banda máximo proporcionado por su ISP aparece en la sección **Ancho de banda**.

PASO 3 En la **Tabla de prioridad de ancho de banda**, haga clic en **Agregar fila**.

PASO 4 Escriba esta información:

Habilitar	Marque esta casilla para habilitar la administración del ancho de banda para este servicio.
Servicio	Elija el servicio que desea priorizar.
Dirección	Elija la dirección del tráfico que desea priorizar (**descendente** o **ascendente**).
Prioridad	Elija la prioridad del servicio (**baja**, **normal**, **media** o **alta**).

PASO 5 Haga clic en **Guardar**.

Para editar la configuración de una entrada en la tabla, marque la casilla correspondiente y haga clic en **Editar**. Cuando haya terminado de hacer cambios, haga clic en **Guardar**.

Para eliminar una entrada de la tabla, marque la casilla correspondiente, haga clic en **Delete** (Eliminar) y luego en **Save** (Guardar).

Para agregar la definición de un nuevo servicio, haga clic en el botón **Administración de servicio**. Usted puede definir un nuevo servicio con el fin de usarlo para todas las definiciones de firewall y QoS. Consulte **Configuración de la administración de servicios**.

Configuración de QoS basada en puertos

Usted puede configurar los valores de QoS para cada puerto LAN en el Cisco RV215W. El dispositivo admite filas de espera de 4 niveles de prioridad que permiten priorizar el tráfico por puerto de switch físico.

Para configurar los valores de QoS para los puertos LAN del dispositivo:

PASO 1 Seleccione **QoS** > **Configuración de QoS basada en puertos**.

PASO 2 Para cada puerto en la tabla **Config. de QoS de Ethernet basada en puertos**, escriba esta información:

Modo de confianza	Elija una de las siguientes opciones en el menú desplegable: • **Puerto**: este valor habilita la QoS basada en puertos. Puede, posteriormente, establecer la prioridad del tráfico para un puerto en particular. Las filas de tráfico pueden tener una prioridad de 1, que es la más baja, y alcanzar una prioridad de 4, que es la más alta. • **DSCP**: punto de código de servicios diferenciados (DSCP). Al habilitar esta función, se prioriza el tráfico de red en LAN según la asignación de filas de espera de DSCP en la página **Configuración DSCP**. • **CoS**: clase de servicio (CoS).
Fila de reenvío de tráfico predeterminada para dispositivos no confiables	Elija un nivel de prioridad (de 1 a 4) para el tráfico saliente.

PASO 3 Para cada puerto en la tabla **Config. de QoS 3G basada en puertos**, escriba esta información:

Modo de confianza	Elija una de las siguientes opciones en el menú desplegable: • **Puerto**: este valor habilita la QoS basada en puertos. Puede, posteriormente, establecer la prioridad del tráfico para un puerto en particular. Las filas de tráfico pueden tener una prioridad de 1, que es la más baja, y alcanzar una prioridad de 4, que es la más alta. • **DSCP**: punto de código de servicios diferenciados (DSCP). Al habilitar esta función, se prioriza el tráfico de red en LAN según la asignación de filas de espera de DSCP en la página **Configuración DSCP**. • **CoS**: clase de servicio (CoS).
Fila de reenvío de tráfico predeterminada para dispositivos no confiables	Elija un nivel de prioridad (de 1 a 4) para el tráfico saliente.

PASO 4 Haga clic en **Guardar**.

Para restaurar la configuración de QoS basada en puertos predeterminada, haga clic en **Restore Default** (Restaurar valor predet.) y luego en **Save** (Guardar).

Configuración de valores de CoS

Puede usar el enlace a la página Configuración de QoS basada en puertos para asignar los valores de prioridad de CoS a la fila de espera de QoS.

Para asignar valores de prioridad de CoS a la fila de reenvío de tráfico:

PASO 1 Elija **QoS** > **Configuración de CoS**.

PASO 2 Elija el botón de radio **Ethernet** o **3G**.

PASO 3 Para cada nivel de prioridad de CoS en la **Tabla de config. de CoS**, elija un valor de prioridad en el menú desplegable **Fila de reenvío de tráfico**.

Estos valores marcan tipos de tráfico con mayor o menor prioridad de tráfico según el tipo de tráfico.

PASO 4 Haga clic en **Guardar**.

Para restaurar la configuración de QoS basada en puertos predeterminada, haga clic en **Restore Default** (Restaurar valor predet.) y luego en **Save** (Guardar).

Configuración de los valores de DSCP

Usted puede usar la página **Configuración DSCP** para configurar la asignación de DSCP a la fila de espera de QoS.

Para configurar la asignación de DSCP a la fila de espera de QoS:

PASO 1 Elija **QoS** > **Configuración DSCP**

PASO 2 Elija el botón de radio **Ethernet** o **3G**.

PASO 3 Elija si solo incluir valores RFC o todos los valores DSCP en la **Tabla de config. de DSCP**; para ello, haga clic en el botón correspondiente.

PASO 4 Para cada valor DSCP en la **Tabla de config. de DSCP**, elija un nivel de prioridad en el menú desplegable **Cola de espera**.

De esta manera, se asigna el valor DSCP a la fila de espera de QoS seleccionada.

PASO 5 Haga clic en **Guardar**.

Para restaurar la configuración de DSCP predeterminada, haga clic en **Restaurar valor predet.** y **Guardar**.

8

Administración del router

En este capítulo, se describen las funciones de administración del dispositivo, entre las que se incluyen la creación de usuarios, la administración de red, los registros y el diagnóstico del sistema, la fecha y la hora y otras configuraciones.

Configuración de complejidad de la contraseña

Su dispositivo puede imponer requisitos mínimos de complejidad de la contraseña para cambios de contraseña.

Para configurar los valores de complejidad de la contraseña:

PASO 1 Elija **Administración** > **Seguridad de la contraseña**.

PASO 2 En el campo **Configuración de complejidad de la contraseña**, marque **Habilitar**.

PASO 3 Configure los valores de complejidad de la contraseña:

Longitud mínima de la contraseña	Escriba la longitud mínima de la contraseña (0 a 64 caracteres).
Cantidad mínima de clases de caracteres	Escriba un número que represente una de las siguientes clases de caracteres: • Letras mayúsculas • Letras minúsculas • Números • Caracteres especiales disponibles en un teclado estándar De manera predeterminada, las contraseñas deben incluir caracteres de, al menos, tres de estas clases.
La contraseña nueva debe ser distinta de la actual	Marque **Habilitar** para solicitar que las contraseñas nuevas difieran de la actual.
Vencimiento de la contraseña	Marque **Habilitar** para que las contraseñas caduquen después de un tiempo especificado.
Tiempo de vencimiento de la contraseña	Escriba el número de días después de los cuales caduca la contraseña (de 1 a 365). El valor predeterminado es 180 días.

PASO 4 Haga clic en **Guardar**.

Configuración de cuentas de usuario

El dispositivo admite dos cuentas de usuario para administrar y visualizar configuraciones: un usuario administrativo (nombre de usuario y contraseña predeterminados: cisco) y un usuario invitado (nombre de usuario predeterminado: invitado).

La cuenta de invitado tiene acceso de solo lectura. Usted puede configurar y cambiar el nombre de usuario y la contraseña para la cuenta de administrador y la cuenta de invitado.

Para configurar las cuentas de usuario:

PASO 1 Elija **Administración** > **Usuarios**.

PASO 2 En el campo **Activación de cuenta**, marque las casillas de las cuentas que desea activar. La cuenta de administrador debe estar activa.

PASO 3 (Opcional) Para editar la cuenta de administrador, marque **Editar config. de administrador** en **Config. de cuenta de administrador**. Para editar la cuenta de invitado, marque **Editar config. de invitado** en **Config. de invitado**. Introduzca la siguiente información:

Nuevo nombre de usuario	Escriba un nuevo nombre de usuario.
Antigua contraseña	Escriba la contraseña actual.
Nueva contraseña	Escriba la nueva contraseña. Recomendamos que se asegure de que la contraseña no sea una palabra del diccionario de ningún idioma y que incluya una combinación de letras (tanto minúsculas como mayúsculas), números y símbolos. La contraseña puede tener hasta 64 caracteres.
Vuelva a escribir la nueva contraseña	Vuelva a escribir la nueva contraseña.

PASO 4 Para importar nombres de usuario y contraseñas de un archivo CSV:

a. En el campo **Importar nombre de usuario y contraseña**, haga clic en **Examinar**.

b. Ubique el archivo y haga clic en **Open** (Abrir).

c. Haga clic en **Importar**.

PASO 5 Escriba la contraseña anterior.

PASO 6 Haga clic en **Guardar**.

Configuración del valor del tiempo de espera de la sesión

El valor del tiempo de espera es la cantidad de minutos de inactividad que pueden transcurrir hasta que finalice la sesión del administrador de dispositivos. Usted puede configurar el tiempo de espera para las cuentas de administrador e invitado.

Para configurar el tiempo de espera de la sesión:

PASO 1 Elija **Administración** > **Tiempo de espera de la sesión**.

PASO 2 En el campo **Caducidad por inactividad de admin.**, escriba la cantidad de minutos, en número, que pueden transcurrir hasta que una sesión caduque por inactividad. Elija **nunca** para permitir que el administrador se mantenga permanentemente conectado.

PASO 3 En el campo **Caducidad por inactividad de invitado**, escriba la cantidad de minutos, en número, que pueden transcurrir hasta que una sesión caduque por inactividad. Elija **nunca** para permitir que el administrador se mantenga permanentemente conectado.

PASO 4 Haga clic en **Guardar**.

Configuración del protocolo de administración de red simple (SNMP)

El protocolo de administración de red simple (SNMP) le permite supervisar y administrar el router desde un administrador SNMP. El SNMP proporciona un medio remoto para supervisar y controlar los dispositivos de red y para administrar configuraciones, la obtención de estadísticas, el rendimiento y la seguridad.

Configuración de información del sistema SNMP

En la sección **Info. de sistema SNMP** de la página **SNMP**, usted puede habilitar el SNMP.

Para poder usarlo, instale el software SNMP en su computadora. El dispositivo admite solo SNMPv3 para administración SNMP y SNNPv1/2/3 para mensajes trampa SNMP.

Para habilitar el SNMP:

PASO 1 Elija **Administración** > **SNMP**.

PASO 2 Marque **Habilitar** para habilitar el SNMP.

PASO 3 Escriba esta información:

SysContact	Escriba el nombre de la persona de contacto para este firewall (por ejemplo, **admin** o **Juan Pérez**).
SysLocation	Escriba la ubicación física del firewall (por ejemplo, **bastidor n.º 2, 4.º piso**).
SysName	Escriba un nombre para una fácil identificación del firewall.

PASO 4 Haga clic en **Guardar**.

Edición de usuarios SNMPv3

Usted puede configurar parámetros SNMPv3 para las dos cuentas de usuario predeterminadas del dispositivo (administrador e invitado).

Para configurar los valores de SNMPv3:

PASO 1 Elija **Administración** > **SNMP**.

PASO 2 En **Config. de usuario SNMPv3**, configure los siguientes valores:

Nombre de usuario	Seleccione la cuenta que desea configurar (**administrador** o **invitado**).

Privilegio de acceso	Se muestran los privilegios de acceso de la cuenta de usuario seleccionada.
Nivel de seguridad	Elija el nivel de seguridad de SNMPv3: **Sin autenticación ni privilegios**: no se requiere ninguna autenticación ni privacidad. **Autenticación y sin privilegios**: se requiere solamente algoritmo y contraseña de autenticación. **Autenticación y privilegios**: se requiere algoritmo y contraseña de autenticación/privacidad.
Servidor de algoritmo de autenticación	Seleccione el tipo de algoritmo de autenticación (**MD5** o **SHA**).
Contraseña de autenticación	Escriba la contraseña de autenticación.
Algoritmo de privacidad	Elija el tipo de algoritmo de privacidad (**DES** o **AES**).
Contraseña de privacidad	Escriba la contraseña de privacidad.

PASO 3 Haga clic en **Guardar**.

Configuración de trampas SNMP

Los campos de la sección **Configuración de trampas SNMP** le permiten configurar un agente SNMP al que el firewall le envía mensajes trampa (notificaciones).

Para configurar las trampas:

PASO 1 Elija **Administración** > **SNMP**.

PASO 2 En **Configuración de trampas**, configure los siguientes valores:

Dirección IP	Escriba la dirección IP del administrador SNMP o agente de mensajes trampa.
Puerto	Escriba el puerto de trampas SNMP de la dirección IP a la que se enviarán los mensajes trampa.

Comunidad	Escriba la cadena de comunidad a la que pertenece el agente. La mayoría de los agentes están configurados para escuchar trampas en la comunidad pública.
Versión de SNMP	Seleccione la versión de SNMP: **v1**, **v2c** o **v3**.

PASO 3 Haga clic en **Guardar**.

Uso de herramientas de diagnóstico

El dispositivo ofrece varias herramientas de diagnóstico para ayudarlo a solucionar problemas de red.

- **Herramientas de red**
- **Configuración de duplicación de puertos**

Herramientas de red

Utilice herramientas de red para resolver problemas de la red.

Uso de PING

Usted puede usar la utilidad PING para probar la conectividad entre el router y otro dispositivo en la red. Puede, además, usar la herramienta Ping para probar la conectividad a Internet al hacer ping a un nombre de dominio totalmente calificado (como www.cisco.com).

Para usar PING:

PASO 1 Elija **Administración** > **Diagnósticos** > **Herramientas de red**.

PASO 2 En el campo **Dirección IP/Nombre de dominio**, escriba la dirección IP del dispositivo o un nombre de dominio totalmente calificado, como www.cisco.com, al que hacer ping.

PASO 3 Haga clic en **Ping**. Aparecen los resultados de ping, que le indican si el dispositivo está accesible.

PASO 4 Haga clic en **Cerrar** cuando haya terminado.

Uso de Traceroute

La utilidad Traceroute muestra todos los routers presentes entre la dirección IP de destino y este router. El router muestra hasta 30 saltos (routers intermedios) entre este router y el destino.

Para usar Traceroute:

PASO 1 Elija **Administración** > **Diagnósticos** > **Herramientas de red**.

PASO 2 En el campo **Dirección IP/Nombre de dominio**, escriba la dirección IP que desea rastrear.

PASO 3 Haga clic en **Traceroute**. Aparecen los resultados de Traceroute.

PASO 4 Haga clic en **Cerrar** cuando haya terminado.

Realización de una búsqueda de DNS

Usted puede usar la herramienta de búsqueda para encontrar la dirección IP del host (por ejemplo, un servidor web, FTP o de correo) en Internet.

Para recuperar la dirección IP de un servidor web, FTP o de correo, o de cualquier otro servidor en Internet, escriba el nombre de Internet en el cuadro de texto y haga clic en **Buscar**. Si el host o el dominio que se escribió existe, verá una respuesta con la dirección IP. Un mensaje de Host desconocido indica que el nombre de Internet especificado no existe.

Para usar la herramienta de búsqueda:

PASO 1 Elija **Administración** > **Diagnósticos** > **Herramientas de red**.

PASO 2 En el campo **Nombre de Internet**, escriba el nombre de Internet del host.

PASO 3 Haga clic en **Buscar**. Aparecen los resultados de nslookup.

PASO 4 Haga clic en **Cerrar** cuando haya terminado.

Configuración de duplicación de puertos

La duplicación de puertos supervisa el tráfico de red al enviar copias de todos los paquetes entrantes y salientes de un puerto a un puerto de supervisión. La duplicación de puertos se puede usar como una herramienta de diagnóstico o depuración, especialmente cuando se rechaza un ataque o visualiza el tráfico de usuario desde LAN hasta WAN para ver si los usuarios acceden a información o sitios web a los que no deben acceder.

El host de LAN (equipo) debe usar una dirección IP estática para evitar problemas con la duplicación de puertos. Los arrendamientos DHCP pueden vencer para un host LAN y pueden hacer que la duplicación de puertos falle si la dirección IP estática no está configurada para el host LAN.

Para configurar la duplicación de puertos:

PASO 1 Elija **Administración** > **Diagnósticos** > **Duplicación de puertos**.

PASO 2 En el campo **Duplicar origen**, seleccione los puertos que desea duplicar.

PASO 3 En el menú desplegable **Duplicar puerto**, elija un puerto para duplicar. Si usa una duplicación de puertos, no la use para ningún otro tráfico.

PASO 4 Haga clic en **Guardar**.

Configuración de registro

El Cisco RV215W le permite configurar opciones de registro.

Configuración de los valores de registro

Para configurar el registro:

PASO 1 Elija **Administración** > **Registro** > **Configuración de registro**.

PASO 2 En el campo **Modo de registro**, marque **Habilitar**.

PASO 3 Haga clic en **Agregar fila**.

PASO 4 Configure los siguientes valores:

Servidor de registro remoto	Escriba la dirección IP del servidor de registro que recopilará registros.
Gravedad de registro para correo electrónico y registro local	Haga clic para elegir la gravedad de los registros que desea configurar. Tenga en cuenta que todos los tipos de registro que están arriba de un tipo de registro seleccionado se incluyen automáticamente y no puede desactivarlos. Por ejemplo, al seleccionar registros de errores, se incluyen automáticamente los registros de emergencia, alerta y críticos, además de los registros de errores. Los niveles de gravedad de los eventos se detallan de mayor gravedad a menor gravedad, de la siguiente manera: • **Emergencia**: el sistema no se puede utilizar. • **Alerta**: se necesita acción. • **Crítico**: el sistema está en condición crítica. • **Error**: el sistema está en condición de error. • **Advertencia**: se presentó una advertencia del sistema. • **Notificación**: el sistema está funcionando correctamente, pero se presentó un aviso del sistema. • **Información**: información de dispositivos. • **Depuración**: proporciona información detallada acerca de un evento. Al seleccionar esta gravedad se usa una gran cantidad de registros para generar y no se recomienda durante el funcionamiento normal del router.
Habilitar	Para habilitar estos valores de registro, marque esta casilla.

PASO 5 Haga clic en **Guardar**.

Para editar una entrada en la **Tabla de config. de registro**, seleccione la entrada y haga clic en **Editar**. Realice sus cambios y luego haga clic en **Guardar**.

Configuración de parámetros de correo electrónico

Puede configurar el Cisco RV215W para enviar registros de eventos, nuevas alertas de firmware y alertas 3G por correo electrónico. Se recomienda configurar una cuenta de correo electrónico aparte para enviar y recibir alertas de correo electrónico.

Para configurar los parámetros de correo electrónico:

PASO 1 Elija **Administración** > **Registro** > **Config. de correo elec.**

PASO 2 En la sección **E-mail Alert Configuration** (Configuración de alerta de correo electrónico):

- Para habilitar el envío de alertas 3G por correo electrónico, marque la casilla de verificación **3G E-mail Alert Enable** (Habilitar alerta 3G de correo electrónico).
- Para habilitar el envío de registros por correo electrónico, marque la casilla de verificación **E-mail Logs Enable** (Habilitar envío de registros por correo electrónico)**.** Asegúrese de haber establecido la gravedad de los eventos que desea registrar. Para obtener más información, consulte **Configuración de los valores de registro**. El campo **Minimum E-mail Log Severity** (Gravedad mínima de registro por correo electrónico) muestra la gravedad de los registros que desea capturar. Para cambiar la gravedad del registro, haga clic en **Configure Severity** (Configurar gravedad).

  En la sección **Send E-mail Logs by Schedule** (Enviar registro c. elec. según prog.) elija si desea enviar correo electrónico **Hourly** (Por hora), **Daily** (Por día) o **Weekly** (Por semana). No se envían registros si elige la opción **Nunca**. Si opta por una programación por semana, elija un día de la semana para enviar los registros por correo electrónico. Si opta por una programación por día o por semana, elija la hora del día en la que el dispositivo debe enviar los registros por correo electrónico.

PASO 3 En la sección **E-mail Settings** (Config. de correo elec.), ingrese la siguiente información para configurar los parámetros para sus alertas de correo electrónico:

Dir. de serv. de correo elec.	Escriba la dirección del servidor SMTP. Este es el servidor de correo asociado con la cuenta de correo electrónico que ha configurado (por ejemplo, mail.companyname.com).
Puerto de serv. de correo elec.	Escriba el puerto del servidor SMTP. Si su proveedor de correo electrónico requiere un puerto especial para correo electrónico, ingréselo aquí. De lo contrario, use el predeterminado (25).
Dir. de correo elec. de devolución	Ingrese la dirección de correo electrónico de devolución a la que el Cisco RV215W enviará mensajes si las alertas enviadas desde el router no se entregan a la dirección de correo electrónico del destinatario.
Enviar a dir. de correo elec. (1)	Escriba la dirección de correo electrónico a la cual enviar alertas (por ejemplo, logging@companyname.com).
Enviar a dir. de correo elec. (2) (opcional)	Ingrese una dirección de correo electrónico adicional a la cual enviar alertas.
Enviar a dir. de correo elec. (3) (opcional)	Ingrese una dirección de correo electrónico adicional a la cual enviar alertas.
Cifrado de correo elec. (SSL)	Para habilitar el cifrado de correo electrónico, marque **Habilitar**.
Autenticación con servidor SMTP	Si el servidor SMTP (correo) solicita autenticación antes de aceptar conexiones, elija el tipo de autenticación en el menú desplegable: **Ninguna**, **INICIO DE SESIÓN**, **SENCILLO** y **CRAM-MD5**.
Nombre de usuario de autent. de c. elec.	Escriba el nombre de usuario de autenticación de correo electrónico (por ejemplo, logging@companyname.com).
Contraseña de autent. de c. elec.	Escriba la contraseña de autenticación de correo electrónico (por ejemplo, la contraseña que se usó para ingresar a la cuenta de correo electrónico que configuró para recibir alertas).

Prueba de autent. de c. elec.	Haga clic en **Test** (Prueba) para realizar la prueba de autenticación de correo electrónico.

PASO 4 En la sección **Enviar registro c. elec. según prog.**, configure los siguientes valores:

Unidad	Elija la unidad de tiempo para los registros (**Nunca**, **Por hora**, **Por día** o **Por semana**). No se envían registros si elige la opción **Nunca**.
Día	Si opta por una programación por semana para el envío de registros, elija un día de la semana en el que enviar los registros.
Hora	Si opta por una programación por día o por semana para el envío de registros, elija la hora del día a la que enviar los registros.

PASO 5 Haga clic en **Guardar**.

Configuración de Bonjour

Bonjour es un protocolo de detección y anuncios de servicios. En el Cisco RV215W, Bonjour solamente anuncia los servicios predeterminados configurados en el dispositivo cuando Bonjour está habilitado.

Para habilitar Bonjour:

PASO 1 Elija **Administración** > **Bonjour**.

PASO 2 Marque **Habilitar** para habilitar Bonjour.

PASO 3 A fin de habilitar Bonjour para una VLAN incluida en la **Tabla de control de interfaz de Bonjour**, marque la casilla de verificación correspondiente **Habilitar Bonjour**.

Usted puede habilitar Bonjour en VLAN específicas. Al habilitar Bonjour en una VLAN, los dispositivos presentes en la VLAN pueden detectar servicios Bonjour disponibles en el router (como HTTP/HTTPS).

Por ejemplo, si la ID de una VLAN es 2, los dispositivos y hosts presentes en VLAN 2 no pueden detectar servicios Bonjour que se ejecutan en el router a menos que Bonjour esté habilitado para VLAN 2.

PASO 4 Haga clic en **Guardar**.

Configuración de los valores de fecha y hora

Usted puede configurar su zona horaria, ajustar o no valores del horario de verano y con qué servidor de Protocolo de tiempo de red (NTP, Network Time Protocol) se debe sincronizar la fecha y la hora. El router luego obtiene la información de su fecha y hora del servidor NTP.

Para configurar valores de NTP y hora:

PASO 1 Elija **Administración** > **Configuración de hora**. Se muestra la hora actual.

PASO 2 Configure esta información:

Zona horaria	Seleccione su zona horaria en relación con la hora del meridiano de Greenwich (GMT).
Ajustar valores del horario de verano	Si su región lo admite, marque la casilla **Ajustar valores del horario de verano**. Esta casilla de verificación se habilita si hace clic en **Automática** en el campo **Configurar fecha y hora** a continuación.
Modo horario de verano	Seleccione **Por fecha** (introduzca la fecha específica en la que comienza el modo horario de verano) o **Recurrente** (introduzca el mes, la semana, el día de la semana y la hora en que comienza el modo horario de verano). Ingrese la información apropiada en los campos de inicio y fin del intervalo.
Desplazamiento del horario de verano	Elija el desplazamiento de la Hora Universal Coordinada (UTC) en el menú desplegable.
Configurar fecha y hora	Seleccione cómo configurar la fecha y la hora.

Servidor NTP	Para usar los servidores NTP predeterminados, haga clic en el botón **Usar predeterminado**. Para usar un servidor NTP específico, haga clic en **Servidor NTP definido por usuario** y escriba el nombre de dominio totalmente calificado o la dirección IP de los servidores NTP en los dos campos disponibles.
Escribir fecha y hora	Escriba la fecha y la hora.

PASO 3 Haga clic en **Guardar**.

Copia de respaldo y restauración del sistema

Usted puede hacer copias de respaldo de valores de configuración personalizada para una restauración posterior o restaurar la configuración personalizada a partir de una copia de respaldo anterior en la página **Administración** > **Config. de respaldo/restauración**.

Cuando el firewall funciona tal como se configuró, usted puede hacer una copia de respaldo de la configuración para una posterior restauración. Durante la copia de respaldo, la configuración se guarda en forma de archivo en su computadora. La configuración del firewall se puede restaurar a partir de este archivo.

PRECAUCIÓN Durante una operación de restauración, no intente conectarse a Internet, desactivar el firewall, apagar la computadora ni usar el firewall hasta que se haya completado la operación, que debería llevar un minuto aproximadamente. Una vez que la luz de prueba se apague, espere unos segundos más antes de usar el firewall.

Respaldo de los valores de configuración

Para realizar una copia de respaldo de la configuración o restaurarla:

PASO 1 Elija **Administración** > **Config. de respaldo/restauración**.

PASO 2 Seleccione la configuración que desea borrar o de la que quiere una copia de respaldo:

Configuración de inicio	Seleccione esta opción para descargar la configuración de inicio. La configuración de inicio es la configuración en ejecución más actual que usa el dispositivo. Si se ha perdido la configuración de inicio del router, use esta página para copiar la configuración de respaldo en la configuración de inicio y para mantener intacta toda la información de configuración previa. Usted puede descargar la configuración de inicio a otros dispositivos Cisco RV215W para una fácil implementación.
Configuración de duplicado	Seleccione esta opción para indicarle al dispositivo que haga una copia de respaldo de la configuración de inicio después de 24 horas de operación sin ninguna modificación en la configuración de inicio.
Configuración de respaldo	Seleccione esta opción para hacer una copia de respaldo de los valores de la configuración actual.

PASO 3 Para descargar el archivo de respaldo a su computadora, haga clic en **Download** (Descarga).

De manera predeterminada, el archivo (startup.cfg, mirror.cfg o backup.cfg) se descarga en la carpeta Descargas; por ejemplo, C:\Documents and Settings\admin\My Documents\Downloads\.

Para guardar un archivo de respaldo en una ubicación de una unidad USB, haga clic en **Save to USB** (Guardar en USB).

PASO 4 Para borrar la configuración seleccionada, haga clic en **Borrar**.

Restauración de los valores de configuración

Usted puede restaurar un archivo de configuración guardado anteriormente:

PASO 1 Elija **Administración** > **Config. de respaldo/restauración**.

PASO 2 En el campo Carga de configuración, seleccione la configuración que desea cargar (**Configuración de inicio** o **Configuración de respaldo**).

PASO 3 Puede cargar el archivo de configuración de su PC o de una unidad USB externa.

Para cargarlo de su computadora, haga clic en el botón de radio **PC**. Haga clic en **Examinar** para ubicar el archivo. Seleccione el archivo y haga clic en **Abrir**.

Para cargarlo de una ubicación en una unidad USB, haga clic en el botón de radio **USB**. Haga clic en **Show USB** (Mostrar USB) para visualizar todos los dispositivos USB conectados. Ubique el archivo en la unidad USB y haga clic en **Open** (Abrir).

NOTA Su dispositivo admite NTFS en modo de solo lectura, y admite los formatos de archivo FAT y FAT32 en modo de lectura/escritura en dispositivos USB.

PASO 4 Haga clic en **Iniciar la carga**.

El dispositivo carga el archivo de configuración y usa los valores que contiene para actualizar la configuración de inicio. Posteriormente, el dispositivo se reinicia y usa la nueva configuración.

Copia de los valores de configuración

Copie la configuración de inicio en la configuración de respaldo para asegurarse de contar con una copia de respaldo en caso de que olvide su nombre de usuario y contraseña y no pueda acceder al Administrador de dispositivos. En este caso, la única manera de ingresar nuevamente al Administrador de dispositivos es restablecer el dispositivo para que vuelva a los valores predeterminados de fábrica.

El archivo de configuración de respaldo permanece en la memoria y permite que la información de la configuración de la que se hizo copia de respaldo se copie en la configuración de inicio, que restablece todos los valores.

Para copiar una configuración (por ejemplo, para copiar una configuración de inicio en la configuración de respaldo):

PASO 1 Elija **Administración** > **Config. de respaldo/restauración**.

PASO 2 En el campo **Copiar**, elija las configuraciones de origen y de destino en los menús desplegables.

PASO 3 Haga clic en **Iniciar la copia**.

Generación de una clave de cifrado

El router le permite generar una clave de cifrado para proteger los archivos de respaldo.

Para generar una clave de cifrado:

PASO 1 Elija **Administración** > **Config. de respaldo/restauración**.

PASO 2 Haga clic en **Mostrar config. avanzada**.

PASO 3 En la casilla, escriba la frase simiente para generar la clave.

PASO 4 Haga clic en **Guardar**.

Actualización del firmware o cambio de idioma

Puede actualizar el firmware a una versión más reciente o cambiar el idioma del router con la página **Administración** > **Actualización del firmware/idioma**.

PRECAUCIÓN Durante una actualización del firmware, no intente conectarse a Internet, desactivar el dispositivo, apagar la computadora ni interrumpir el proceso de ninguna manera hasta que se haya completado la operación, que dura un minuto aproximadamente, incluido el proceso de reinicio. La interrupción del proceso de actualización en momentos específicos cuando se escribe en la memoria flash puede dañar esta última y hacer que el router resulte inutilizable.

Actualización automática del firmaware

PASO 1 Elija **Administration** (Administración) > **Firmware/Language Upgrade** (Actualización de firmware/idioma).

PASO 2 En la sección **Automatic Firmware Upgrade** (Actualización automática del firmware), seleccione la frecuencia con que desea que el dispositivo busque actualizaciones del firmware, en el campo **Interval - Check every** (Intervalo: Comprobar cada).

PASO 3 En el campo **Automatically Upgrade** (Actualización automática), elija si desea actualizar al firmware más reciente inmediatamente después de que se detecta una versión nueva o en un momento especificado.

PASO 4 Para ser notificado cuando haya nuevo firmware disponible o una vez actualizado al firmware más reciente, marque una de las siguientes casillas de verificación:

- **Notify via Admin GUI** (Notificar a través de GUI de administración): reciba notificaciones en la GUI de administración de RV215W en el próximo inicio de sesión.
- **Email to** (Enviar correo electrónico a): reciba notificaciones mediante alertas de correo electrónico. Haga clic en **Email Address** (Dirección de correo electrónico) para configurar parámetros de correo electrónico. Esta casilla de verificación está atenuada si la opción **New Firmware E-mail Alert** (Alerta de correo electrónico de nuevo firmware) no está habilitada. Para obtener más información, consulte **Configuración de parámetros de correo electrónico**.

PASO 5 Haga clic en **Guardar**.

Actualización automática de firmware/configuración desde un dispositivo USB

Para actualizar en forma automática su firmware y configuración desde un dispositivo USB:

PASO 1 Elija **Enable** (Habilitar) en el campo **Upgrade from USB drive when device powers on** (Actualizar desde unidad USB cuando se inicia el dispositivo).

Con este ajuste de implementación automatizada, si se inserta el dispositivo USB:

- El firmware en su dispositivo se actualiza automáticamente cuando se inicia el dispositivo.
- El archivo de configuración se carga automáticamente cuando se inicia el dispositivo y cuando el dispositivo se restablece a los valores predeterminados de fábrica.

PASO 2 Haga clic en **Guardar**.

Actualización manual del firmware

PASO 1 Elija **Administration** (Administración) > **Firmware/Language Upgrade** (Actualización de firmware/idioma).

PASO 2 En la sección **Manual Firmware/Language Upgrade** (Actualización manual de firmware/idioma), haga clic en el botón de radio **Firmware Image** (Imagen de firmware) en el campo **File Type** (Tipo de archivo).

PASO 3 Descargue el firmware más reciente a su PC o a un dispositivo USB. Para descargar la versión más reciente del firmware desde cisco.com a un dispositivo USB, haga clic en **Start Download** (Inicio de descarga) en **Save to USB from cisco.com** (Guardar en USB desde cisco.com).

PASO 4 Para actualizar a la versión más reciente del firmware, elija una de las siguientes opciones para realizar la actualización:

- **cisco.com**: descargue el firmware desde el sitio web de cisco.com.
- **PC**: haga clic en **Browse** (Examinar) para ubicar y seleccionar el firmware descargado en su computadora.
- **USB**: haga clic en **Show USB** (Mostrar USB) para visualizar todos los archivos de su dispositivo USB, en la **Tabla de contenido de USB**. Ubique y seleccione el archivo del firmware.

NOTA Su dispositivo admite NTFS en modo de solo lectura, y admite los formatos de archivo FAT y FAT32 en modo de lectura/escritura en dispositivos USB.

PRECAUCIÓN Al restablecer el dispositivo de modo que vuelva a los valores predeterminados de fábrica, se borran todos sus parámetros de configuración.

PASO 5 Haga clic en **Iniciar actualización**.

Una vez validada la imagen del firmware nuevo, la nueva imagen se guarda en la memoria flash del dispositivo y el router se reinicia automáticamente con el firmware nuevo. La sección **System Information** (Información del sistema) muestra el firmware más reciente.

Cambio del idioma

Para cambiar el idioma:

PASO 1 Elija **Administración** > **Actualización del firmware/idioma**.

PASO 2 En el campo **Tipo de archivo**, haga clic en el botón **Archivo de idioma**.

PASO 3 Haga clic en **Examinar** para ubicar y seleccionar el archivo de idioma.

PASO 4 Opcionalmente, para restaurar los parámetros de configuración del dispositivo a los valores predeterminados de fábrica, seleccione **Reset all configuration/ settings to factory defaults** (Restablecer toda la configuración a los valores predet. de fábrica).

PASO 5 Haga clic en **Iniciar actualización**.

Reinicio del Cisco RV215W

Para reiniciar el router:

PASO 1 Elija **Administración** > **Reiniciar**.

PASO 2 Haga clic en **Reiniciar**.

Restauración de los valores predeterminados de fábrica

PRECAUCIÓN Durante una operación de restauración, no intente conectarse a Internet, desactivar el router, apagar la computadora ni usar el router hasta que se haya completado la operación, que debería llevar un minuto aproximadamente. Una vez que la luz de prueba se apague, espere unos segundos más antes de usar el router.

Para restaurar los valores predeterminados de fábrica en el router:

PASO 1 Elija **Administración** > **Restaurar valores predet. de fábrica**.

PASO 2 Haga clic en **Predeterminado**.

Ejecución del asistente de instalación

Para ejecutar el asistente de instalación:

PASO 1 Elija **Administración** > **Asistente de instalación**.

PASO 2 Siga las instrucciones en línea.

A

Utilización del software QuickVPN de Cisco

Información general

En este apéndice, se explica cómo instalar y utilizar el software QuickVPN de Cisco, que se puede descargar de Cisco.com. QuickVPN funciona con computadoras que ejecutan Windows 7, Windows XP, Windows Vista o Windows 2000. (Las computadoras que tengan otros sistemas operativos deberán utilizar software VPN de otra empresa).

En este apéndice, se incluyen las siguientes secciones:

- **Antes de empezar**
- **Instalación del software QuickVPN de Cisco**
- **Utilización del software QuickVPN de Cisco**

Antes de empezar

El programa QuickVPN solo funciona con un router que esté configurado correctamente para aceptar una conexión QuickVPN. Debe realizar los siguientes pasos:

PASO 1 Habilite la administración remota. Consulte **Configuración de los parámetros básicos de firewall**.

PASO 2 Cree cuentas de usuario QuickVPN. Consulte **Configuración de PPTP**. Una vez creada una cuenta de usuario, el cliente QuickVPN podrá utilizar las credenciales.

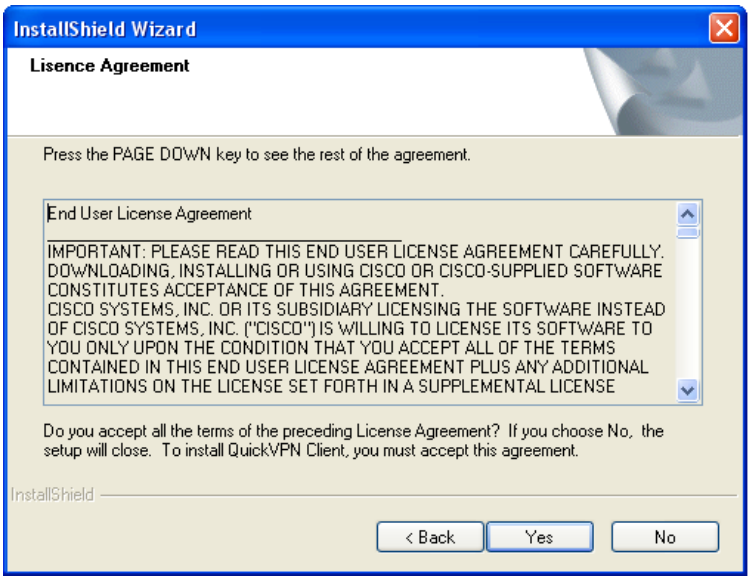
Instalación del software QuickVPN de Cisco

Instalación desde el CD-ROM

PASO 1 Introduzca el CD-ROM Cisco RV215W en la unidad de CD-ROM. Una vez que se inicie el Asistente de instalación, haga clic en el enlace **Install QuickVPN** (Instalar QuickVPN).

Aparece la ventana License Agreement (Contrato de licencia).

Ventana License Agreement



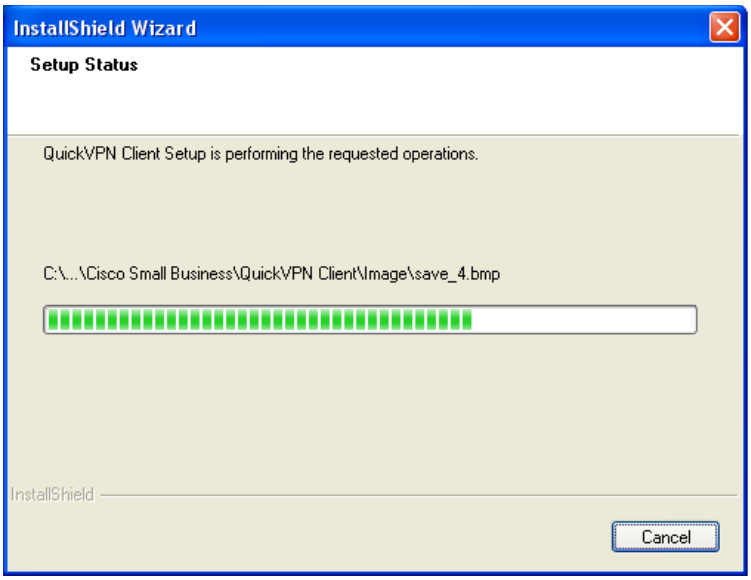
PASO 2 Haga clic en **Yes** (Sí) para aceptar el contrato.

PASO 3 Haga clic en **Examinar** y elija dónde copiar los archivos (por ejemplo, C:\Cisco Small Business\QuickVPN Client).

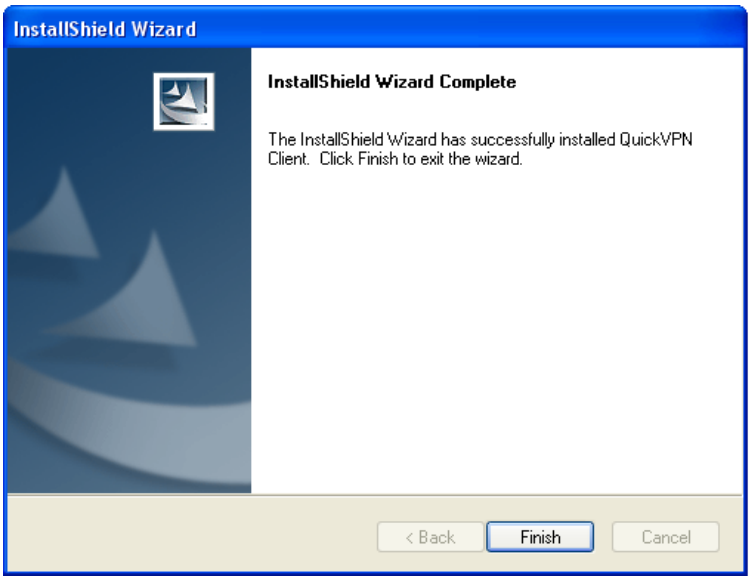
PASO 4 Haga clic en **Next** (Siguiente).

El Asistente de configuración copia los archivos en la ubicación elegida.

Copia de archivos



Finalización de la instalación de archivos



PASO 5 Haga clic en **Finish** (Finalizar) para completar la instalación. Continúe con **?$paratext>? en la p?ina 147**.

Descarga e instalación de Internet

PASO 1 En **Ap?dice B, ?$paratext>?** vaya al enlace Software Downloads (Descargas de software).

PASO 2 Escriba Cisco RV215W en la casilla de búsqueda y encuentre el software **QuickVPN**.

PASO 3 Guarde el archivo zip en su computadora y extraiga el archivo .exe.

PASO 4 Haga doble clic en el archivo .exe y siga las instrucciones que aparecen en la pantalla.

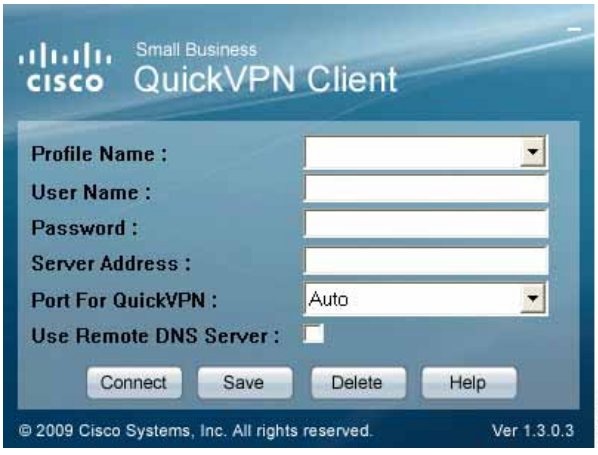
Utilización del software QuickVPN de Cisco

PASO 1 Haga doble clic en el ícono de QuickVPN de Cisco que aparece en su escritorio o en la bandeja del sistema.

QuickVPN Desktop Icon

QuickVPN Tray Icon—
No Connection

Aparece la ventana de inicio de sesión de QuickVPN.



PASO 2 En el campo **Profile Name** (Nombre de perfil), escriba un nombre para su perfil.

PASO 3 En los campos **User Name** (Nombre de usuario) y **Password** (Contraseña), escriba el nombre de usuario y la contraseña.

PASO 4 En el campo **Dirección del servidor**, escriba la dirección IP o el nombre de dominio del Cisco RV215W.

PASO 5 En el campo **Port For QuickVPN** (Puerto para QuickVPN), escriba el número de puerto que el cliente QuickVPN utiliza para comunicarse con el router VPN remoto o conserve la configuración predeterminada **Auto** (Automática).

PASO 6 Para guardar este perfil, haga clic en **Save** (Guardar).

Para eliminar este perfil, haga clic en **Delete** (Eliminar). Para obtener más información, haga clic en **Help** (Ayuda).

NOTA Si existen varios sitios para los que deba crear un túnel, puede crear varios perfiles, pero solo un túnel puede estar activo por vez.

PASO 7 Para iniciar su conexión QuickVPN, haga clic en **Connect** (Conectar).

El progreso de la conexión muestra: Connecting (Conectando), Provisioning (Abasteciendo), Activating Policy (Activando la política) y Verifying Network (Verificando la red).

PASO 8 Una vez que se establece la conexión QuickVPN, el ícono de la bandeja de QuickVPN se torna color verde y aparece la ventana de estado de QuickVPN.

En ella se muestran la dirección IP del extremo remoto del túnel VPN, la hora y la fecha de inicio del túnel VPN y el tiempo total que el túnel VPN ha estado activo.

Para finalizar el túnel VPN, haga clic en **Disconnect** (Desconectar). Si desea modificar su contraseña, haga clic en **Change Password** (Cambiar contraseña). Para obtener más información, haga clic en **Help** (Ayuda).

PASO 9 Si hizo clic en **Cambiar contraseña** y tiene permiso para modificar su propia contraseña, aparece la ventana **Establecer conexión privada virtual**.

PASO 10 Escriba su contraseña en el campo **Old Password** (Contraseña anterior). Escriba su nueva contraseña en el campo **New Password** (Nueva contraseña). Luego, escriba su nueva contraseña en el campo **Confirm New Password** (Confirmar nueva contraseña).

PASO 11 Haga clic en **OK** (Aceptar) para guardar la nueva contraseña.

NOTA Usted puede modificar su contraseña solo si se ha marcado la casilla **Allow User to Change Password** (Permitir a usuario cambiar la contraseña) para el nombre de usuario correspondiente.

B

Cómo seguir

Asistencia técnica	
Comunidad de Soporte Cisco	www.cisco.com/go/smallbizsupport
Asistencia técnica y documentación en línea (se debe iniciar sesión)	www.cisco.com/support
Contactos de asistencia técnica telefónica	www.cisco.com/en/US/support/tsd_cisco_small_business_support_center_contacts.html
Descargas de software (se debe iniciar sesión)	Vaya a tools.cisco.com/support/downloads e introduzca el número de modelo en la casilla Buscar software.

Documentación del producto	
Wireless-N VPN Firewall	www.cisco.com/en/US/products/ps9923/tsd_products_support_series_home.html
Central para socios Cisco (deberá iniciar sesión como socio)	www.cisco.com/web/partners/sell/smb
Mercado	www.cisco.com/go/marketplace