



370111

# GUÍA DE ADMINISTRACIÓN

## Cisco
Router RV320/RV325 Gigabit Dual WAN VPN

# Contents

# 1

# Introducción

Los ajustes predeterminados son suficientes para muchas pequeñas empresas. Los requisitos de red o del proveedor de servicios de Internet (ISP) pueden exigir modificaciones en los ajustes. Para usar la interfaz web, se necesita un equipo con Internet Explorer (versión 6 o posterior), Firefox o Safari (para Mac).

Para abrir la interfaz web:

**PASO 1** Conecte un equipo a un puerto LAN numerado del dispositivo. Si el equipo está configurado para convertirse en un cliente DHCP, se asigna a dicho equipo una dirección IP incluida en el rango de 192.168.1.x.

**PASO 2** Inicie el navegador web.

**PASO 3** En la barra de direcciones, escriba la dirección IP predeterminada del dispositivo, **192.168.1.1**. El navegador puede mostrar una advertencia que indica que el sitio web no es de confianza. Continúe para acceder al sitio web.

**PASO 4** Cuando se muestre la página inicio de sesión, especifique el nombre de usuario predeterminado **cisco** y la contraseña predeterminada **cisco** (en minúscula).

**PASO 5** Haga clic en **Inicio de sesión**. Se muestra la página **Resumen del sistema**. Compruebe la **actividad de puerto** para ver si hay una conexión WAN que esté habilitada. De no ser así, continúe con el siguiente paso.

**PASO 6** En la página Resumen del sistema, haga clic en **Asistente para la configuración** para utilizar el asistente a fin de configurar la conexión a Internet. También puede hacer clic en **Asistente** en el árbol de navegación y seleccionar **Iniciar ahora** en la sección Configuración básica. Siga las instrucciones que aparezcan en pantalla.

Si el navegador web muestra un mensaje de advertencia sobre la ventana emergente, indique que se permita el contenido bloqueado.

**PASO 7** Para configurar otros ajustes, use los enlaces del árbol de navegación.

### Sugerencias para la solución de problemas

Si tiene problemas para conectarse a Internet o a la interfaz web:

- Compruebe que el navegador web no esté configurado para trabajar sin conexión.
- Compruebe los ajustes de la conexión de la red de área local para el adaptador Ethernet. El equipo debe obtener una dirección IP a través de DHCP. Como alternativa, el equipo puede tener una dirección IP estática incluida en el rango 192.168.1.x con la gateway predeterminada configurada con 192.168.1.1 (la dirección IP predeterminada del dispositivo).
- Compruebe que haya especificado los ajustes correctos en el asistente para configurar la conexión a Internet.
- Reinicie el módem y el dispositivo apagándolos. A continuación, encienda el módem y déjelo inactivo durante unos 2 minutos. A continuación, encienda el dispositivo. Ahora debería recibir una dirección IP de WAN.
- Si tiene un módem DSL, pida al ISP que lo configure en el modo de puente.

## Características de la interfaz de usuario

La interfaz de usuario está diseñada para facilitar los procesos de configuración y administración del dispositivo.

### Navegación

Los módulos principales de la interfaz web están representados mediante botones en el panel de navegación de la izquierda. Haga clic en un botón para ver más opciones. Haga clic en una opción para abrir una página.

### Ventanas emergentes

Algunos enlaces y botones abren ventanas emergentes en las que se muestra más información o páginas de configuración relacionadas. Si el navegador web muestra un mensaje de advertencia sobre la ventana emergente, indique que se permita el contenido bloqueado.

### Ayuda

Para ver información acerca de la página de configuración seleccionada, haga clic en **Ayuda**, junto a la esquina superior derecha de la interfaz web. Si el navegador web muestra un mensaje de advertencia sobre la ventana emergente, indique que se permita el contenido bloqueado.

### Cierre de sesión

Para salir de la interfaz web, haga clic en **Cierre de sesión**, junto a la esquina superior derecha de la interfaz web. Se muestra la página **Inicio de sesión**.

# 2

# Asistente

La página Asistente se utiliza para iniciar el asistente para la configuración básica que le orientará durante el proceso de configuración inicial del dispositivo. El asistente Regla de acceso ofrece orientación durante el proceso de configuración de la directiva de seguridad para la red.

**Configuración básica**

Use el asistente para la configuración básica con objeto de cambiar el número de puertos WAN o configurar la conexión a Internet.

Haga clic en **Iniciar ahora** para ejecutar el asistente para la configuración básica. Siga las instrucciones que aparezcan en pantalla para continuar. Consulte la información que le proporcione el ISP para especificar los ajustes necesarios para la conexión.

**Configuración de regla de acceso**

Use el asistente Configuración de regla de acceso para crear las reglas de acceso del cortafuegos. Haga clic en **Iniciar ahora** para ejecutar el asistente Configuración de regla de acceso. El asistente proporciona información sobre las reglas predeterminadas para este dispositivo. Siga las instrucciones que aparezcan en pantalla para continuar.

# 2

# Asistente

3

# Resumen del sistema

En Resumen del sistema se muestra información acerca del estado actual de las conexiones, el estado, los ajustes y los registros del dispositivo.

## Información del sistema

Descripciones de la información del sistema:

- **Número de serie**: número de serie del dispositivo.
- **Versión de firmware**: número de versión del firmware instalado.
- **PID VID**: número de versión del hardware.
- **Suma de comprobación MD5**: valor que se usa para la validación de los archivos.
- **Máscara de subred/IP de LAN (IPv4)**: dirección IP de administración de IPv4 y máscara de subred del dispositivo.
- **LAN IPv6/ Prefix** (Prefijo/LAN IPv6): prefijo y dirección IP de administración de IPv6.
- **Modo de operación**: controla el comportamiento del dispositivo con respecto a la conexión WAN. El modo de gateway se selecciona cuando el dispositivo aloja una conexión WAN de Internet. El modo de router se selecciona cuando el dispositivo está en una red que no tiene una conexión WAN o cuando se utiliza otro dispositivo para establecer la conexión WAN. Si desea cambiar este parámetro, haga clic en **Modo de operación** para que se muestre la ventana Enrutamiento avanzado.
- **Tiempo de funcionamiento del sistema**: periodo de tiempo en días, horas y minutos que lleva activo el dispositivo.

# Configuración (Asistente)

Para acceder al asistente para la configuración de la conexión a Internet y recibir orientación sobre el proceso, haga clic en **Asistente para la configuración** para iniciar el **Asistente**.

# Actividad de puerto

La opción Actividad de puerto permite identificar las interfaces de los puertos e indica el estado de cada puerto:

- **Id. de puerto**: etiqueta del puerto.
- **Interfaz**: tipo de interfaz, que puede ser LAN, WAN o DMZ. Si hay varias interfaces de WAN, se indican mediante un número, por ejemplo, WAN1 o WAN2.
- **Estado**: estado del puerto, que puede estar Deshabilitado (rojo), Habilitado (negro) o Conectado (verde). El valor que representa el estado es un hipervínculo. Haga clic en él para abrir la ventana **Port Information** (Información del puerto).

# IPv4 e IPv6

La sección IPv4 o IPv6 muestra las estadísticas de cada puerto WAN (la ficha IPv6 está disponible cuando la opción IP con pila dual está habilitada en la página **Configuración de red**).

**Información de WAN**

Se proporciona la siguiente información de WAN:

- **Dirección IP**: dirección IP pública de esta interfaz.
- **Gateway predeterminada**: gateway predeterminada de esta interfaz.
- **DNS**: dirección IP del servidor DNS de esta interfaz.
- **DNS dinámico**: configuración de DDNS para este puerto, que puede ser Habilitado o Deshabilitado.

# Estado de seguridad

En esta sección se muestra el estado de las funciones de seguridad:

- **SPI (inspección de paquetes con estado)**: estado del cortafuegos, que puede ser Activado (verde) o Desactivado (rojo). Permite realizar un seguimiento del estado de las conexiones de red (por ejemplo, los flujos de TCP y la comunicación de UDP) que pasan por el cortafuegos. El cortafuegos distingue los paquetes legítimos para los distintos tipos de conexiones. Solo los paquetes que coinciden con una conexión activa conocida pueden pasar por el cortafuegos; los que no, se rechazan.
- **DoS (denegación de servicio)**: estado del filtro de DoS, que puede ser Activado (verde) o Desactivado (rojo). Un ataque de DoS constituye un intento de hacer que una máquina o un recurso de red no estén disponibles para los usuarios a los que están destinados.
- **Bloquear solicitud de WAN**: dificulta a los usuarios externos el acceso a la red, ya que *oculta* los puertos de red a los dispositivos de Internet e impide que otros usuarios de Internet detecten el tráfico de red o que puedan hacer un "ping". El estado puede ser Activado (verde) o Desactivado (rojo).
- **Administración remota**: indica si se debe permitir o denegar una conexión remota cuyo objetivo sea administrar el dispositivo. Si el estado es Activado (verde), significa que se permite la administración remota. Si el estado es Desactivado (negro), significa que no se permite la administración remota.
- **Regla de acceso**: número de reglas de acceso que se han definido.

Para mostrar información detallada acerca de la función de seguridad, haga clic en la etiqueta correspondiente a dicha función.

# Estado de configuración VPN

En esta sección se muestra el estado de los túneles VPN:

- **Túneles de VPN usados**: túneles VPN en uso.
- **Túneles de VPN disponibles**: túneles VPN disponibles.
- **Túneles de Easy VPN usados**: túneles Easy VPN en uso.
- **Túneles de Easy VPN disponibles**: túneles Easy VPN disponibles.

- **Túneles de PPTP usados**: túneles de PPTP (Point-to-Point Tunneling Protocol, protocolo de tunelización de punto a punto) en uso. PPTP es un método para implementar redes privadas virtuales. PPTP utiliza un canal de control sobre TCP y un túnel GRE (Generic Routing Encapsulation, encapsulado de enrutamiento genérico) para encapsular los paquetes PPP.
- **Túneles de PPTP disponibles**: túneles PPTP disponibles.

## Estado de ajuste de registro

En esta sección se muestra el estado de los registros:

- **Servidor Syslog**: estado de Syslog, que puede ser Activado (verde) o Desactivado (rojo).
- **Enviar registro por correo electrónico**: estado del registro de correo electrónico, que puede ser Activado (verde) o Desactivado (rojo).

# 4

# Configuración

La página Configuración permite ver las opciones de configuración del router. Use la página Configuración > Red para configurar una red LAN, WAN (Internet), DMZ, etc.

## Configuración de red

Algunos ISP requieren que se asigne un nombre de host y un nombre de dominio para identificar el dispositivo. Se proporcionan valores predeterminados que se pueden cambiar si es necesario:

- **Nombre del host**: mantenga el ajuste predeterminado o escriba el nombre de host que especifique el ISP.
- **Nombre de dominio**: mantenga el ajuste predeterminado o escriba el nombre de dominio que especifique el ISP.

### Modo de IP

Elija el tipo de direccionamiento que se debe usar en las redes:

- **Solo IPv4**: solo direccionamiento IPv4.
- **IP con pila dual**: direccionamiento IPv4 e IPv6. Después de guardar los parámetros, puede configurar direcciones IPv4 e IPv6 para las redes LAN, WAN y DMZ.

### Adición o edición de una red IPv4

De forma predeterminada, hay una subred LAN IPv4 configurada (192.168.1.1). Normalmente, una subred es suficiente para la mayoría de las pequeñas empresas. El cortafuegos deniega el acceso si una dirección IP de origen de un dispositivo LAN está en una subred que no tenga un permiso específico. Puede permitir el tráfico desde otras subredes y usar este dispositivo como un router perimetral que proporcione conectividad de Internet a una red.

**PASO 1** Haga clic en la ficha **IPv4** para mostrar la Tabla de varias subredes.

**PASO 2** Para agregar una subred, haga clic en **Agregar**. Los campos Dirección IP y Máscara de subred se muestran en las columnas. Después de hacer clic en **Guardar**, podrá editar la subred para que forme parte de una VLAN, administrar las direcciones IP a través del servidor DHCP o definir los parámetros del servidor TFTP.

**PASO 3** Especifique los valores oportunos en los campos **Dirección IP** y **Máscara de subred** del dispositivo.

**PASO 4** Haga clic en **Guardar** para guardar los cambios o haga clic en **Cancelar** para deshacerlos.

Para editar una subred, seleccione la subred IPv4 que desee modificar y haga clic en **Editar**. En la sección **Configuración de DHCP** se describe el proceso para modificar los parámetros de la subred.

### Edición del prefijo de las direcciones IPv6

Si previamente ha habilitado IP con pila dual en el campo Modo de IP, podrá configurar el prefijo IPv6.

Para configurar el prefijo IPv6, haga clic en la ficha **IPv6**, seleccione el prefijo IPv6 y haga clic en **Editar**. La dirección IP predeterminada es fc00::1. La longitud predeterminada del prefijo es 7. La ficha IPv6 está disponible únicamente si **IP con pila dual** está habilitado en la tabla **Modo de IP**. Se abre la ventana **Configuración de DHCP**.

## Ajustes de los puertos WAN

La tabla Ajuste de WAN muestra la interfaz (por ejemplo, USB1, WAN1 o WAN2) y el tipo de conexión. Los ajustes de las interfaces se pueden modificar.

**NOTA** Si está utilizando IPv6, seleccione la ficha **IPv6** antes de seleccionar la interfaz WAN que desee configurar. De lo contrario, los parámetros de IPv6 no se mostrarán en la ventana **Ajustes de conexión WAN**.

Para configurar **Ajustes de conexión WAN**, seleccione una interfaz WAN y haga clic en **Editar**. Se muestra **Ajustes de conexión WAN**.

Seleccione **Tipo de conexión WAN** en el menú y modifique los parámetros relacionados, tal y como se describe en estas secciones:

**Obtener una IP automáticamente**

Elija esta opción si el ISP asigna dinámicamente una dirección IP al dispositivo (la mayoría de los abonados a módems por cable utilizan este tipo de conexión). El ISP asigna la dirección IP del dispositivo para este puerto, incluidas las direcciones IP del servidor DNS.

Para especificar un servidor DNS, active la casilla **Utilizar las siguientes direcciones del servidor DNS** y especifique la dirección IP del **servidor DNS 1**. Si lo desea, también puede especificar un segundo servidor DNS. Se utiliza el primer servidor DNS disponible.

Para definir automáticamente el tamaño de la **MTU** (Maximum Transmission Unit, unidad de transmisión máxima), seleccione la opción **Automático**. En caso contrario, para configurar manualmente el tamaño de la **MTU**, seleccione **Manual** y especifique el tamaño de la MTU (el tamaño en bytes de la unidad de datos de protocolo más grande que puede pasar la capa).

Para configurar los parámetros de IPv6, seleccione la opción **Habilitar**. Se habilitan las solicitudes y los procesos del cliente DHCPv6 para la delegación de prefijos a través de la interfaz seleccionada. Use esta opción si el ISP puede enviar prefijos LAN usando DHCPv6. Si el ISP no admite esta opción, configure manualmente un prefijo LAN:

**NOTA** Si la opción DHCP-PD está habilitada, el direccionamiento manual IPv6 de la red LAN estará deshabilitado. Si la opción DHCP-PD está deshabilitada, el direccionamiento manual IPv6 de la red LAN estará habilitado.

- **Dirección LAN IPv6**: prefijo IPv6 global que el ISP asigna a los dispositivos LAN, si procede. (Póngase en contacto con el ISP para obtener más información).
- **Longitud del prefijo**: longitud del prefijo IPv6. La red IPv6 (subred) se identifica mediante los bits iniciales de la dirección a los que se denomina "prefijo". Todos los hosts de la red tienen los mismos bits iniciales en sus direcciones IPv6. Especifique el número de bits iniciales comunes en las direcciones de red. La longitud predeterminada del prefijo es 64.
- **Asignación de prefijo LAN**:
  - **Sin acción alguna**: no se proporcionan direcciones IPv6 Sin estado ni Con estado para los equipos de la red LAN.
  - **Configurar a RA automáticamente**: se proporcionan direcciones IPv6 *Sin estado* para los equipos de la red LAN.
  - **Configurar a DHCPv6 automáticamente**: se proporcionan direcciones IPv6 *Con estado* para los equipos de la red LAN.
  - Configurar a RA y DHCPv6 automáticamente: se proporcionan direcciones IPv6 Sin estado y Con estado para los equipos de la red LAN.

**IP estática**

Elija esta opción si el ISP ha asignado una dirección IP permanente a la cuenta. Especifique los ajustes que haya proporcionado el ISP:

- **Especifique la dirección IP de WAN**: dirección IP que el ISP ha asignado a la cuenta.
- **Máscara de subred (IPv4)**: máscara de subred.
- **Dirección de gateway predeterminada**: dirección IP de la gateway predeterminada.

Para especificar un servidor DNS, escriba la dirección IP del **servidor DNS 1**. Si lo desea, también puede especificar un segundo servidor DNS. Se utiliza el primer servidor DNS disponible.

Para definir automáticamente el tamaño de la **MTU** (Maximum Transmission Unit, unidad de transmisión máxima), seleccione la opción **Automático**. En caso contrario, para configurar manualmente el tamaño de la **MTU**, seleccione **Manual** y especifique el tamaño de la MTU (el tamaño en bytes de la unidad de datos de protocolo más grande que puede pasar la capa).

Para configurar los parámetros de IPv6:

- **Dirección LAN IPv6**: prefijo IPv6 global que el ISP asigna a los dispositivos LAN, si procede. (Póngase en contacto con el ISP para obtener más información).
- **Longitud del prefijo**: longitud del prefijo IPv6. La red IPv6 (subred) se identifica mediante los bits iniciales de la dirección a los que se denomina "prefijo". Todos los hosts de la red tienen los mismos bits iniciales en sus direcciones IPv6. Especifique el número de bits iniciales comunes en las direcciones de red. La longitud predeterminada del prefijo es 64.
- **Asignación de prefijo LAN**
  - **Sin acción alguna**: no se proporcionan direcciones IPv6 Sin estado ni Con estado para los equipos de la red LAN.
  - **Configurar a RA automáticamente**: se proporcionan direcciones IPv6 *Sin estado* para los equipos de la red LAN.
  - **Configurar a DHCPv6 automáticamente**: se proporcionan direcciones IPv6 *Con estado* para los equipos de la red LAN.
  - **Configurar a RA y DHCPv6 automáticamente**: se proporcionan direcciones IPv6 Sin estado y Con estado para los equipos de la red LAN.

**PPPoE**

Elija esta opción si el ISP utiliza PPPoE (Point-to-Point Protocol over Ethernet, protocolo punto a punto a través de Ethernet) para establecer las conexiones de Internet (normalmente para líneas DSL). A continuación, especifique los ajustes que haya proporcionado el ISP:

- **Nombre de usuario** y **Contraseña**: nombre de usuario y contraseña para la cuenta del ISP. El número máximo de caracteres para cada entrada es de 255.
- **Nombre del servicio**: nombre para referirse al conjunto de servicios que proporciona el ISP.
- **Temporizadores de conexión**: la conexión se desconecta después de un periodo de inactividad.
  - **Conexión a petición**: cuando esta función está habilitada, el dispositivo establece automáticamente la conexión. Si ha habilitado esta función, especifique un valor para **Tiempo máx. inact.**, es decir, el número de

minutos que puede estar inactiva la conexión antes de que se le ponga fin. El tiempo máximo predeterminado de inactividad es de 5 minutos.

- **Mantener activo**: el router siempre está conectado a Internet. Cuando se selecciona esta opción, el router mantiene la conexión activa mediante el envío periódico de algunos paquetes de datos. Esta opción permite mantener la conexión activa de forma indefinida, incluso cuando el enlace queda inactivo durante un extenso periodo de tiempo. Si habilita esta función, también deberá especificar un valor para **Periodo de remarcado** para determinar la frecuencia con la que el router comprueba la conexión a Internet. El periodo predeterminado es de 30 segundos.

- **Utilizar las siguientes direcciones del servidor DNS**: permite obtener información sobre la conexión desde los servidores DNS.
- **Servidor DNS 1** y **Servidor DNS 2**: dirección IP de los servidores DNS. Si lo desea, también puede especificar un segundo servidor DNS. Se utiliza el primer servidor DNS disponible.
- **MTU**: tamaño de la unidad de transmisión máxima (**MTU**, Maximum Transmission Unit). Seleccione **Automático** para que el tamaño se defina automáticamente. En caso contrario, para configurar manualmente el tamaño de la **MTU**, seleccione **Manual** y especifique el tamaño de la MTU (el tamaño en bytes de la unidad de datos de protocolo más grande que puede pasar la capa).

Para configurar los parámetros de IPv6, seleccione la opción **Habilitar**. Se habilitan las solicitudes y los procesos del cliente DHCPv6 para la delegación de prefijos a través de la interfaz seleccionada. Use esta opción si el ISP puede enviar prefijos LAN usando DHCPv6. Si el ISP no admite esta opción, configure manualmente un prefijo LAN:

**NOTA** Si la opción DHCP-PD está habilitada, el direccionamiento manual IPv6 de la red LAN estará deshabilitado. Si la opción DHCP-PD está deshabilitada, el direccionamiento manual IPv6 de la red LAN estará habilitado.

- **Dirección LAN IPv6**: prefijo IPv6 global que el ISP asigna a los dispositivos LAN, si procede. (Póngase en contacto con el ISP para obtener más información).
- **Longitud del prefijo**: longitud del prefijo IPv6. La red IPv6 (subred) se identifica mediante los bits iniciales de la dirección a los que se denomina "prefijo". Todos los hosts de la red tienen los mismos bits iniciales en sus direcciones IPv6. Especifique el número de bits iniciales comunes en las direcciones de red. La longitud predeterminada del prefijo es 64.

- **Asignación de prefijo LAN**:
  - **Sin acción alguna**: no se proporcionan direcciones IPv6 Sin estado ni Con estado para los equipos de la red LAN.
  - **Configurar a RA automáticamente**: se proporcionan direcciones IPv6 *Sin estado* para los equipos de la red LAN.
  - **Configurar a DHCPv6 automáticamente**: se proporcionan direcciones IPv6 *Con estado* para los equipos de la red LAN.
  - **Configurar a RA y DHCPv6 automáticamente**: se proporcionan direcciones IPv6 Sin estado y Con estado para los equipos de la red LAN.

**PPTP (IPv4)**

Elija esta opción si así se lo solicita el ISP. PPTP (Point-to-Point Tunneling Protocol, protocolo de túnel punto a punto) es un servicio que se usa en Europa e Israel.

- **Especifique la dirección IP de WAN**: dirección IP que el ISP ha asignado a la cuenta.
- **Máscara de subred (IPv4)**: máscara de subred asignada a la cuenta.
- **Dirección de gateway predeterminada**: dirección IP de la gateway predeterminada.
- **Nombre de usuario** y **Contraseña**: nombre de usuario y contraseña para la cuenta del ISP. El número máximo de caracteres es 60.
- **Temporizadores de conexión**: la conexión se desconecta después de un periodo de inactividad.
  - **Conexión a petición**: cuando esta función está habilitada, el dispositivo establece automáticamente la conexión. Si ha habilitado esta función, especifique un valor para **Tiempo máx. inact.**, es decir, el número de minutos que puede estar inactiva la conexión antes de que se le ponga fin. El tiempo máximo predeterminado de inactividad es de 5 minutos.
  - **Mantener activo**: el router siempre está conectado a Internet. Cuando se selecciona esta opción, el router mantiene la conexión activa mediante el envío periódico de algunos paquetes de datos. Esta opción permite mantener la conexión activa de forma indefinida, incluso cuando el enlace queda inactivo durante un extenso periodo de tiempo. Si habilita esta función, también deberá especificar un valor para **Periodo de remarcado** para determinar la frecuencia con la que el router

comprueba la conexión a Internet. El periodo predeterminado es de 30 segundos.

- **MTU**: tamaño de la unidad de transmisión máxima (**MTU**, Maximum Transmission Unit). Seleccione **Automático** para que el tamaño se defina automáticamente. En caso contrario, para configurar manualmente el tamaño de la **MTU**, seleccione **Manual** y especifique el tamaño de la MTU (el tamaño en bytes de la unidad de datos de protocolo más grande que puede pasar la capa).

**Puente transparente (IPv4)**

Elija esta opción si está usando este router para conectar dos segmentos de red. Solo se puede definir una interfaz WAN como puente transparente.

- **Especifique la dirección IP de WAN**: la dirección IP externa que el ISP ha asignado a la cuenta.
- **Máscara de subred**: máscara de subred que especifica el ISP.
- **Dirección de gateway predeterminada**: dirección IP de la gateway predeterminada.
- **Servidor DNS 1** y **Servidor DNS 2**: direcciones IP de los servidores DNS. Si lo desea, también puede especificar un segundo servidor DNS. Se utiliza el primer servidor DNS disponible.
- **Rango de IP de LAN interna**: rango de IP de LAN interna establecido como puente. Las redes WAN y LAN del puente transparente deben estar en la misma subred.
- **MTU**: tamaño de la unidad de transmisión máxima (**MTU**, Maximum Transmission Unit). Seleccione **Automático** para que el tamaño se defina automáticamente. En caso contrario, para configurar manualmente el tamaño de la **MTU**, seleccione **Manual** y especifique el tamaño de la MTU (el tamaño en bytes de la unidad de datos de protocolo más grande que puede pasar la capa).

**Configuración automática de dirección sin estado (IPv6)**

Elija esta opción si el ISP utiliza anuncios y solicitudes de router de IPv6. Los hosts averigüan a qué red están conectados y, una vez que lo hagan, pueden configurar automáticamente un Id. de host en dicha red.

Para especificar un servidor DNS, escriba la dirección IP del **servidor DNS 1**. Si lo desea, también puede especificar un segundo servidor DNS. Se utiliza el primer servidor DNS disponible.

Para definir automáticamente el tamaño de la **MTU** (Maximum Transmission Unit, unidad de transmisión máxima), seleccione la opción **Automático**. En caso contrario, para configurar manualmente el tamaño de la **MTU**, seleccione **Manual** y especifique el tamaño de la MTU (el tamaño en bytes de la unidad de datos de protocolo más grande que puede pasar la capa).

Para configurar los parámetros de IPv6:

- **Dirección LAN IPv6**: prefijo IPv6 global que el ISP asigna a los dispositivos LAN, si procede. (Póngase en contacto con el ISP para obtener más información).
- **Longitud del prefijo**: longitud del prefijo IPv6. La red IPv6 (subred) se identifica mediante los bits iniciales de la dirección a los que se denomina "prefijo". Todos los hosts de la red tienen los mismos bits iniciales en sus direcciones IPv6. Especifique el número de bits iniciales comunes en las direcciones de red. La longitud predeterminada del prefijo es 64.
- **Asignación de prefijo LAN**:
  - **Sin acción alguna**: no se proporcionan direcciones IPv6 Sin estado ni Con estado para los equipos de la red LAN.
  - **Configurar a RA automáticamente**: se proporcionan direcciones IPv6 *Sin estado* para los equipos de la red LAN.
  - **Configurar a DHCPv6 automáticamente**: se proporcionan direcciones IPv6 *Con estado* para los equipos de la red LAN.
  - **Configurar a RA y DHCPv6 automáticamente**: se proporcionan direcciones IPv6 Sin estado y Con estado para los equipos de la red LAN.

**Túnel IPv6 en IPv4 (IPv6)**

Elija esta opción si el ISP utiliza un túnel IPv6 en IPv4 para establecer las conexiones de Internet.

Debe especificar una dirección **IP estática** IPv4. A continuación, especifique los ajustes que haya proporcionado el ISP:

- **Dirección IPv6 local**: dirección IPv6 local de la cuenta del ISP.
- **Dirección IPv4 remota**: dirección IPv4 remota de la cuenta del ISP.
- **Dirección IPv6 remota**: dirección IPv6 remota de la cuenta del ISP.
- **Servidor DNS 1** y **Servidor DNS 2**: direcciones IP de los servidores DNS. Si lo desea, también puede especificar un segundo servidor DNS. Se utiliza el primer servidor DNS disponible.

- **Dirección LAN IPv6**: prefijo IPv6 global que el ISP asigna a los dispositivos LAN, si procede. (Póngase en contacto con el ISP para obtener más información).
- **Longitud del prefijo**: longitud del prefijo IPv6. La red IPv6 (subred) se identifica mediante los bits iniciales de la dirección a los que se denomina "prefijo". Todos los hosts de la red tienen los mismos bits iniciales en sus direcciones IPv6. Especifique el número de bits iniciales comunes en las direcciones de red. La longitud predeterminada del prefijo es 64.
- **Asignación de prefijo LAN**
  - **Sin acción alguna**: no se proporcionan direcciones IPv6 Sin estado ni Con estado para los equipos de la red LAN.
  - **Configurar a RA automáticamente**: se proporcionan direcciones IPv6 *Sin estado* para los equipos de la red LAN.
  - **Configurar a DHCPv6 automáticamente**: se proporcionan direcciones IPv6 *Con estado* para los equipos de la red LAN.
  - **Configurar a RA y DHCPv6 automáticamente**: se proporcionan direcciones IPv6 Sin estado y Con estado para los equipos de la red LAN.

**Túnel 6to4 (IPv6)**

Elija esta opción para establecer un túnel automáticamente en una red IPv4 (o una conexión de Internet IPv4 real) a través de dos redes IPv6 independientes. Especifique los siguientes parámetros:

**Dirección IPv4 de retransmisión**: permite que un host 6to4 se comunique con Internet IPv6 nativo. Debe tener una gateway IPv6 predeterminada definida en una dirección 6to4 que contenga la dirección IPv4 de un router de retransmisión 6to4. Para evitar que los usuarios tengan que realizar la configuración manualmente, se ha asignado la dirección anycast `192.88.99.1` para enviar paquetes a un router de retransmisión 6to4.

- **Servidor DNS 1** y **Servidor DNS 2**: direcciones IP de los servidores DNS. Si lo desea, también puede especificar un segundo servidor DNS. Se utiliza el primer servidor DNS disponible.
- **Dirección LAN IPv6**: prefijo IPv6 global que el ISP asigna a los dispositivos LAN, si procede. (Póngase en contacto con el ISP para obtener más información).

- **Longitud del prefijo**: longitud del prefijo IPv6. La red IPv6 (subred) se identifica mediante los bits iniciales de la dirección a los que se denomina "prefijo". Todos los hosts de la red tienen los mismos bits iniciales en sus direcciones IPv6. Especifique el número de bits iniciales comunes en las direcciones de red. La longitud predeterminada del prefijo es 64.
- **Asignación de prefijo LAN**
  - **Sin acción alguna**: no se proporcionan direcciones IPv6 Sin estado ni Con estado para los equipos de la red LAN.
  - **Configurar a RA automáticamente**: se proporcionan direcciones IPv6 *Sin estado* para los equipos de la red LAN.
  - **Configurar a DHCPv6 automáticamente**: se proporcionan direcciones IPv6 *Con estado* para los equipos de la red LAN.
  - **Configurar a RA y DHCPv6 automáticamente**: se proporcionan direcciones IPv6 Sin estado y Con estado para los equipos de la red LAN.

**Túnel IPv6 Rapid Deployment (6rd) (IPv6)**

Elija esta opción si el ISP utiliza un túnel 6rd (IPv6 Rapid Deployment, implementación rápida de IPv6) para establecer las conexiones de Internet. Especifique los ajustes que haya proporcionado el ISP.

- **Modo de configuración 6rd**:
  - **Manual**: defina manualmente los valores del prefijo de 6rd, la dirección IPv4 de retransmisión y la longitud de la máscara IPv4, según los datos que proporcione el ISP.
  - **Automático (DHCP)**: use DHCP (opción 212) para obtener el prefijo de 6rd, la dirección IPv4 de transmisión y la longitud de la máscara IPv4.
- **Prefijo de 6rd**: el prefijo de 6rd de la cuenta del ISP.
- **Dirección IPv4 de retransmisión**: dirección IPv4 de retransmisión de la cuenta del ISP.
- **Longitud de máscara de IPv4**: longitud de la máscara de subred de IPv4 de 6rd para la cuenta del ISP. (Normalmente este valor es 0).
- **Servidor DNS 1** y **Servidor DNS 2**: direcciones IP de los servidores DNS. Si lo desea, también puede especificar un segundo servidor DNS. Se utiliza el primer servidor DNS disponible.

- **Dirección LAN IPv6**: prefijo IPv6 global que el ISP asigna a los dispositivos LAN, si procede. (Póngase en contacto con el ISP para obtener más información).
- **Longitud del prefijo**: longitud del prefijo IPv6. La red IPv6 (subred) se identifica mediante los bits iniciales de la dirección a los que se denomina "prefijo". Todos los hosts de la red tienen los mismos bits iniciales en sus direcciones IPv6. Especifique el número de bits iniciales comunes en las direcciones de red. La longitud predeterminada del prefijo es 64.
- **Asignación de prefijo LAN**
  - **Sin acción alguna**: no se proporcionan direcciones IPv6 Sin estado ni Con estado para los equipos de la red LAN.
  - **Configurar a RA automáticamente**: se proporcionan direcciones IPv6 *Sin estado* para los equipos de la red LAN.
  - **Configurar a DHCPv6 automáticamente**: se proporcionan direcciones IPv6 *Con estado* para los equipos de la red LAN.
  - **Configurar a RA y DHCPv6 automáticamente**: se proporcionan direcciones IPv6 Sin estado y Con estado para los equipos de la red LAN.

## Ajustes de los puertos USB1 o USB2

La configuración de los puertos USB administra la conexión entre este dispositivo y la llave USB. También administra la conmutación por error de los puertos WAN (redundancia). Algunas llaves USB configuran sus credenciales de forma automática. Sin embargo, otras (como la llave Verizon UML290VW 4G) requieren una configuración manual. Consulte la documentación del fabricante para obtener más información sobre la llave.

### Conexión 3G/4G

Para establecer una conexión 3G o 4G, especifique los siguientes valores:

- **Código PIN** y **Confirmar código PIN**: código PIN asociado a la tarjeta SIM. Este campo solo se muestra para las tarjetas SIM GSM.
- **Nombre de punto de acceso**: red de Internet a la que se conecta el dispositivo móvil. Especifique el nombre de punto de acceso que le indique el proveedor de servicios de red móvil. Si desconoce el nombre del punto de acceso, póngase en contacto con el proveedor de servicios.

- **Número de marcado**: número proporcionado por el proveedor de servicios de red móvil para la conexión de Internet.
- **Nombre de usuario** y **Contraseña**: nombre de usuario y contraseña proporcionados por el proveedor de servicios de red móvil.
- **Habilitar DNS**: seleccione esta casilla para habilitar DNS.
- **Servidor DNS (obligatorio)** y **Servidor DNS (opcional)**: direcciones IP de los servidores DNS. Si lo desea, también puede especificar un segundo servidor DNS. Se utiliza el primer servidor DNS disponible.
- **MTU**: tamaño de la unidad de transmisión máxima (**MTU**, Maximum Transmission Unit). Seleccione **Automático** para que el tamaño se defina automáticamente. En caso contrario, para configurar manualmente el tamaño de la **MTU**, seleccione **Manual** y especifique el tamaño de la MTU (el tamaño en bytes de la unidad de datos de protocolo más grande que puede pasar la capa).

### Ajustes de conmutación por error y recuperación

Aunque Ethernet y el enlace de red móvil estén disponibles, solo se puede usar una conexión cada vez para establecer un enlace WAN. Cada vez que se produce un fallo en una conexión WAN, el dispositivo intenta establecer otra conexión en otra interfaz. Esta función se denomina *conmutación por error*. Cuando se restaura la conexión WAN principal, se vuelve a utilizar dicha ruta y se abandona la conexión de respaldo. Esta función se denomina *recuperación*.

**PASO 1** Para mostrar la ventana Failover & Recovery (Conmutación por error y recuperación), haga clic en **Configuración** > **Red**.

**PASO 2** Seleccione un puerto USB y haga clic en **Editar**. Se abre la ventana Red.

**PASO 3** Haga clic en la ficha **USB Failover** (Conmutación por error de USB) y especifique los siguientes datos:

- **Modo operativo**: cuando un enlace WAN Ethernet se queda inactivo, el dispositivo intenta activar el enlace de red móvil en la interfaz USB. Configure el comportamiento de conmutación por error:
  - Espera activa de conmutación por error 3G/4G: en caso de que se pierda una conexión en un puerto WAN Ethernet, se redirige el tráfico de la WAN mediante un enlace USB 3G o 4G. La llave USB está activada mientras se está en modo de espera.

- Espera pasiva de conmutación por error 3G/4G: en caso de que se pierda una conexión en un puerto WAN Ethernet, se redirige el tráfico de la WAN mediante un enlace USB 3G o 4G. La llave USB está desactivada mientras se está en modo de espera.
- Modo principal: el enlace 3G/4G se usa como conexión WAN principal.

▪ **Calidad de la señal**: refleja la intensidad de la señal entre la llave USB 3G/4G y el punto de acceso. Haga clic en **Actualizar** para actualizar el valor.

**PASO 4** Para evitar que se produzca un exceso de datos, seleccione **Recuento de cargos**. La opción **Tráfico (KB)** permite realizar un seguimiento del volumen de datos enviados o recibidos en kilobytes a través del enlace USB. **Hora (min.)** muestra los minutos que lleva activa la conexión 3G/4G.

▪ Si elige Tráfico (KB), especifique los siguientes datos:

- **Premium**: coste en dólares para un volumen de datos concreto.
- **Cargo extra**: coste en dólares por kilobyte de datos si se excede un volumen concreto.
- **Detener conexión...**: al seleccionar esta opción, la conexión se interrumpe cuando el volumen es superior al valor especificado.

▪ Si elige Hora (min.), especifique los siguientes datos:

- **Premium**: coste en dólares para un periodo de tiempo concreto.
- **Cargo extra**: coste en dólares si se excede un periodo de tiempo concreto.
- **Detener conexión...**: al seleccionar esta opción, la conexión se interrumpe cuando el tiempo es superior al valor especificado.

Se abre la ventana:

▪ **Tiempo acumulado anterior**: cantidad de tiempo que lleva activa la conexión 3G/4G desde la última vez que se reinició.

▪ **Tiempo acumulado actual**: cantidad de tiempo transcurrido desde que el dispositivo inició una conexión 3G/4G.

▪ **Cargar**: coste estimado de la conexión desde que se restablecieron los contadores.

**PASO 5** Defina los comportamientos de **Diagnóstico**:

- **Reiniciar recuento el día**: seleccione esta opción y especifique el día del mes en el que se deben reiniciar los contadores. Si el valor es superior al número de días del mes (por ejemplo, si se especifica el valor 31 en un mes que tenga 30 días), los contadores se reiniciarán el último día del mes.
- **Autoprueba diaria a las**: seleccione esta opción y especifique la hora del día (24 horas) en la que se debe probar la conexión. Se considera que el resultado de la autoprueba es satisfactorio si el dispositivo puede obtener una dirección IP del proveedor de servicios. Los fallos que se produzcan se recopilan en un registro.
- **Registro de autoprueba**: seleccione esta opción para registrar los resultados de las autopruebas (todos los resultados de las pruebas se envían al registro).

**PASO 6** Haga clic en **Guardar** para guardar estos ajustes.

# Habilitar DMZ

DMZ es una subred que está abierta al público, pero oculta tras un cortafuegos. Una DMZ permite redirigir los paquetes que llegan al puerto WAN a una dirección IP específica de la LAN. Se pueden configurar reglas del cortafuegos para que permitan el acceso a puertos y servicios específicos de DMZ desde la LAN o la WAN. Si se produce un ataque en alguno de los nodos de DMZ, no tiene por qué afectar necesariamente a la LAN. Se recomienda que los hosts que deben exponerse en la WAN (como los servidores de correo electrónico o web) se coloquen en la red DMZ.

Para configurar DMZ:

**PASO 1** Elija **Configuración** > **Red** y seleccione la opción **Habilitar DMZ**. Aparece un mensaje.

**PASO 2** Haga clic en **Sí** para aceptar el cambio.

**PASO 3** Seleccione la interfaz de DMZ en la tabla **Ajustes de DMZ** y haga clic en **Editar**. Se abre la ventana **Editar conexión DMZ**.

**PASO 4** Seleccione **Subred** para identificar una subred para los servicios de DMZ. Además, especifique la **dirección IP de DMZ** y la **máscara de subred**. También puede seleccionar **Rango** para reservar un grupo de direcciones IP en la misma subred para los servicios de DMZ y especificar el rango de direcciones IP.

**PASO 5** Haga clic en **Guardar**.

# Contraseña

El nombre de usuario y la contraseña permiten el acceso administrativo al dispositivo. El nombre de usuario es **cisco**. La contraseña predeterminada es **cisco**. El nombre de usuario y la contraseña se pueden cambiar. Recomendamos encarecidamente que se cambie la contraseña predeterminada por una contraseña segura.

Si la administración remota está habilitada en la página **General** (Cortafuegos), *deberá* cambiar la contraseña.

**PRECAUCIÓN** La contraseña no se puede recuperar si se pierde o se olvida. En caso de que la contraseña se pierda o se olvide, el dispositivo deberá restablecerse a los ajustes predeterminados, lo que eliminará todos los cambios de configuración. Si accede al dispositivo de forma remota y lo restablece a los valores predeterminados, no podrá iniciar sesión en el dispositivo hasta que haya establecido un enlace local con cable en la misma subred.

Después de cambiar el nombre de usuario o la contraseña, se cierra la sesión. Tendrá que iniciar sesión de nuevo en el dispositivo con las nuevas credenciales.

**Para cambiar el nombre de usuario o la contraseña:**

**PASO 1** Elija **Configuración**>**Contraseña**.

**PASO 2** En el campo **Nombre de usuario**, escriba el nuevo nombre de usuario. Para mantener el nombre de usuario actual, deje este campo en blanco.

**PASO 3** En el campo **Contraseña anterior**, escriba la contraseña actual. Esto es obligatorio si desea cambiar el nombre de usuario y conservar la contraseña actual.

**NOTA** Si va a cambiar el nombre de usuario y a mantener la contraseña actual, deje en blanco los campos **Nueva contraseña** y **Confirmar la nueva contraseña**.

**PASO 4** En el campo **Nueva contraseña**, escriba la nueva contraseña para el dispositivo. Use una combinación de caracteres alfanuméricos y símbolos. La contraseña no debe incluir espacios. Vuelva a especificar la nueva contraseña en el campo **Confirmar la nueva contraseña**. Las dos contraseñas deben coincidir.

**PASO 5** Seleccione **Habilitar** para activar la configuración de complejidad de la contraseña:

**Para configurar los ajustes de complejidad de contraseña:**

**PASO 1** En el campo **Ajustes de complejidad de contraseña**, marque la casilla **Habilitar**.

**PASO 2** Configure los campos siguientes:

| | |
|---|---|
| Longitud mínima de la contraseña | Especifique la longitud mínima que debe tener la contraseña (entre 0 y 64 caracteres). El valor mínimo predeterminado es 8. |
| Número mínimo de clases de caracteres | Especifique el número de clases de caracteres que debe incluir la contraseña. De forma predeterminada, la contraseña debe contener caracteres de, al menos, tres de estas clases:<br>▪ Letras mayúsculas<br>▪ Letras minúsculas<br>▪ Números<br>▪ Caracteres especiales disponibles en un teclado estándar |
| La contraseña nueva debe ser distinta a la actual | Marque la opción **Habilitar** si la nueva contraseña debe ser diferente de la actual. |

| | |
|---|---|
| Medidor de seguridad de la contraseña | El **Medidor de seguridad** indica cuán segura es la contraseña según las reglas de complejidad. El nivel de seguridad varía entre rojo (inaceptable), amarillo (aceptable) y verde (seguro. |
| Momento de caducidad de contraseña | Especifique los días que deben transcurrir para que caduque la contraseña (entre 1 y 365). El valor predeterminado es 180 días. |

**PASO 3** .En el campo **Tiempo de espera de la sesión**, escriba el número de minutos después de los que debe caducar la sesión. Guarde los cambios

**PASO 4** Haga clic en **Guardar**.

# Hora

La hora es fundamental para un dispositivo de red a fin de que se reflejen correctamente las marcas horarias en los registros del sistema y los mensajes de error, y para que las transferencias de datos se puedan sincronizar con otros dispositivos de red.

Puede configurar la zona horaria, ajustar o no el horario de verano y configurar con qué servidor NTP (Network Time Protocol, protocolo de hora de red) se debe sincronizar la fecha y la hora. A continuación, el router obtendrá la información de fecha y hora del servidor NTP.

Para configurar los ajustes de NTP y de la hora, elija **Configuración** > **Hora**.

- **Zona horaria**: zona horaria relativa a la Hora del meridiano de Greenwich (GMT).
- **Horario de verano**: habilite o deshabilite el ajuste para el horario de verano. Especifique la fecha de inicio en los campos **Desde** y la de finalización en los campos **Hasta**.

- **Establecer fecha y hora**: la opción **Automático** habilita el servidor NTP. Si elige Automático, especifique el FQDN (Fully Qualified Domain Name, nombre de dominio completo) del **Servidor NTP** o la dirección IP. La opción **Manual** permite configurar la fecha y la hora de forma local. Se utiliza el reloj del dispositivo para mantener la hora. Si elige la opción **Manual**, especifique un valor para **Fecha y hora**.

# Host DMZ

El host DMZ permite que un host de la LAN expuesto a Internet pueda usar servicios como los juegos en línea y las videoconferencias. El acceso al host DMZ desde Internet se puede restringir usando reglas de acceso del cortafuegos.

Para configurar un host DMZ, escriba un valor en **Dirección IP privada de DMZ** y haga clic en **Guardar**.

# Reenvío (de puertos)

El reenvío de puertos permite el acceso público a servicios en dispositivos de red en la LAN abriendo un puerto específico o un rango de puertos para un servicio, por ejemplo, un FTP. El redireccionamiento de puertos abre un rango de puertos para servicios como los juegos en Internet que utilizan puertos alternativos para establecer la comunicación entre el servidor y el host LAN.

**Configuración de reenvío de puertos**

Cuando los usuarios efectúan solicitudes de servicios en la red, el dispositivo reenvía esas solicitudes a los servidores basándose en los parámetros de reenvío de puertos. Los servicios que no estén especificados no podrán acceder. Por ejemplo, cuando el número de puerto 80 (HTTP) se reenvía a la dirección IP 192.168.1.2, todas las solicitudes HTTP de la interfaz se reenvían a 192.168.1.2. El resto del tráfico se rechaza, a menos que lo autorice específicamente otra entrada.

Use esta función para establecer servidores web o FTP. Especifique una dirección IP válida (para ejecutar un servidor de Internet, puede que sea necesario utilizar una dirección IP estática). Para mayor seguridad, los usuarios externos pueden comunicarse con el servidor, pero no pueden conectarse con los dispositivos de red.

Para agregar un servicio a una tabla o editarlo:

**PASO 1** Para agregar un servicio, haga clic en **Agregar** en la tabla de retransmisión de rango de puertos.

Para editar un servicio, seleccione la fila y haga clic en **Editar**.

Los campos se abren para que sea posible modificarlos.

**PASO 2** Configure lo siguiente:

- En el menú desplegable, seleccione un **servicio** (si un servicio no aparece en la lista, podrá modificar la lista siguiendo las instrucciones que aparecen en la sección **Adición o edición de un nombre de servicio**).
- Especifique la **dirección IP** del servidor.
- Seleccione la opción que desee en **Interfaz**.
- Seleccione un valor en **Estado**. Seleccione la casilla para habilitar el servicio. Para deshabilitar el servicio, desactive la casilla.

**PASO 3** Haga clic en **Guardar**.

### Adición o edición de un nombre de servicio

Para agregar una entrada a la lista Servicio o editarla:

**PASO 1** Haga clic en **Administración de servicios**. Si el navegador web muestra una advertencia sobre la ventana emergente, indique que se permita el contenido bloqueado.

**PASO 2** Para agregar un servicio, haga clic en **Agregar** en la tabla de administración de servicios.

Para editar un servicio, seleccione la fila y haga clic en **Editar**.

Los campos se abren para que sea posible modificarlos. Si el navegador web muestra una advertencia sobre la ventana emergente, indique que se permita el contenido bloqueado.

**PASO 3** Puede haber 30 servicios en la lista como máximo:

- **Nombre del servicio**: descripción breve.
- **Protocolo**: protocolo obligatorio. Consulte la documentación del servicio que desee alojar.

- **Rango de puertos**: rango de números de puerto reservados para este servicio.

**PASO 4** Haga clic en **Guardar**.

### Configuración de redireccionamiento de puertos

El redireccionamiento de puertos permite al dispositivo supervisar los datos salientes para números de puerto específicos. El dispositivo recuerda la dirección IP del cliente que ha enviado los datos coincidentes. Cuando los datos solicitados se devuelve mediante el dispositivo, los datos se transmiten al cliente adecuado usando la dirección IP y las reglas de asignación de puertos.

Algunos juegos o aplicaciones de Internet utilizan puertos poco habituales para las comunicaciones entre el servidor y el host LAN. Para usar estas aplicaciones, especifique el puerto de redireccionamiento (saliente) y el puerto entrante alternativo en la tabla de redireccionamiento de puertos.

Para agregar un nombre de aplicación a una tabla o editarlo:

**PASO 1** Haga clic en **Configuración** > **Reenvío**.

**PASO 2** Para agregar un nombre de aplicación, haga clic en **Agregar** en la tabla de retransmisión de rango de puertos.

Para editar un nombre de aplicación, seleccione la fila y haga clic en **Editar**. Los campos se abren para que sea posible modificarlos.

Si el navegador web muestra una advertencia sobre la ventana emergente, indique que se permita el contenido bloqueado.

**PASO 3** Configure lo siguiente:

- **Nombre de aplicación**: nombre de la aplicación.
- **Rango de puerto redireccionado**: números de los puertos de inicio y de finalización del rango de puerto direccionado. Consulte la documentación de la aplicación para obtener más información.
- **Rango de puerto entrante**: números de los puertos de inicio y de finalización del rango de puerto entrante. Consulte la documentación de la aplicación para obtener más información.

**PASO 4** Haga clic en **Guardar**.

### Eliminación de una entrada de la tabla

Para eliminar entradas de la tabla, haga clic en las entradas que desee eliminar y elija **Eliminar**.

## Conversión de dirección de puerto

PAT (Port Address Translation, conversión de dirección de puerto) es una extensión de NAT (Network Address Translation, traducción de direcciones de red) que permite que varios dispositivos de una LAN se asignen a una única dirección IP pública para preservar las direcciones IP.

PAT es similar al reenvío de puertos, excepto por el hecho de que un paquete entrante con puerto de destino (puerto externo) se traduce en un puerto de destino diferente de paquete (puerto interno). El proveedor de servicios de Internet (ISP) asigna una única dirección IP al dispositivo perimetral. Cuando un equipo inicia sesión en Internet, este dispositivo asigna al cliente un número de puerto que se anexa a la dirección IP interna, por lo que el equipo tendrá una dirección IP exclusiva.

Si otro equipo inicia sesión en Internet, este dispositivo le asigna la misma dirección IP pública, pero con un número de puerto diferente. Aunque los dos equipos comparten la misma dirección IP pública, este dispositivo sabe a qué equipo debe enviar sus paquetes, porque el dispositivo usa los números de puerto para asignar a los paquetes la dirección IP interna exclusiva de los equipos.

Para agregar o editar PAT:

**PASO 1** Para agregar un servicio, haga clic en **Agregar** en la tabla de conversión de dirección de puerto.

Para editar un servicio, seleccione la fila y haga clic en **Editar**. Los campos se abren para que sea posible modificarlos.

Si el navegador web muestra una advertencia sobre la ventana emergente, indique que se permita el contenido bloqueado.

**PASO 2** En el menú desplegable, seleccione el **servicio**. Puede tener 30 servicios como máximo (si un servicio no aparece en la lista, podrá modificar la lista siguiendo las instrucciones que aparecen en la sección **Adición o edición de un nombre de servicio**).

**PASO 3** Especifique la dirección IP o el nombre del dispositivo de red en el que reside el servicio.

**PASO 4** Haga clic en **Guardar**.

### Adición o edición de un nombre de servicio

Para agregar una entrada a la lista Servicio o editarla:

**PASO 1** Haga clic en **Administración de servicios**. Si el navegador web muestra una advertencia sobre la ventana emergente, indique que se permita el contenido bloqueado.

**PASO 2** Para agregar un servicio, haga clic en **Agregar** en la tabla de administración de servicios.

Para editar un servicio, seleccione la fila y haga clic en **Editar**. Los campos se abren para que sea posible modificarlos.

Si el navegador web muestra una advertencia sobre la ventana emergente, indique que se permita el contenido bloqueado.

**PASO 3** Puede haber 30 servicios en la lista como máximo:

- **Nombre del servicio**: descripción breve.
- **Protocolo**: protocolo obligatorio. Consulte la documentación del servicio que desee alojar.
- **Puerto externo**: número de puerto externo.
- **Puerto interno**: número de puerto interno.

**PASO 4** Haga clic en **Guardar**.

## Configuración de NAT uno a uno

La configuración de NAT uno a uno crea una relación que asigna una dirección IP de WAN válida a las direcciones IP LAN que están ocultas para la WAN (Internet) mediante NAT. Esto protege a los dispositivos LAN para evitar que se detecten y sufran ataques.

Para obtener los mejores resultados, reserve direcciones IP para los recursos internos a los que desee llegar mediante NAT uno a uno.

Puede asignar una única dirección IP LAN o un rango de direcciones IP a un rango externo de direcciones IP de WAN de la misma longitud (por ejemplo, tres direcciones internas y tres direcciones externas). La primera dirección interna se asigna a la primera dirección externa, la segunda dirección IP interna se asigna a la segunda dirección externa, y así sucesivamente.

Para habilitar esta función, seleccione la opción **Habilitar**.

Para agregar una entrada a la lista, haga clic en **Agregar** y especifique la siguiente información:

- **Comienzo de rango privado**: dirección IP de inicio del rango de direcciones IP internas que desea asignar al rango público. No incluya la dirección IP de administración del router en este rango.
- **Comienzo de rango público**: dirección IP de inicio del rango de direcciones IP públicas que proporciona el ISP. No incluya la dirección IP de WAN del router en este rango.
- **Longitud de rango**: número de direcciones IP del rango. La longitud de rango no puede superar el número de direcciones IP válidas. Para asignar una única dirección, escriba 1.

Para modificar una entrada, selecciónela y haga clic en **Editar**. La información aparece en los campos de texto. Realice los cambios oportunos y haga clic en **Guardar**.

# Clonación de direcciones MAC

Algunos ISP requieren que se registre una dirección MAC (el código de identificación exclusivo de 12 dígitos que está asignado a cada dispositivo de red). Si previamente ha registrado una dirección MAC diferente para el dispositivo con el ISP, podrá seleccionar esta función para clonar dicha dirección en el dispositivo. De lo contrario, deberá ponerse en contacto con el ISP para cambiar la dirección MAC registrada.

**NOTA** Cuando se habilita la opción Clon de dirección MAC, la réplica de puertos no funciona.

Para clonar una dirección MAC:

**PASO 1** Haga clic en el botón de opción **Interfaz**.

**PASO 2** Haga clic en **Editar** para que se muestre la página Editar clon de dirección MAC.

- **Dirección MAC de WAN definida por el usuario**: haga clic en el botón de opción y especifique los 12 dígitos de la dirección MAC que registró previamente con el ISP.
- **Dirección MAC de este PC**: haga clic aquí para usar la dirección MAC del equipo como la dirección MAC clonada para el dispositivo.

**PASO 3** Haga clic en **Guardar**.

# DNS dinámico

El servicio DDNS (Dynamic Domain Name System, sistema de nombre de dominio dinámico) asigna un nombre de dominio fijo a una dirección IP de WAN dinámica, para que pueda alojar su propia página web, un servidor FTP u otro tipo de servidor TCP/IP en la LAN. Seleccione esta función para configurar las interfaces WAN con su información DDNS.

Antes de configurar un DNS dinámico en el router, se recomienda visitar www.dyndns.org y registrar un nombre de dominio (el servicio lo proporciona DynDNS.org). Los usuarios de China deben visitar www.3322.org para registrarse.

Después de seleccionar una interfaz y hacer clic en **Editar**, se muestra la página Editar configuración de DNS dinámico.

Para editar el servicio DDNS:

**PASO 1** En la lista **DDNS Service** (Servicio DDNS), elija un servicio.

**PASO 2** Especifique la información de la cuenta:

- **Nombre de usuario**: nombre de usuario de la cuenta DDNS. Si no ha registrado un nombre de host, haga clic en **Registrar** para acceder al sitio web DynDNS.com, donde podrá registrarse de forma gratuita en el servicio DNS dinámico.
- **Contraseña**: contraseña de la cuenta DDNS.
- **Nombre del host**: nombre de host registrado con el proveedor DDNS. Por ejemplo, si su nombre de host es *myhouse.dyndns.org*, escriba *myhouse* en el primer campo, *dyndns* en el segundo y *org* en el último campo.

Se muestra la siguiente información de solo lectura:

- **Dirección IP de Internet**: dirección IP de WAN para la interfaz.
- **Estado**: estado de DDNS. Si la información de estado indica que hay un error, compruebe que haya introducido correctamente la información de la cuenta en el servicio DDNS.

**PASO 3** Haga clic en **Guardar**.

# Enrutamiento avanzado

Esta función permite el enrutamiento dinámico y permite agregar rutas estáticas a la tabla de enrutamiento IPv4 e IPv6.

Para ver la tabla de enrutamiento, haga clic en **View Routing Table** (Ver tabla de enrutamiento). Haga clic en **Actualizar** para actualizar los datos. Haga clic en **Cerrar** para cerrar la ventana emergente.

## Configuración de enrutamiento dinámico

El enrutamiento dinámico permite construir automáticamente tablas de enrutamiento en función de la información que transportan los protocolos de enrutamiento. Además, permite que la red actúe prácticamente de forma autónoma a la hora de evitar fallos de red y bloqueos.

Para configurar un enrutamiento dinámico IPv4 usando RIP (Routing Information Protocol, protocolo de enrutamiento de información), haga clic en la ficha **IPv4**.

Para configurar un enrutamiento dinámico IPv6 usando RIPng (Routing Information Protocol Next Generation, protocolo de enrutamiento de información de nueva generación), haga clic en la ficha **IPv6**.

**Configuración de un enrutamiento dinámico IPv4**

**PASO 1** Elija un valor en Modo de operación:

- **Gateway**: elija este modo si este dispositivo es el que aloja la conexión de red para Internet. Este es el ajuste predeterminado.

- **Router**: elija este modo si el dispositivo está en una red con otros routers y otro dispositivo es el gateway de red para Internet o si esta red no está conectada a Internet. En el modo de router, la conectividad de Internet está disponible en los dispositivos de red solo si hay otro router que funciona como gateway. Como la protección del cortafuegos la proporciona el gateway, deshabilite el cortafuegos de este dispositivo.

**PASO 2** Habilite **RIP** para permitir que este dispositivo pueda intercambiar su información de enrutamiento automáticamente con otros routers y ajustar dinámicamente las tablas de enrutamiento a medida que se produzcan cambios en la red. El ajuste predeterminado es Deshabilitado. Si habilita esta función, configure también los siguientes ajustes:

- **Recibir versiones de RIP**: seleccione el protocolo RIP para recibir datos de red: **Ninguno**, **RIPv1**, **RIPv2** o **Tanto RIP v1 como v2**.

  **RIPv1** es una versión de enrutamiento basada en clases. No incluye información de subred y, en consecuencia, no es compatible con VLSM (Variable Length Subnet Masks, máscaras de subred de longitud variable). RIPv1 tampoco admite la autenticación de router, por lo que es vulnerable a los ataques. **RIPv2** incluye una máscara de subred y es compatible con la seguridad de autenticación mediante contraseña.

- **Transmitir versiones de RIP**: seleccione el protocolo RIP para transmitir datos de red: **Ninguno**, **RIPv1**, **RIPv2 - Broadcast** (RIPv2 - Difusión) o **RIPv2 - Multicast** (RIPv2 - Multidifusión).

  **RIPv2 - Broadcast** (RIPv2 - Difusión) (opción recomendada) permite difundir los datos por toda la subred. **RIPv2 - Multicast** (RIPv2 - Multidifusión) envía los datos a las direcciones de multidifusión. Esta opción también evita cargas innecesarias al efectuar la multidifusión de las tablas de enrutamiento a routers adyacentes en lugar de realizar la multidifusión a toda la red.

**PASO 3** Haga clic en **Guardar**.

### Configuración de un enrutamiento dinámico IPv6

La ficha IPv6 está disponible cuando la opción IP con pila dual está habilitada en la página Configuración > Red.

Para habilitar RIPng, active la casilla **RIPng**.

## Configuración de rutas estáticas

Se pueden configurar rutas estáticas para IPv4 e IPv6. Se trata de rutas que no se quedan anticuadas en la tabla de enrutamiento. Se pueden introducir hasta 30 rutas.

Para configurar una ruta estática, haga clic en **Agregar** o seleccione una entrada y haga clic en **Editar**:

- **IP de destino**: dirección de subred del segmento de LAN remota. Para un dominio IP de Clase C, la dirección de red son los tres primeros campos de la IP de LAN de destino (el último campo debe ser cero).
- **Máscara de subred (solo IPv4)**: máscara de subred que se usa en el dominio IP de la LAN de destino. Para los dominios IP de Clase C, la máscara de subred suele ser 255.255.255.0.
- **Longitud del prefijo (IPv6 solo)**: longitud del prefijo IPv6.
- **Gateway predeterminada**: dirección IP del router de último recurso.
- **Recuento de saltos**: número máximo de nodos o saltos (el valor máximo es 15 saltos) por los que pasa un paquete antes de ser descartado. Un nodo es cualquier dispositivo de la red, como los switches o los routers.
- **Interfaz**: interfaz que se debe usar para esta ruta.

Para eliminar una entrada de la lista, haga clic en la entrada que desee eliminar y elija **Eliminar**.

Para ver los datos actuales, haga clic en **View Routing Table** (Ver tabla de enrutamiento). Se abre la Routing Table Entry List (Lista de entradas de la tabla de enrutamiento). Haga clic en **Actualizar** para actualizar los datos. También puede hacer clic en **Cerrar** para cerrar la ventana emergente.

# Equilibrio de carga entrante

La función de equilibrio de la carga entrante distribuye el tráfico entrante a partes iguales entre todos los puertos WAN para hacer el mejor uso posible del ancho de banda. También evita las distribuciones irregulares del tráfico y las congestiones.

Para habilitar y configurar el equilibrio de carga entrante:

**PASO 1** Haga clic en **Habilitar Equilibrio de carga entrante**.

**PASO 2** Especifique la información sobre el **nombre de dominio**:

- **Nombre de dominio**: nombre de dominio asignado por el proveedor de servicios DNS.
- **TTL** (Time-to-Live, periodo de vida): intervalo de tiempo para las consultas DNS (segundo, 0~65535). Si se establece un intervalo grande, repercute en el tiempo de actualización. Si se establece un intervalo corto, aumenta la carga del sistema, pero se mejora la precisión del equilibrio de carga entrante. Puede ajustar este parámetro para obtener el mejor rendimiento de la red.
- **Administrador**: dirección de correo electrónico del administrador.

**PASO 3** Especifique los parámetros adecuados para el **servidor DNS**:

- **Servidor de nombres**: servidor DNS que traduce el nombre del dominio.
- **Interfaz**: interfaz WAN correspondiente al servidor de nombres. El sistema muestra las direcciones IP de WAN habilitadas y adquiridas.

**PASO 4** Especifique el nombre de host que proporciona servicios, por ejemplo, el servidor de correo o el servidor FTP en el campo **Nombre de host** (Registro) y seleccione la interfaz **IP de WAN** a la que se distribuye el tráfico entrante.

**PASO 5** Especifique un valor en los campos **Alias**, que asigna varios nombres a un equipo (un host que podría proporcionar varios servicios) y **Destino** (un nombre de dominio existente en el registro A).

**PASO 6** Haga clic en **Ajustes de SPF** para agregar texto de SPF. SPF (Sender Policy Framework, marco de directivas de remitente) es un sistema de validación de correo electrónico que evita el spam al detectar las simulaciones en el correo electrónico (una vulnerabilidad habitual) al verificar las direcciones IP de los remitentes (no es obligatorio configurar este campo. Encontrará más información en http://www.openspf.org/Tools#wizard?mydomain=&x=35&y=6).

**PASO 7** Especifique los parámetros para el **servidor de correo**:

- **Nombre del host**: nombre (sin nombre de dominio) del host de correo.
- **Peso**: orden de los hosts de correo. El número más bajo es el que tiene la mayor prioridad.
- **Servidor de correo**: nombre del servidor que está guardado en el registro A o el nombre de un servidor de correo externo.

**PASO 8** Haga clic en **Guardar**.

## Actualización de dispositivos USB

El firmware de los dispositivos USB se puede actualizar usando este dispositivo de red.

Para actualizar un dispositivo USB conectado a un puerto USB, acceda al archivo que se debe cargar en el dispositivo USB procedente de un equipo y haga clic en **Actualizar**.

5

# DHCP

DHCP (Dynamic Host Configuration Protocol, protocolo de configuración dinámica de hosts) es un protocolo de red que se usa para configurar dispositivos de red a fin de que puedan comunicarse a través de una red IP. Un cliente DHCP utiliza el protocolo DHCP para adquirir información de configuración, por ejemplo, una dirección IP, una ruta predeterminada y una o varias direcciones de servidor DNS procedentes de un servidor DHCP. El cliente DHCP utiliza esta información para configurar el host. Una vez que finaliza el proceso de configuración, el host puede comunicarse a través de Internet.

El servidor DHCP mantiene una base de datos con direcciones IP disponibles e información de configuración. Cuando se recibe una solicitud de un cliente, el servidor DHCP determina a qué red está conectado el cliente DHCP, asigna una dirección IP o un prefijo adecuado para el cliente y envía la información de configuración adecuada para este.

El servidor DHCP y el cliente DHCP deben estar conectados al mismo enlace de red. En las redes más grandes, cada enlace de red contiene uno o varios agentes de retransmisión DHCP. Dichos agentes reciben mensajes desde los clientes DHCP y los reenvían a los servidores DHCP. Estos últimos envían respuestas al agente de retransmisión, el cual las reenvía al cliente DHCP en el enlace de red local.

Los servidores DHCP normalmente conceden direcciones IP a los clientes durante un intervalo de tiempo limitado, denominado *tiempo de cesión*. Los clientes DHCP son responsables de renovar sus direcciones IP antes de que venza dicho periodo. En caso de que no hayan efectuado una renovación, deben dejar de usar las direcciones cuando el plazo haya terminado.

DHCP se usa para IPv4 e IPv6. Aunque ambas versiones atienden al mismo propósito, los detalles del protocolo para IPv4 e IPv6 son lo suficientemente diferentes como para que se consideren protocolos independientes.

# Configuración de DHCP

Configuración de DHCP se utiliza para configurar DHCP para IPv4 o IPv6. También permite que algunos dispositivos descarguen su configuración desde un servidor TFTP. Cuando se inicia un dispositivo, si este no tiene preconfiguradas la dirección IP y la dirección IP del servidor TFTP, se envía una solicitud con las opciones 66, 67 y 150 al servidor DHCP para obtener esta información.

La opción 150 de DHCP es propiedad de Cisco. El estándar IEEE similar a este requisito es la opción 66. Al igual que la opción 150, la 66 se utiliza para especificar el nombre del servidor TFTP. La opción 67 proporciona el nombre del archivo de arranque.

La opción 82 (opción de información del agente de retransmisión DHCP) permite a un agente de retransmisión DHCP incluir información sobre sí mismo al reenviar paquetes DHCP procedentes de un cliente a un servidor DHCP. El servidor DHCP puede usar esta información para implementar direccionamientos IP u otras políticas de asignación de parámetros.

Para configurar DHCP para IPv4, haga clic en la ficha **IPv4**. Para configurar DHCP para IPv6, haga clic en la ficha **IPv6**.

**Configuración de DHCP para IPv4**

Para configurar DHCP para IPv4:

**PASO 1** Elija **VLAN** o bien **Opción 82**.

**PASO 2** Si elige **Opción 82**, agregue los Id. de circuito mediante DHCP > **Opción 82**. Estos ID de circuito aparecerán en el menú desplegable **ID de circuito**.

Si elige **VLAN**, seleccione la VLAN en el menú **Id. de VLAN** y especifique estos datos:

- **Dirección IP del dispositivo**: dirección IP de administración.
- **Máscara de subred**: máscara de subred IP de administración.

**PASO 3** Seleccione un valor en **Modo DHCP**:

- **Deshabilitar**: deshabilita DHCP en este dispositivo. No hay que completar ningún parámetro más.
- **Servidor DHCP**: transmite las solicitudes DHCP del cliente al servidor DHCP del dispositivo.

- **Retransmisión DHCP**: pasa las respuestas y las solicitudes DHCP procedentes de otro servidor DHCP a través del dispositivo. Si elige la opción Retransmisión DHCP, especifique la dirección IP del **servidor DHCP remoto**.
- **Tiempo de cesión de cliente**: periodo de tiempo (en minutos) que un usuario de red puede conectarse al router con la dirección IP actual. Valores válidos: entre 5 y 43 200 minutos. Valor predeterminado: 1440 minutos (es decir, 24 horas).
- **Inicio de rango** y **Fin de rango**: direcciones IP de inicio y de finalización que crean un rango de direcciones IP que se pueden asignar dinámicamente. El rango puede incluir hasta el número máximo de direcciones IP que el servidor puede asignar sin solapar funciones como PPTP y VPN SSL. No incluya la dirección IP de la LAN del dispositivo en este rango de IP dinámica. Por ejemplo, si el router utiliza la dirección IP predeterminada de la LAN, **192.168.1.1**, el valor de inicio debe ser 192.168.1.2 o uno superior.
- **Servidor DNS**: tipo de servicio DNS donde se adquiere la dirección IP del servidor DNS.
- **DNS estático 1** y **DNS estático 2**: dirección IP estática de un servidor DNS. (Opcional) Si especifica un segundo servidor DNS, el dispositivo usa el primero que responda a una solicitud.
- **WINS**: dirección IP opcional de un servidor WINS (Windows Internet Naming Service, servicio de nombres de Internet de Windows) que convierte los nombres de NetBIOS en direcciones IP. Si no conoce la dirección IP del servidor WINS, use el valor predeterminado (0.0.0.0).

**PASO 4** Especifique los parámetros para el servidor TFTP:

- **Nombre de host de servidor TFTP**: nombre de host del servidor TFTP.
- **IP de servidor TFTP**: dirección IP del servidor TFTP.
- **Nombre de archivo de configuración**: nombre del archivo de configuración que se utiliza para actualizar un dispositivo.

### Configuración de DHCP para IPv6

Para configurar DHCP para IPv6:

**PASO 1** Especifique la **dirección IPv6**.

**PASO 2** Especifique la **longitud del prefijo**.

**PASO 3** Seleccione un valor en **Modo DHCP**:

- **Deshabilitar**: deshabilita DHCP en este dispositivo. No hay que completar ningún parámetro más.
- **Servidor DHCP**: transmite las solicitudes DHCP del cliente al servidor DHCP del dispositivo.
- **Retransmisión DHCP**: pasa las respuestas y las solicitudes DHCP procedentes de otro servidor DHCP a través del dispositivo.
- **Tiempo de cesión de cliente**: periodo de tiempo que un usuario de red puede conectarse al router con la dirección IP actual. Especifique un periodo de tiempo en minutos. Valores válidos: entre 5 y 43 200 minutos. Valor predeterminado: 1440 minutos (es decir, 24 horas).
- **Servidor DNS 1** y **Servidor DNS 2**: (opcional) dirección IP de un servidor DNS. Si especifica un segundo servidor DNS, el dispositivo usa el primero que responda. Especificar un servidor DNS puede proporcionar un acceso más rápido que si se usa un servidor DNS asignado dinámicamente. Use el ajuste predeterminado (0.0.0.0) para utilizar un servidor DNS asignado dinámicamente.

**PASO 4** Especifique el grupo de direcciones IPv6:

- **Dirección inicial**: dirección de inicio del grupo de direcciones IPv6.
- **Dirección final**: dirección de finalización del grupo de direcciones IPv6.
- **Longitud del prefijo**: longitud del prefijo de la dirección IP IPv6.

# Estado de DHCP

Estado de DHCP muestra el estado del servidor DHCP y de sus clientes.

Para ver el estado de DHCP y los clientes, haga clic en la ficha **IPv4** o **IPv6**. Para IPv4, seleccione **VLAN** o bien **Opción 82**. Para IPv6, seleccione el **Prefijo**.

Para el servidor DHCP, se muestra la siguiente información:

- **Servidor DHCP**: dirección IP del servidor DHCP.
- **IP dinámica utilizada**: número de direcciones IP dinámicas utilizadas.

- **IP estática utilizada (solo IPv4)**: número de direcciones IP estáticas utilizadas.
- **DHCP disponible**: número de direcciones IP dinámicas utilizadas.
- **Total**: número total de direcciones IP dinámicas administradas por el servidor DHCP.

La tabla de clientes muestra información sobre los clientes DHCP:

- **Nombre de host de cliente**: nombre asignado a un host de cliente.
- **Dirección IP**: dirección IP dinámica asignada a un cliente.
- **Dirección MAC (solo IPv4)**: dirección MAC de un cliente.
- **Tiempo de cesión de cliente**: periodo de tiempo que un usuario de red puede permanecer conectado al router con una dirección IP dinámica.

En el caso de IPv4, para liberar la dirección IP de un cliente, seleccione **Nombre de host de cliente** y haga clic en **Eliminar**.

Haga clic en **Actualizar** para renovar los datos.

# Opción 82

La opción 82 (opción de información del agente de retransmisión DHCP) permite a un agente de retransmisión DHCP incluir información sobre sí mismo al reenviar paquetes DHCP procedentes de un cliente a un servidor DHCP. El servidor DHCP puede usar esta información para implementar direccionamientos IP u otras políticas de asignación de parámetros.

El ID de circuito configurable de la opción 82 de DHCP mejora la seguridad de la validación, ya que le permite determinar qué información se proporciona en la descripción del Id. de circuito de la opción 82.

Para agregar un **ID de circuito**, haga clic en **Agregar**. Se agrega una nueva fila a la tabla y los ID de circuito aparecen en el menú desplegable ID de circuito, en la ventana **Configuración de DHCP**.

Para editar un **ID de circuito**, seleccione la fila y haga clic en **Editar**. La fila se abre para que se pueda modificar.

# Vinculación IP y MAC

Cuando el dispositivo se configura como servidor DHCP o para la retransmisión de DHCP, se pueden vincular direcciones IP estáticas con un máximo de 80 dispositivos de red; por ejemplo, un servidor web o uno FTP.

En general, la dirección MAC de un dispositivo aparece físicamente en una etiqueta en el panel inferior o posterior del dispositivo en cuestión.

**Vinculación de direcciones IP por detección**

Para vincular direcciones IP conocidas con direcciones MAC y asignar un nombre a la vinculación:

**PASO 1** Haga clic en **Mostrar direcciones MAC desconocidas**. Se muestra la tabla de vinculación IP y MAC. Si el navegador web muestra un mensaje sobre la ventana emergente, permita el contenido bloqueado.

Los dispositivos aparecen en la lista según las direcciones IP y MAC. Si es necesario, haga clic en **Actualizar** para actualizar los datos.

**PASO 2** Ingrese un **Nombre** descriptivo.

**PASO 3** Marque la casilla **Habilitar**. Si lo desea, también puede seleccionar todos los dispositivos de la lista haciendo clic en la casilla de verificación situada en la parte superior de la columna Habilitar.

**PASO 4** Haga clic en **Guardar** para agregar los dispositivos a la lista IP estática o en **Cerrar** para cerrar la ventana emergente sin agregar los dispositivos seleccionados.

**Vinculación manual de direcciones IP**

Para agregar una nueva vinculación a la lista, haga clic en **Agregar** y especifique la siguiente información:

- **Dirección IPv4 estática:** especifique la dirección IP que se debe asignar al dispositivo.
- **Dirección MAC:** la dirección MAC del dispositivo.
- **Nombre:** nombre descriptivo del dispositivo.

**Habilitar:** marque esta casilla para vincular la dirección IP estática a este dispositivo.

**Edición o eliminación de entradas vinculadas**

Para **Editar** los ajustes, seleccione una entrada de la lista y haga clic en **Editar**. La información aparece en los campos de texto. Realice los cambios y haga clic en **Guardar**.

Para **Eliminar** una entrada de la lista, selecciónela y haga clic en **Eliminar**. Para seleccionar un grupo de entradas, haga clic en la primera entrada, mantenga presionada la tecla **Mayús** y, a continuación, haga clic en la entrada final del grupo. Para seleccionar entradas individuales, presione la tecla **Ctrl** mientras hace clic en cada entrada. Para anular la selección de una entrada, presione la tecla **Ctrl** mientras hace clic en la entrada.

**Uso de la lista IP estática para bloquear dispositivos**

La lista IP estática se puede utilizar para controlar el acceso a la red.

Para bloquear el acceso de los dispositivos que no figuran en la lista o no tienen la dirección IP correcta:

- **Bloquear direcciones MAC de la lista con direcciones IP correctas**: marque esta casilla para impedir que un dispositivo acceda a la red si su dirección IP cambió. Por ejemplo, si asignó una dirección IP estática 192.168.1.100 y alguien configura el dispositivo para que use 192.168.149, este no podrá conectarse a la red Esto evita que los usuarios cambien las direcciones IP de los dispositivos sin permiso. Desmarque la casilla para permitir el acceso independientemente de la asignación de dirección IP actual.
- **Bloquear direcciones MAC no incluidas en la lista**: marque esta casilla para bloquear el acceso de los dispositivos que no están incluidos en la lista IP estática. Esto impide que los dispositivos desconocidos accedan a la red. Desmarque la casilla para permitir el acceso de cualquier dispositivo que está configurado con una dirección IP incluida en el rango correcto.

# Base de datos local de DNS

El DNS (Domain Name Service, servicio de nombres de dominio) relaciona un nombre de dominio con su dirección IP enrutable. Se puede configurar una base de datos local de DNS que permita al dispositivo actuar como servidor DNS local para los nombres de dominio de uso frecuente. Usar una base de datos local puede ser más rápido que usar un servidor DNS externo. Si un nombre de dominio solicitado no se encuentra en la base de datos local, la solicitud se reenvía al servidor DNS especificado en la página **Configuración de red** > Ajuste de WAN.

Si habilita esta función, también debe configurar los dispositivos cliente para que usen el dispositivo como servidor DNS. De forma predeterminada, los equipos Windows están configurados para obtener automáticamente la dirección del servidor DNS a partir de la gateway predeterminada.

Para cambiar los ajustes de la conexión TCP/IP, por ejemplo, en un equipo Windows, acceda a la ventana *Propiedades de conexión de área local > Protocolo de Internet > Propiedades de TCP/IP*. Elija **Utilizar la siguiente dirección del servidor DNS** y especifique la dirección IP de la LAN del router como el servidor DNS preferido. Para obtener más información, consulte la documentación del cliente que está configurando.

**Adición, edición o eliminación de entradas DNS locales**

Para agregar una nueva entrada, haga clic en **Agregar** y especifique la siguiente información:

- **Nombre del host**: escriba el nombre de dominio, como *ejemplo.com* o *ejemplo.org*. Si no incluye el nivel final del nombre de dominio, Microsoft Windows® agregará automáticamente *.com* a la entrada.
- **Dirección IP:** especifique la dirección IP del recurso.

Para **editar** los ajustes, seleccione una entrada de la lista. La información aparece en los campos de texto. Realice los cambios oportunos y haga clic en **Guardar**.

Para **eliminar** una entrada de la lista, seleccione la entrada que desee y haga clic en **Eliminar**. Para seleccionar un grupo de entradas consecutivas, haga clic en la primera entrada, mantenga presionada la tecla **Mayús** y, a continuación, haga clic en la entrada final del grupo. Para seleccionar entradas individuales, presione la tecla **Ctrl** mientras hace clic en cada entrada. Para deseleccionar una entrada, presione la tecla **Ctrl** mientras hace clic en la entrada.

# Anuncio de router (IPv6)

RADVD (Router Advertisement Daemon, daemon de anuncio de router) se utiliza para el enrutamiento y la configuración automática de IPv6. Si se habilita, el router enviará los mensajes periódicamente y a modo de respuesta a las solicitudes. Un host usa la información para conocer los prefijos y parámetros de la red local. Si deshabilita esta función, se deshabilitará de forma eficaz la configuración automática, lo que requerirá la configuración manual de la dirección IPv6, el prefijo de subred y la gateway predeterminada en cada dispositivo.

Esta página está disponible si se habilitó la opción IP con pila dual en la página **Configuración de red**. Si no se ha habilitado, se muestra un mensaje cuando se intenta abrir esta página.

Para activar la opción **Habilitar anuncio de router**, seleccione la casilla y cumplimente el resto de los campos:

- **Modo de anuncio:** seleccione una de las siguientes opciones:
  - **Multidifusión no solicitada**: envía mensajes de anuncios de router a todas las interfaces que pertenezcan al grupo de multidifusión. Esta opción es el ajuste predeterminado. Especifique también un valor en **Intervalo de anuncio** para indicar el intervalo con el que se deben enviar los mensajes de anuncio de router. Especifique un valor entre 10 y 1800 segundos. El valor predeterminado es 30 segundos.
  - **Solo unidifusión**: envía mensajes de anuncio de router solo a las direcciones IPv6 conocidas.
- **Marcas de anuncio de router**: determina si los hosts pueden usar o no usar DHCPv6 para obtener las direcciones IP y la información relacionada. Las opciones son:
  - **Administradas**: los hosts utilizan un protocolo de configuración administrado con estado (DHCPv6) para obtener direcciones con estado y otras informaciones a través de DHCPv6.
  - **Otros**: utiliza un protocolo de configuración administrado con estado (DHCPv6) para obtener otra información sin dirección, como las direcciones del servidor DNS.
- **Preferencia de router (Alta, Media** o **Baja)**: la métrica de preferencia se utiliza en una topología de red en la que los hosts con más de una conexión tienen acceso a varios routers. Esta métrica ayuda a un host a elegir el

router adecuado. Si se puede acceder a los dos routers, se elige el que tenga la preferencia más alta. Los hosts que no implementan las preferencias del router hacen caso omiso de estos valores. El valor predeterminado es Alta.

- **MTU**: tamaño máximo de paquete que puede enviarse a través de la red. MTU (Maximum Transmission Unit, unidad máxima de transmisión) se usa en los mensajes de anuncio de router para garantizar que todos los nodos de la red usan el mismo valor de MTU cuando no se conoce la MTU de LAN. El ajuste predeterminado es 1500 bytes, que es el valor estándar para las redes Ethernet. En el caso de las conexiones PPPoE, el valor estándar es 1492 bytes. Esta configuración no debe cambiarse, a no ser que el ISP así lo requiera.
- **Vigencia de router**: duración de los mensajes de anuncio de router en la ruta, en segundos. El valor predeterminado es 3600 segundos.

Para agregar una nueva subred, haga clic en **Agregar** y especifique valores en los campos **Dirección IPv6**, **Longitud del prefijo** y **Vigencia**.

# 6

# Administración del sistema

La función Administración del sistema incluye ajustes avanzados (por ejemplo, herramientas de diagnóstico) y permite realizar actualizaciones de firmware, copias de seguridad y reinicios del dispositivo, entre otras tareas.

## Conexiones WAN duales

Si utiliza más de una interfaz WAN, use esta función para configurar los ajustes de las conexiones a Internet.

Para configurar el equilibrio de carga, elija uno de los siguientes modos con el fin de administrar las conexiones WAN:

- **Smart Link de respaldo**: garantiza una conectividad continua. Si la conexión WAN principal no está disponible, se utilizará la conexión WAN de seguridad. Elija la interfaz WAN principal en el menú desplegable.
- **Equilibrio de carga**: use las dos conexiones WAN simultáneamente para aumentar el ancho de banda disponible. El router equilibra el tráfico entre las dos interfaces utilizando el método Weighted Round-Robin.

**NOTA** Las consultas DNS no están sujetas al equilibrio de carga.

Para configurar los ajustes de la interfaz, seleccione **WAN Interface** (Interfaz WAN) y haga clic en **Editar**. Se abre la ventana de ajustes de la interfaz. Especifique los siguientes parámetros:

**Máximo ancho de banda proporcionado por el ISP**

Especifique el ajuste de ancho de banda máximo, tal y como se lo haya especificado el ISP. Si el ancho de banda excede el número especificado, el router utiliza otra interfaz WAN para la próxima conexión.

- **Ascendente**: ancho de banda ascendente máximo proporcionado por el ISP. El valor predeterminado es 10 000 kbit/s. El valor máximo es 1 000 000 kbit/s.

- **Descendente**: ancho de banda descendente máximo proporcionado por el ISP. El valor predeterminado es 10 000 kbit/s.

**Detección de servicio de red**

Si lo desea, active la casilla para que el dispositivo pueda detectar la conectividad de red haciendo ping a los dispositivos especificados y especifique los ajustes que se describen a continuación:

- **Recuento de reintentos**: número de veces que se puede hacer ping a un dispositivo. El rango es de 1 a 99 999. El valor predeterminado es 3.
- **Tiempo de espera de reintento**: número de segundos que se debe esperar entre un ping y el siguiente. El rango es de 1 a 99 999. El valor predeterminado es 10 segundos.
- **En caso de fallo**: acción que se debe realizar si se produce un fallo con la prueba Ping:
  - **Generate the Error Condition in the System Log** (Generar condición de error en el registro del sistema): recoge el fallo en el registro del sistema. No se realiza conmutación por error a la otra interfaz.
  - **Keep System Log and Remove the Connection** (Mantener registro de sistema y eliminar la conexión): se realiza la conmutación por error y se utiliza la interfaz de copia de seguridad. Cuando se restaura la conectividad del puerto WAN, se restablece el tráfico.
- **Gateway predeterminada, Host de ISP, Host remoto** y **Host de búsqueda DNS**: seleccione el dispositivo al que desea hacer ping para determinar la conectividad de red. En el caso de un host de ISP o un host remoto, escriba la dirección IP. Si se trata de un host de búsqueda DNS, escriba un nombre de host o un nombre de dominio. Desactive la casilla si no desea hacer ping a este dispositivo para detectar el servicio de red.

### Enlace de protocolo

Enlace de protocolo requiere que se use esta interfaz para los protocolos, el origen y las direcciones de destino especificados. Permite a un administrador vincular tráfico saliente específico con una interfaz WAN. Se usa normalmente cuando las dos interfaces WAN tienen diferentes características o cuando determinado tráfico de la LAN o la WAN debe pasar por la misma interfaz WAN.

Para agregar o editar entradas de la tabla, haga clic en **Agregar** o **Editar** y especifique la siguiente información:

- **Servicio**: servicio (o Todo el tráfico) que se debe vincular a esta interfaz WAN. Si un servicio no aparece en la lista, puede hacer clic en **Administración de servicios** para agregarlo. Para obtener más información, consulte **Creación o edición de un servicio**.
- **IP de origen** e **IP de destino**: origen interno y destino externo del tráfico que pasa por este puerto WAN. Para especificar un rango de direcciones IP, escriba la primera dirección en el primer campo y escriba la dirección final en el campo *Hasta*. Para especificar una única dirección IP, escriba la misma dirección en los dos campos.

Si desea habilitar el enlace de protocolo, active la casilla para habilitar esta regla o desactívela para deshabilitarla.

Para **editar** los ajustes, seleccione una entrada de la lista. La información aparece en los campos de texto. Realice los cambios oportunos y haga clic en **Guardar**.

Para **eliminar** una entrada de la lista, seleccione la entrada que desee y haga clic en **Eliminar**. Para seleccionar un grupo de entradas consecutivas, haga clic en la primera entrada, mantenga presionada la tecla **Mayús** y, a continuación, haga clic en la entrada final del grupo. Para seleccionar entradas individuales, presione la tecla **Ctrl** mientras hace clic en cada entrada. Para deseleccionar una entrada, presione la tecla **Ctrl** mientras hace clic en la entrada.

### Creación o edición de un servicio

Para agregar una entrada nueva a la lista Servicio o para cambiar una entrada, haga clic en **Administración de servicios**. Puede haber 30 servicios en la lista como máximo. Si el navegador web muestra una advertencia sobre la ventana emergente, indique que se permita el contenido bloqueado.

Para agregar un servicio a la lista, haga clic en **Agregar** y especifique la siguiente información:

- **Nombre del servicio**: descripción breve.

- **Protocolo**: protocolo obligatorio. Consulte la documentación del servicio que desee alojar.
- **Rango de puertos**: rango de puertos obligatorio.

Para **editar** los ajustes, seleccione una entrada de la lista y haga clic en **Editar**. La información aparece en los campos de texto. Realice los cambios oportunos y haga clic en **Guardar**.

Para **eliminar** una entrada de la lista, seleccione la entrada que desee y haga clic en **Eliminar**. Para seleccionar un grupo de entradas consecutivas, haga clic en la primera entrada, mantenga presionada la tecla **Mayús** y, a continuación, haga clic en la entrada final del grupo. Para seleccionar entradas individuales, presione la tecla **Ctrl** mientras hace clic en cada entrada. Para deseleccionar una entrada, presione la tecla **Ctrl** mientras hace clic en la entrada.

# Administración del ancho de banda

La función Administración del ancho de banda permite definir los ajustes del ancho de banda para el tráfico ascendente y descendente, así como configurar los ajustes de QoS (Quality of Service, calidad del servicio) para los distintos tipos de tráfico, como los servicios de voz.

**Máximo ancho de banda proporcionado por el ISP**

Especifique el ajuste de ancho de banda máximo, tal y como se lo haya especificado el ISP:

- **Ascendente**: ancho de banda ascendente máximo proporcionado por el ISP.
- **Descendente**: ancho de banda descendente máximo proporcionado por el ISP.

**Tipo de administración del ancho de banda**

Seleccione una de las siguientes opciones de administración:

- **Control de velocidad**: ancho de banda mínimo (garantizado) y ancho de banda máximo (limitado) para cada servicio o dirección IP. Puede agregar 100 servicios como máximo.
- **Prioridad**: administre el ancho de banda identificando cuáles son los servicios de alta y baja prioridad.

### Control de velocidad

Para agregar una interfaz que esté sujeta a la administración del ancho de banda, haga clic en **Agregar** y especifique los siguientes ajustes:

- **Interfaz**: interfaz compatible con el servicio.
- **Servicio**: servicio que se debe administrar. Si un servicio no aparece en la lista, haga clic en **Administración de servicios** para agregarlo.
- **IP**: dirección IP o rango que se debe controlar.
- **Dirección**: seleccione **Ascendente** para el tráfico saliente. Seleccione **Descendente** para el tráfico entrante.
- **Velocidad mín.**: velocidad mínima en kbit/s para el ancho de banda garantizado.
- **Velocidad máxima**: velocidad máxima en kbit/s para el ancho de banda garantizado.

Seleccione la casilla para habilitar el servicio.

### Configuración de la prioridad

Para agregar una interfaz que esté sujeta a la administración del ancho de banda, haga clic en **Agregar** y especifique los siguientes ajustes:

- **Interfaz**: interfaz compatible con el servicio.
- **Servicio**: servicio que se debe administrar. Si un servicio no aparece en la lista, haga clic en **Administración de servicios** para agregarlo.
- **Dirección**: seleccione **Ascendente** para el tráfico saliente. Seleccione **Descendente** para el tráfico entrante.
- **Prioridad:** seleccione la prioridad para este servicio. **Alta** o **Baja**. El nivel de prioridad predeterminado es Media, que se considera de forma implícita y no se muestra en la interfaz web.

Seleccione la casilla para habilitar este servicio.

Para **editar** los ajustes, seleccione una entrada de la lista y haga clic en **Editar**. La información aparece en los campos de texto. Realice los cambios oportunos y haga clic en **Guardar**.

Para **eliminar** una entrada de la lista, seleccione la entrada que desee y haga clic en **Eliminar**. Para seleccionar un grupo de entradas consecutivas, haga clic en la primera entrada, mantenga presionada la tecla **Mayús** y, a continuación, haga clic en la entrada final del grupo. Para seleccionar entradas individuales, presione la tecla **Ctrl** mientras hace clic en cada entrada. Para deseleccionar una entrada, presione la tecla **Ctrl** mientras hace clic en la entrada.

# SNMP

SNMP (Simple Network Management Protocol, protocolo simple de administración de red) permite a los administradores de red administrar y supervisar la red, además de recibir notificaciones de los eventos críticos a medida que se producen en la red. El dispositivo es compatible con SNMP v1/v2c y SNMP v3. El dispositivo es compatible con MIB (Management Information Bases, bases de información de gestión) estándar como MIBII y con las MIB privadas.

El dispositivo actúa como un agente SNMP que responde a los comandos SNMP desde los sistemas de administración de redes SNMP. Los comandos que se pueden usar son los comandos SNMP estándares get, next y set. También genera mensajes trap para informar al administrador de SNMP en el momento en que se produce una condición de alarma, por ejemplo, reinicios, ciclos de apagado y encendido o eventos relacionados con los enlaces WAN.

## Configuración de SNMP

- **Nombre del sistema**: nombre de host del dispositivo.
- **Contacto del sistema**: nombre del administrador de red al que se le deben notificar las novedades sobre el dispositivo.
- **Ubicación del sistema**: información de contacto sobre el administrador de red. Puede tratarse de una dirección de correo electrónico, un número de teléfono o un número de radiolocalizador.
- **Nombre de la comunidad de trap**: contraseña que se envía con cada trap al administrador de SNMP. La cadena puede tener hasta 64 caracteres alfanuméricos. El valor predeterminado es **public**.

- **Habilitar SNMPv1/v2c**: habilita SNMP v1/v2c.
  - **Obtener nombre de la comunidad**: cadena de comunidad para la autenticación de los comandos SNMP GET. Puede escribir un número que tenga 64 caracteres alfanuméricos como máximo. El valor predeterminado es *public*.
  - **Establecer nombre de la comunidad**: cadena de comunidad para la autenticación de los comandos SNMP SET. Puede escribir un número que tenga 64 caracteres alfanuméricos como máximo. El valor predeterminado es *private*.
  - **Dirección IP de receptor del trap SNMPv1/v2c**: dirección IP o nombre de dominio para el servidor en el que está ejecutando el software de administración de SNMP.
- **Habilitar SNMPv3**: habilita SNMPv3 (marque la casilla y haga clic en **Guardar** antes de crear usuarios y grupos de SNMP). Siga las instrucciones que aparecen en **Configuración de SNMPv3**.
  - **Dirección IP de receptor del trap SNMPv3**: dirección IP o nombre de dominio para el servidor en el que está ejecutando el software de administración de SNMP.
  - **Usuario receptor del trap SNMPv3**: nombre de usuario para el servidor en el que se está ejecutando el software de administración de SNMP.

**Configuración de SNMPv3**

Puede crear grupos de SNMPv3 para administrar el acceso SNMP MIB e identificar los usuarios que tienen acceso a cada grupo.

Para agregar o editar un grupo:

**PASO 1** Haga clic en **Agregar** o seleccione un grupo y haga clic en **Editar** en la Tabla de grupo.

**PASO 2** Especifique el **nombre de grupo**.

**PASO 3** En el menú desplegable, seleccione un **nivel de seguridad**. Al seleccionar **Autenticación** o **Privacidad**, los usuarios se ven obligados a autenticarse usando contraseñas. Cuando se selecciona **Sin autenticación** o **Sin privacidad**, los usuarios de este grupo no necesitan definir una contraseña de autenticación ni de privacidad. El valor predeterminado es **Sin autenticación, Sin privacidad**. Las contraseñas de autenticación y privacidad deben tener 8 caracteres como mínimo.

**PASO 4** Seleccione las **MIB** a las que pueden acceder los miembros del grupo.

**PASO 5** Haga clic en **Guardar**.

Para agregar o editar un usuario:

**PASO 1** Haga clic en **Agregar** o seleccione un usuario y haga clic en **Editar** en la Tabla de usuario.

**PASO 2** Especifique el **nombre de usuario**.

**PASO 3** En el menú desplegable, seleccione el **grupo**.

**PASO 4** Seleccione el **método de autenticación** y escriba la **contraseña de autenticación**.

**PASO 5** Seleccione el **método de privacidad** y escriba la **contraseña de privacidad**.

**PASO 6** Haga clic en **Guardar**.

# SMTP

El protocolo simple de transferencia de correo (SMTP) es un estándar de Internet para la transmisión de correo electrónico. Para configurar el SMTP, proporcione los ajustes del SMTP que se usarán para enviar el archivo de configuración Log u OpenVPN.

Para configurar el SMTP, seleccione **Administración de sistemas > SMTP,** escriba los siguientes ajustes y haga clic en **Guardar**.

- **Remitente**: dirección de correo electrónico del remitente.
- **Servidor de correo**: nombre o dirección IP del servidor de correo.
- **Autenticación**: tipo de autenticación del inicio de sesión del servidor de correo.
  - **Ninguna**: sin autenticación.
  - **Inicio de sesión sin formato**: autenticación con texto sin formato.

  - **TLS (Transport Layer Security, seguridad de capa de transporte)**: protocolo de autenticación de la conexión segura (por ejemplo, Gmail usa la opción de autenticación de TLS en el puerto 587).
  - **SSL (Secure Socket Layer, capa de conexión segura)**: protocolo de autenticación de la conexión segura (por ejemplo, Gmail usa la opción de autenticación de SSL en el puerto 465).

- **Puerto del SMTP**: número de puerto del protocolo simple de transferencia de correo.
- **Nombre de usuario**: nombre del usuario de correo electrónico. Por ejemplo:
  Servidor de correo: smtp.gmail.com
  Autenticación: SSL
  PUERTO DEL SMTP: 465
  Nombre de usuario: xxxxx@gmail.com
  Contraseña: yyyyyy

**Contraseña**: contraseña del correo electrónico.

# Discovery: Bonjour

Bonjour es un protocolo de detección de servicios que permite localizar dispositivos de red (por ejemplo, equipos y servidores) en una LAN. Cuando esta función está habilitada, el dispositivo realiza periódicamente una multidifusión de registros de servicio Bonjour a la LAN para anunciar su existencia.

**NOTA** Para detectar productos de Cisco, Cisco proporciona una utilidad denominada FindIt que funciona mediante una sencilla barra de herramientas que se instala en el navegador web. Esta utilidad detecta los dispositivos de Cisco que haya en la red y muestra información básica, como números de serie y direcciones IP. Para obtener más información y descargar la utilidad, visite www.cisco.com/go/findit.

Para habilitar Bonjour de forma global, active la casilla **Discovery Enable** (Habilitar Discovery). Esta opción está habilitada de forma predeterminada.

Para habilitar Bonjour para una VLAN, active la casilla de la columna **Habilitar Bonjour**. Esta opción está habilitada de forma predeterminada.

# Propiedades de LLDP

LLDP (Link Layer Discovery Protocol, protocolo de detección de capa de enlace) es un protocolo independiente de los proveedores incluido en el conjunto de protocolos de Internet. Los dispositivos de red lo utilizan para anunciar su identidad, sus funciones y dispositivos vecinos en una red de área local de IEEE 802, principalmente Ethernet con cable. Los dispositivos envían la información LLDP desde cada una de sus interfaces a intervalos fijos, en formato de tramas de Ethernet. Cada trama contiene una unidad de datos LLDP (LLDPDU). Cada LLDPDU es una secuencia de estructuras TLV (Type-Length-Value, tipo, longitud, valor).

Para habilitar las propiedades de LLDP, active la casilla **Habilitar**. (esta opción está habilitada de forma predeterminada).

Para habilitar las propiedades de LLDP en una interfaz, active las casillas **Habilitar**, **WAN1** o **WAN2** (estas opciones están habilitadas de forma predeterminada).

La Tabla de vecinos de LLDP muestra la siguiente información:

- **Puerto local**: identificador del puerto.
- **Subtipo de Id. de chasis**: tipo de Id. de chasis (por ejemplo, la dirección MAC).
- **Id. de chasis**: identificador del chasis. En los casos en los que el subtipo de Id. de chasis es una dirección MAC, se muestra la dirección MAC del dispositivo.
- **Subtipo de Id. de puerto**: tipo de identificador de puerto.
- **Id. de puerto**: identificador del puerto.
- **Nombre del sistema**: nombre del dispositivo.
- **Periodo de vida**: velocidad en segundos a la que se envían las actualizaciones de los anuncios LLDP.

# Uso de Diagnósticos

La página Diagnóstico permite acceder a dos herramientas integradas, Búsqueda de nombre DNS y Ping. Si sospecha que hay un problema con la conectividad, puede usar estas herramientas para investigar la causa.

Si desea usar DNS para conocer una dirección IP, elija **Búsqueda DNS**, especifique un valor en **Buscar nombre de dominio** (por ejemplo, www.cisco.com) y haga clic en **Ir**. Se mostrará la dirección IP.

Para probar la conectividad con un host concreto, elija **Ping**, especifique una dirección IP o un nombre de host y haga clic en **Ir**. Si no conoce la dirección IP, use la herramienta Búsqueda DNS para averiguarla. La herramienta Ping muestra si el dispositivo puede enviar un paquete a un host remoto y recibir una respuesta.

Si la prueba es satisfactoria, se muestra la siguiente información:

- **Estado**: estado de la prueba, que puede ser Prueba, Prueba realizada correctamente o Prueba fallida
- **Paquetes**: número de paquetes transmitidos, número de paquetes recibidos y porcentaje de paquetes perdidos en la prueba Ping.
- **Recorrido de ida y vuelta**: valores mínimo, máximo y medio del recorrido de ida y vuelta de la prueba Ping.

# Ajustes predeterminados

Para reiniciar el dispositivo y restablecer todos los parámetros a los valores predeterminados, haga clic en **Ajustes predeterminados**.

Para restaurar el dispositivo a los valores predeterminados, incluidos los certificados predeterminados, haga clic en **Ajustes predeterminados, incluidos certificados**.

# Actualización de firmware

Esta función permite descargar el firmware para el dispositivo desde un equipo o una unidad flash USB e instalarlo. La ventana muestra la **versión de firmware** que está instalada actualmente en el dispositivo.

**NOTA** Si elige una versión anterior del firmware, el dispositivo podría restablecerse a los ajustes predeterminados. Se recomienda hacer una copia de seguridad de la configuración usando el procedimiento descrito en **Copia de seguridad y restauración** antes de actualizar el firmware.

La actualización del firmware puede tardar varios minutos.

No desconecte la alimentación, no presione el botón de reinicio, no cierre el navegador ni desconecte el enlace durante este proceso.

Para cargar firmware desde un equipo, seleccione **Actualización de firmware desde PC** y busque el archivo.

Para cargar firmware desde una unidad flash USB, seleccione **Actualización de firmware desde USB** y seleccione el archivo.

# Selección de idioma o Configuración de idioma

Use las páginas Selección de idioma o Configuración de idioma para cambiar el idioma asociado a la interfaz del usuario y a la ayuda del dispositivo.

Para las versiones de firmware posteriores a la 1.0.2.03, use la página Selección de idioma para elegir un idioma.

**PASO 1** Acceda a **Administración del sistema** > **Selección de idioma**.

**PASO 2** En la lista desplegable **Seleccionar idioma**, seleccione un idioma.

**PASO 3** Haga clic en **Guardar**.

Si lo desea, también puede elegir un idioma de la siguiente manera:

- En la página Inicio de sesión, elija un idioma en la lista desplegable **Idioma**.
- En cada página de configuración, elija un idioma en la lista desplegable de la esquina superior derecha.

Para las versiones del firmware 1.0.2.03 o anteriores, use la página Configuración de idioma para elegir un idioma nuevo cargando un paquete de idiomas en el dispositivo.

Para agregar un paquete de idiomas y elegir un idioma:

**PASO 1** Acceda a **Administración del sistema** > **Configuración de idioma**.

**PASO 2** En la lista desplegable **Modo**, seleccione **Agregar**.

**PASO 3** Especifique el **nombre de nuevo idioma**.

**PASO 4** Busque el **nombre de archivo de idioma** para cargar el nuevo archivo de idioma.

**PASO 5** Haga clic en **Guardar**.

**PASO 6** Una vez que haya cargado el paquete de idiomas, elija un idioma en la lista desplegable de la esquina superior derecha de la página Configuración de idioma o de otras páginas de configuración.

# Reiniciar

Al reiniciar desde la página Reiniciar, el router envía el archivo de registro (si la función de registro está habilitada) antes de restablecer el dispositivo. Los parámetros del dispositivo se conservan.

Para reiniciar el dispositivo, haga clic en **Reiniciar router**.

# Copia de seguridad y restauración

Los archivos de configuración se pueden importar, exportar y copiar. El router tiene dos archivos de configuración administrados: el de inicio y el de réplica. El dispositivo carga el archivo de inicio desde la memoria al arrancar en la configuración que se está ejecutando y copia dicho archivo de inicio en el archivo de réplica. De esta manera, el archivo de réplica contiene la última configuración conocida válida.

Si el archivo de configuración de inicio está dañado o falla por cualquier razón, se utilizará el archivo de configuración de réplica. El router copia automáticamente la configuración de inicio en la configuración de réplica cuando hayan transcurrido 24 horas de ejecución estable (24 horas en las que no se produzcan reinicios ni cambios de configuración).

**Restauración de los ajustes desde un archivo de configuración**

Para restaurar la configuración de inicio desde un archivo previamente guardado en un equipo o una unidad flash USB:

**PASO 1** En la sección Restaurar configuración de inicio, seleccione **Restaurar configuración de inicio desde PC** y haga clic en **Explorar**. También puede seleccionar **Restaurar configuración de inicio desde USB** y hacer clic en **Actualizar**.

**PASO 2** Seleccione un archivo de configuración (.config).

**PASO 3** Haga clic en **Restaurar**. Este proceso puede tardar hasta un minuto. Si el archivo de configuración contiene una contraseña diferente de la contraseña de administración actual del dispositivo, deberá introducir esta contraseña para que el archivo de configuración se pueda restaurar.

**PASO 4** Haga clic en **Administración del sistema > Reiniciar** en el árbol de navegación.

Los ajustes importados no se aplican hasta que se reinicie el dispositivo mediante **Administración del sistema > Reiniciar**.

Si lo desea, presione el botón **Reiniciar** del dispositivo durante un segundo y, a continuación, suéltelo para reiniciar el router.

### Copia de seguridad de los archivos de configuración y de réplica

Para guardar los archivos de configuración de inicio y de réplica en un equipo o en una unidad flash USB:

**PASO 1** Seleccione **Realizar copia de seguridad de archivo de configuración en PC** o **Realizar copia de seguridad de archivo de configuración en USB**.

**PASO 2** Haga clic en **Configuración de inicio de copia de seguridad** o en **Configuración de réplica de copia de seguridad**. Aparece la ventana Descarga de archivo.

**PASO 3** Haga clic en **Guardar** y elija la ubicación del archivo. Si lo desea, puede especificar un nombre de archivo y hacer clic en **Guardar**.

**TIP** Los nombres de archivo predeterminados son *Startup.config* y *Mirror.config*. La extensión *.config* es obligatoria. Para facilitar la identificación, puede resultar útil especificar un nombre de archivo que incluya la fecha y la hora actuales.

### Copia del archivo de réplica en el archivo de inicio

Puede copiar manualmente el archivo de configuración de inicio del dispositivo en el archivo de configuración de réplica.

Puede usar este proceso para realizar una copia de seguridad de una configuración buena conocida antes de realizar cambios en la configuración de inicio:

- El archivo de configuración de inicio se copia automáticamente en el archivo de configuración de réplica cada 24 horas.

- Si se realiza algún cambio en los parámetros del dispositivo, el contador de tiempo se restablece y la próxima copia automática se realiza 24 horas más tarde, a menos que el archivo de inicio se guarde manualmente como el archivo de réplica.

Para copiar el archivo de inicio en el archivo de réplica, haga clic en **Copiar réplica en inicio**. La operación de copia se realiza inmediatamente, sin que haya opción de cancelarla. Cuando finaliza la operación, la página se actualiza.

**Limpieza de la configuración**

Al limpiar la configuración, se elimina el archivo de réplica y el archivo de configuración de inicio.

Para eliminar el archivo de réplica y el de configuración de inicio, haga clic en **Limpiar configuración**.

**PRECAUCIÓN** La configuración de réplica se elimina inmediatamente, sin que haya opción a cancelar la operación. El dispositivo se restablece de modo que utilice la configuración predeterminada y se reinicia.

**Copia de seguridad del firmware en una unidad flash USB**

Para realizar una copia de seguridad del firmware en una unidad flash ubicada en el puerto USB, seleccione el puerto en el menú desplegable y haga clic en **Copia de seguridad**. El dispositivo guarda la imagen del firmware con el nombre **`image.bin`**.

7

# Administración de puertos

Use la Administración de puertos para habilitar la duplicación de puertos, configurar los ajustes de los puertos, y ver el estado y las estadísticas de tráfico del puerto. Además, puede configurar VLAN, 802.1x, asociar el DSCP a una fila y la CoS a DSCP.

## Configuración de puertos

Puede habilitar o deshabilitar la duplicación de puertos, administrar la configuración de puertos LAN/WAN, incluido el cierre de forma administrativa del puerto, y habilitar o deshabilitar EEE, la prioridad del puerto y el modo de negociación del puerto.

La duplicación de puertos es un método de supervisión del tráfico de red. Cuando la duplicación de puertos está habilitada, el enrutador envía una copia de todos los paquetes de red, que están visibles en uno o más puertos, a otro puerto dedicado, donde se pueden analizar los paquetes.

Para habilitar la duplicación de puertos, seleccione **Administración de puertos > Configuración de puertos** y marque **Duplicar todo el tráfico de WAN y LAN en el puerto 1**. Todos los paquetes entrantes y salientes de los puertos WAN y LAN se copian en LAN1.

**NOTA** Cuando la clonación de direcciones MAC está habilitada, la duplicación de puertos no captura el tráfico WAN.

Para habilitar la réplica de puertos para RV320, seleccione la opción **Habilitar puerto de réplica**. Los paquetes entrantes y salientes de los puertos WAN y LAN se copian en la LAN1.

Para habilitar la réplica de puertos para RV325, seleccione la opción **Habilitar puerto de réplica**. Los paquetes entrantes y salientes de los puertos LAN se copian en la LAN1.

Se muestra la siguiente información de solo lectura sobre cada puerto:

- **Id. de puerto**: nombre o número del puerto, tal y como aparece etiquetado en el dispositivo.
- **Interfaz**: tipo de interfaz, que puede ser LAN, WAN o DMZ.

Realice los siguientes ajustes:

- **Deshabilitar**: seleccione esta casilla para deshabilitar un puerto. De forma predeterminada, todos los puertos están habilitados.
- **EEE**: marque esta casilla para habilitar la función de eficiencia energética de Ethernet, que reduce el consumo de alimentación durante los periodos de baja actividad de los datos.
- **Prioridad**: seleccione el nivel de prioridad adecuado para cada puerto, que puede ser **Alta** o **Normal**. Esto garantiza la QoS (Quality of Service, calidad del servicio) al priorizar el tráfico para dispositivos en determinados puertos. Por ejemplo, puede asignar un nivel de prioridad alto a un puerto que se use para juegos o videoconferencias. El valor predeterminado es Normal.
- **Modo**: velocidad del puerto y modo dúplex. Cuando se selecciona **Negociación automática**, el dispositivo negocia de forma automática las velocidades de conexión y el modo dúplex con el dispositivo conectado.

## Estado de puerto

La opción Estado de puerto muestra un resumen del estado de los puertos. Haga clic en **Actualizar** para actualizar los datos.

La tabla de Ethernet muestra la siguiente información:

- **Id. de puerto**: ubicación del puerto.
- **Tipo**: tipo de puerto.
- **Estado de enlace**: estado de la conexión.
- **Actividad de puerto**: estado del puerto.
- **Prioridad**: prioridad del puerto definida en la ventana Configuración de puerto.
- **Estado de velocidad**: velocidad del puerto, que puede ser 10 Mbps, 100 Mbps o 1000 Mbps.

- **Estado dúplex**: modo dúplex, que puede ser *Semi* o *Completo*.
- **Negociación automática**: estado del modo dúplex.

# Estadísticas de tráfico

La tabla Estadísticas muestra la siguiente información sobre el puerto seleccionado:

- **Id. de puerto**: ubicación del puerto.
- **Estado de enlace**: estado de la conexión.
- **Paquetes Rx**: número de paquetes recibidos a través del puerto.
- **Paquetes Rx**: número de paquetes recibidos (cantidad expresada en bytes).
- **Paquetes Tx**: número de paquetes enviados a través del puerto.
- **Paquetes Tx**: número de paquetes enviados (cantidad expresada en bytes).
- **Error de paquete**: número de paquetes con errores.

# Pertenencia a VLAN

Todos los puertos LAN están en VLAN 1 de forma predeterminada.

Para habilitar las VLAN, seleccione la opción **Habilitar VLAN**.

Para agregar o editar una VLAN:

- **Id. de VLAN**: identificador de la VLAN.
- **Descripción**: descripción de esta VLAN.
- **Enrutamiento entre VLAN**: hace posible que los paquetes viajen a través de las VLAN. Una VLAN que tenga deshabilitado el enrutamiento entre VLAN quedará aislada de otras VLAN. Se pueden configurar reglas de acceso al cortafuegos para regular aún más (permitir o denegar) el tráfico entre VLAN.
- **Para RV320**, **LAN 1** through **LAN 4** (De LAN 1 a LAN 4): un puerto puede estar etiquetado o sin etiquetar y también se puede excluir de la VLAN.

- **Para RV325**, **LAN 1** through **LAN 14** (De LAN 1 a LAN 14): un puerto puede estar etiquetado o sin etiquetar y también se puede excluir de la VLAN.

## Ajuste QoS:CoS/DSCP

Esta opción agrupa el tráfico por CoS (Classes of Service, clases de servicio), lo que garantiza el ancho de banda y una mayor prioridad para los servicios especificados. Todo el tráfico que no se agrega al Grupo IP utiliza el modo Equilibrador inteligente.

Para configurar las colas de servicios, seleccione la prioridad de la **cola** (4 es el valor máximo y 1 el mínimo) en el menú desplegable.

Para definir el DSCP (Differential Services Code Point, punto de código de servicios diferenciados), seleccione la **Cola** en los menús desplegables.

## Marcado DSCP

El punto de código de servicios diferenciados (o DiffServ) especifica un método sencillo y escalable para clasificar y administrar el tráfico de red y proporcionar calidad del servicio. DiffServ se puede usar para proporcionar baja latencia al tráfico de red crítico (como la voz o el flujo de contenido multimedia) y, a la vez, proporcionar el mejor servicio dentro de lo posible a los servicios no críticos (como el tráfico web o las transferencias de archivos).

Para configurar las colas de servicios, haga clic en **Editar**, configure Cos/802.1p y especifique el estado y la prioridad.

# Configuración de 802.1X

El control de acceso a la red basado en puertos utiliza las características físicas de acceso de las infraestructuras LAN IEEE 802 para brindar un medio de autenticación y autorización de dispositivos conectados a un puerto LAN que posee características de conexión de punto a punto, y para evitar el acceso a dicho puerto en los casos en que falle la autenticación y la autorización. Un puerto en este contexto es un único punto de conexión con la infraestructura de la red LAN.

Para ver esta página, seleccione **Administración de puertos > Configuración de 802.1X.** Para configurar la autenticación basada en puertos:

**PASO 1** Marque **Autenticación basada en puertos** para habilitar esta función.

**PASO 2** Introduzca la dirección IP del servidor RADIUS.

**PASO 3** Escriba el número de **Puerto UDP de RADIUS**.

**PASO 4** Introduzca la clave **secreta de RADIUS**.

**PASO 5** En el menú-desplegable, seleccione **Estado de administración** en la tabla de puertos:

- **Autorizado a la fuerza**: es el estado predeterminado de fábrica de los puertos de la red LAN. Autoriza la interfaz sin autenticación.
- **Fuerza no autorizada**: se niega acceso a la interfaz y se coloca en estado no autorizado. El dispositivo no brinda servicios de autenticación al cliente a través de la interfaz.

  **NOTA** El acceso a la red, incluida la utilidad de administración del enrutador, queda bloqueado para la red LAN cuando todos los puertos de la LAN están configurados como No autorizado a la fuerza. Si el acceso remoto no está habilitado, se deben restablecer los valores predeterminados de fábrica.

- **Automático**: habilita la autenticación basada en puertos. La interfaz alterna entre el estado autorizado o no autorizado, según el intercambio de autenticación entre el dispositivo y el cliente.

**PASO 6** Haga clic en **Guardar**.

8

# Cortafuegos

El principal objetivo de un cortafuegos es controlar el tráfico de red entrante y saliente mediante el análisis de los paquetes de datos y la determinación de si se debe o no permitirles el paso, en función de un conjunto de reglas predeterminado. Un cortafuegos de red construye un puente entre una red interna que se considera segura y de confianza y otra red que suele ser externa (por ejemplo, Internet) y no se considera segura ni de confianza.

## General

Los controles generales del cortafuegos administran las funciones que usan normalmente los navegadores de Internet y las aplicaciones.

**Activación de las funciones del cortafuegos**

Para activar el **cortafuegos**, seleccione la opción **Habilitar**. Las siguientes funciones de cortafuegos se pueden habilitar o deshabilitar según sea necesario:

- **SPI (inspección de paquetes con estado)**: supervisa el estado de las conexiones de red (por ejemplo, los flujos TCP o la comunicación UDP) que viajan por esta. El cortafuegos distingue los paquetes legítimos para los distintos tipos de conexiones. Solo los paquetes que coinciden con una conexión activa conocida pueden pasar por el cortafuegos; los que no, se rechazan.
- **DoS (Denegación de servicio)**: detecta intentos de generar una sobrecarga en el servidor. En líneas generales, los ataques DoS se llevan a cabo forzando el reinicio de los equipos objetivo del ataque, consumiendo sus recursos de forma que no puedan proporcionar el servicio para el que fueron diseñados u obstruyendo los medios de comunicación entre los usuarios previstos y la víctima, de forma tal que no se pueden llevar a cabo unas comunicaciones adecuadas.
- **Bloquear solicitud de WAN**: bloquea las solicitudes TCP y los paquetes ICMP.

- **Administración remota**: cuando se habilita esta opción, permite realizar la administración remota del dispositivo. El puerto predeterminado es el 443. Se puede cambiar por cualquier otro puerto que defina el usuario. La cadena sería https://<IP-WAN>:<puerto-administración-remota>.
- **Tránsito de multidifusión**: permite que los mensajes de multidifusión pasen a través del dispositivo.
- **HTTPS** (Hypertext Transfer Protocol Secure, protocolo seguro de transferencia de hipertexto): es un protocolo de comunicaciones que garantiza la seguridad de las comunicaciones a través de una red informática. En Internet se usa con mucha frecuencia.
- **SIP ALG**: gateway de capa de aplicaciones que aumenta el nivel de un cortafuegos o NAT. Permite conectar los filtros transversales NAT personalizados a la gateway para permitir la conversión de puertos y direcciones para los protocolos *control/data* de SIP.
- **UPnP** (Universal Plug and Play, Plug and Play universal): es un conjunto de protocolos de red que permite que los dispositivos de red (por ejemplo, equipos personales, impresoras, gateways de Internet, puntos de acceso Wi-Fi y dispositivos móviles) puedan detectar mutuamente su presencia sin problemas en la red y establecer unos servicios de red funcionales para compartir datos y para las comunicaciones.
- **SSH**: el shell seguro (SSH) es un protocolo de red que les brinda a los administradores una manera segura de tener acceso a una computadora remota. Los administradores de redes usan mucho SSH para administrar sistemas y aplicaciones de manera remota, lo que les permite iniciar sesión en otra computadora mediante la red, ejecutar comandos y transferir archivos de una computadora a otra.
- **SSH remoto**: el shell remoto seguro es un método para el inicio de sesión remoto seguro desde una computadora a otra. Ofrece numerosas opciones para la autenticación segura y protege la seguridad e integridad de las comunicaciones con un cifrado fuerte.

**Restricción de características Web**

Para restringir las características Web **Java**, **Cookies**, **ActiveX** o **Acceso a servidores proxy HTTP**, active la casilla correspondiente.

Para permitir *únicamente* las características seleccionadas (Java, Cookies, ActiveX o Acceso a servidores proxy HTTP) y restringir todas las demás, active la opción **Excepción**.

**Configuración de nombres de dominio de confianza**

Para agregar dominios de confianza, haga clic en **Agregar** y especifique el **nombre de dominio**.

Para editar un dominio de confianza, haga clic en **Editar** y modifique el **nombre de dominio**.

# Reglas de acceso

Las reglas de acceso limitan el acceso a la subred al permitir o denegar el acceso de dispositivos o servicios específicos identificados mediante su dirección IP.

Para agregar o editar un servicio, haga clic en **Administración de servicios**. Esta función se describe en **Adición o edición de un nombre de servicio**.

**Adición de una regla de acceso a la Tabla de reglas de acceso de IPv4**

Para agregar (o editar) una regla de acceso de IPv4:

**PASO 1** Haga clic en la ficha **IPv4**.

**PASO 2** Haga clic en **Agregar** (o seleccione una fila y haga clic en **Editar**).

**PASO 3** En el menú desplegable, seleccione la acción **Permitir** o **Denegar** para aplicarla a esta regla.

**PASO 4** En el menú desplegable, seleccione un **servicio**.

**PASO 5** Seleccione **Registrar paquetes que coincidan con esta regla** o **No registrar**.

**PASO 6** En el menú desplegable, seleccione la **interfaz de origen**.

**PASO 7** En el menú desplegable, seleccione la dirección **IP de origen**. Si seleccionó **Única**, especifique la dirección IP de origen. Si seleccionó **Rango**, especifique el rango de direcciones IP de origen.

**PASO 8** En el menú desplegable, seleccione la dirección **IP de destino**. Si seleccionó **Única**, especifique la dirección IP de destino. Si seleccionó **Rango**, especifique el rango de direcciones IP de destino.

**PASO 9** Seleccione la hora para configurar la **programación** de esta regla de acceso. Seleccione **Siempre** para que la regla de acceso esté en vigor las 24 horas del día. Seleccione **Intervalo** para definir una hora y especifique las horas y los minutos durante los que estará activa la regla de acceso en los campos **Desde** y

**Hasta**. Por ejemplo, desde las *07:00* hasta las *20:00*. La regla de acceso no permite definir dos intervalos de tiempo.

**PASO 10** Seleccione la opción **Entra en vigor** para seleccionar los días de la semana.

**PASO 11** Haga clic en **Guardar**.

---

**Adición de una regla de acceso a la Tabla de reglas de acceso de IPv6**

Para agregar (o editar) una regla de acceso de IPv6:

---

**PASO 1** Haga clic en la ficha **IPv6**.

**PASO 2** Haga clic en **Agregar** (o seleccione una fila y haga clic en **Editar**).

**PASO 3** En el menú desplegable, seleccione la acción **Permitir** o **Denegar** para aplicarla a esta regla.

**PASO 4** En el menú desplegable, seleccione el **servicio**.

**PASO 5** En el menú desplegable, seleccione el **registro**.

**PASO 6** En el menú desplegable, seleccione la **interfaz de origen**.

**PASO 7** En el menú desplegable, seleccione un valor en **Longitud de prefijo/IP de origen**. Si seleccionó **Única**, especifique el prefijo IP de origen. Si seleccionó **Rango**, especifique el prefijo IP de inicio y la longitud del prefijo.

**PASO 8** En el menú desplegable, seleccione un valor en **Destination Prefix Length** (Longitud del prefijo de destino). Si seleccionó **Única**, especifique el prefijo IP de destino. Si seleccionó **Rango**, especifique el prefijo IP de inicio y la longitud del prefijo.

**PASO 9** Haga clic en **Guardar**.

---

# Filtro de contenido

El Filtro de contenido permite limitar el acceso a determinados sitios web no deseados. Puede bloquear el acceso a sitios web según nombres de dominio o palabras clave. También es posible programar el momento en que el filtro de contenido se activa. Para configurar y habilitar el Filtro de contenido, siga estos pasos.

**PASO 1** Haga clic en Firewall > Filtro de contenido.

**PASO 2** Seleccione **Bloquear dominios prohibidos** para bloquear determinadas páginas web o seleccione **Aceptar dominios permitidos** para aceptar determinadas páginas web.

**PASO 3** En la sección Dominios prohibidos, seleccione **Habilitar** para habilitar los dominios prohibidos.

**PASO 4** En la Tabla de dominios prohibidos, haga clic en **Añadir** para agregar el nombre de dominio y escríbalo. Haga clic en **Editar** o **Eliminar** para modificar un dominio existente en la Tabla de dominios prohibidos.

**PASO 5** En la sección Bloqueo de sitios web mediante palabras clave, seleccione **Habilitar** para habilitar el bloqueo de dominios.

**PASO 6** En la tabla Bloqueo de sitios web mediante palabras clave, haga clic en **Añadir** y escriba las palabras clave que deben bloquearse.

**PASO 7** Para especificar cuándo deben estar activas las reglas de filtrado, configure la programación seleccionando la hora de la lista desplegable. Puede personalizar los campos Desde y Hasta, y seleccionar el día de inicio del filtro.

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

9

# VPN

Una VPN es una conexión entre dos puntos de terminación en distintas redes que permite enviar datos privados de forma segura a través de una red compartida o pública, como Internet. Este túnel establece una red privada que puede enviar datos de forma segura usando técnicas de autenticación y cifrado estándar en el sector para garantizar la protección de los datos que se mandan.

## Resumen

Esta función muestra información general acerca de los ajustes del túnel VPN. El dispositivo admite hasta 100 túneles. El rango de IP virtuales está reservado para los usuarios de Easy VPN o los clientes de VPN que se conectan a este dispositivo teniendo activada la opción de configuración de modo (descrita en **Ajustes avanzados para IKE con clave precompartida e IKE con certificado**).

Para definir un rango de direcciones IP para que se usen en los túneles VPN, haga clic en **Editar** y especifique los siguientes parámetros:

- **Inicio de rango** y **Fin de rango**: inicio y finalización del rango de direcciones IP usadas para los túneles VPN.
- **Servidor DNS 1** y **Servidor DNS 2**: dirección IP opcional de un servidor DNS. Si especifica un segundo servidor DNS, el dispositivo usa el primero que responda. Especificar un servidor DNS puede proporcionar un acceso más rápido que si se usa un servidor DNS asignado dinámicamente. Use el ajuste predeterminado (0.0.0.0) para utilizar un servidor DNS asignado dinámicamente.
- **Servidor WINS 1** y **Servidor WINS 2**: dirección IP opcional de un servidor WINS. WINS (Windows Internet Naming Service, servidor de servicios de nombres de Internet de Windows) permite convertir los nombres de NetBIOS en direcciones IP. Si no conoce la dirección IP del servidor WINS, use el valor predeterminado (0.0.0.0).

- **Nombre de dominio 1** hasta **4**: si este router tiene una dirección IP estática y un nombre de dominio registrado, por ejemplo, *MiServidor.MiDominio.com*, escriba el **nombre de dominio** que se debe usar para la autenticación. Un nombre de dominio se puede usar solo para una conexión de túnel.

La opción **Estado del túnel VPN** muestra el número de **Túneles utilizados**, **Túneles disponibles**, **Túneles habilitados** y **Túneles definidos**.

**Tabla de conexiones de estados de los túneles**

La Tabla de conexiones muestra las entradas creadas en **VPN** > **De gateway a gateway** y **VPN** > **De cliente a gateway**:

- (Túnel) **No**: número de Id. del túnel generado automáticamente.
- (Túnel) **Nombre**: nombre de este túnel VPN, por ejemplo, Oficina de Los Ángeles, Sucursal de Chicago o División de Nueva York. Esta descripción es de referencia. No es necesario que concuerde con el nombre utilizado en el otro extremo del túnel.
- **Estado**: estado del túnel VPN, que puede ser *Conectado* o *Waiting for Connection* (Esperando conexión).
- **Cif./Aut./Grupo de fase 2**: tipo de cifrado de fase 2 (NULL, DES, 3DES, AES-128, AES-192 o AES-256), método de autenticación (NULL, MD5 o SHA1) y el número de grupo DH (1, 2 o 5).
- **Grupo local**: dirección IP y máscara de subred del grupo local.
- **Grupo remoto**: dirección IP y máscara de subred del grupo remoto.
- **Gateway remota**: dirección IP de la gateway remota.
- **Acción**: conecta/desconecta el túnel.

**Tabla de conexión de estado de FlexVPN**

En la tabla de conexión se muestran las entradas creadas en **VPN > FlexVPN (spoke)**:

- **Nombre**: nombre de esta FlexVPN. Esta descripción es a modo de referencia; no es necesario que coincida con el nombre usado en el otro extremo del túnel.
- **Estado**: estado de la FlexVPN, conectado o esperando conexión.
- **Red de spoke**: la subred de spoke.
- **Dirección IP virtual de spoke**: la dirección IP virtual de spoke.

- **Dirección IP del hub**: la dirección IP del hub.
- **Dirección IP virtual del hub**: la dirección IP virtual del hub.
- **Red del hub**: la subred del hub.
- **Acción**: conectar o desconectar el túnel.

**Tabla de conexiones de estado de las VPN de grupo**

La Tabla de conexiones muestra las entradas creadas en **VPN** > **De cliente a gateway**:

- **Nombre de grupo**: nombre de este túnel VPN. Esta descripción es de referencia. No es necesario que concuerde con el nombre utilizado en el otro extremo del túnel.
- **Túneles**: número de usuarios registrados en las VPN de grupo.
- **Cif./Aut./Grupo de fase 2**: tipo de cifrado de fase 2 (NULL, DES, 3DES, AES-128, AES-192 o AES-256), método de autenticación (NULL, MD5 o SHA1) y el número de grupo DH (1, 2 o 5).
- **Grupo local**: dirección IP y máscara de subred del grupo local.
- **Cliente remoto**: dirección IP y máscara de subred del cliente remoto.
- **Detalles**: dirección IP de la gateway remota.
- **Acción**: conecta/desconecta el túnel.

# De gateway a gateway

En una VPN de ubicación a ubicación de gateway a gateway, el router local de una oficina se conecta con un router remoto a través de un túnel VPN. Los dispositivos cliente pueden acceder a los recursos de red como si estuvieran todos en la misma ubicación. Este modelo se puede usar para varios usuarios de una oficina remota.

Para que una conexión se efectúe correctamente, es necesario que, como mínimo, uno de los routers se pueda identificar mediante una dirección IP estática o un nombre de host de DNS dinámico. Como alternativa, si un router tiene solo una dirección IP dinámica, se puede usar cualquier dirección de correo electrónico como autenticación para establecer la conexión.

Los dos extremos del túnel no pueden estar en la misma subred. Por ejemplo, si la LAN de la Ubicación A utiliza la subred 192.168.1.x/24, la Ubicación B puede usar 192.168.2.x/24.

Para configurar un túnel, especifique los ajustes correspondientes (invirtiendo los datos de *local* y *remoto*) al configurar los dos routers. Supongamos que este router se llama Router A. Especifique los ajustes necesarios en la sección *Configuración de grupo local*. Especifique los ajustes del otro router (Router B) en la sección *Configuración de grupo remoto*. Al configurar el otro router (Router B), especifique sus ajustes en la sección *Configuración de grupo local*. Los ajustes del Router A deben especificarse en la sección *Configuración de grupo remoto*.

## Agregar un nuevo túnel

Especifique los ajustes para un túnel:

- **Número de túnel**: número de Id. del túnel.
- **Nombre de túnel**: nombre de este túnel VPN, por ejemplo, Oficina de Los Ángeles, Sucursal de Chicago o División de Nueva York. Esta descripción es de referencia. No es necesario que concuerde con el nombre utilizado en el otro extremo del túnel.
- **Interfaz**: puerto WAN que se debe usar para este túnel.
- **Modo de creación de claves**: identifica el tipo de seguridad del túnel, que puede ser Manual, IKE con clave precompartida o IKE con certificado.
- **Habilitar**: seleccione esta casilla para habilitar el túnel VPN o desactívela para deshabilitar el túnel. El túnel está habilitado de forma predeterminada.

## Configuración de grupo local

Especifique los ajustes para la configuración de grupo local de este router. (Replique estos ajustes cuando configure el túnel VPN en el otro router).

**NOTA** Todas las opciones están documentadas, pero solo se muestran aquellas opciones que están relacionadas con el parámetro seleccionado.

**Modo de creación de claves = Manual o IKE con clave precompartida**

- **Tipo de gateway de seguridad local**: método de identificación del router para establecer el túnel VPN. La gateway de seguridad local está en este router. Por el contrario, la gateway de seguridad remota está en el otro router. Al menos uno de los routers debe tener una dirección IP estática o un nombre de host de DNS para poder establecer una conexión.
  - **Solo IP**: este router tiene una dirección IP de WAN estática. La dirección IP de WAN aparece automáticamente.
  - **IP + Certificado**: este router tiene una dirección IP de WAN estática que aparece automáticamente. Esta opción solo está disponible cuando se selecciona IKE con certificado.
  - **IP + Autenticación de nombre de dominio (FQDN)**: este dispositivo tiene una dirección IP estática y un nombre de dominio registrado, por ejemplo, *MiServidor.MiDominio.com*. Especifique también un valor en **Nombre de dominio** para usarlo en la autenticación. El nombre de dominio se puede usar solo para una conexión de túnel.
  - **IP + Autenticación de dirección de correo electrónico (FQDN DE USUARIO)**: este dispositivo tiene una dirección IP estática y se utiliza una dirección de correo electrónico para la autenticación. La dirección IP de WAN aparece automáticamente. Especifique la **dirección de correo electrónico** para usarla en la autenticación.
  - **IP dinámica + Autenticación de nombre de dominio (FQDN)**: este router tiene una dirección IP dinámica y un nombre de host de DNS dinámico registrado (ofrecido por proveedores como DynDNS.com). Especifique un valor en **Nombre de dominio** para usarlo en la autenticación. El nombre de dominio se puede usar solo para una conexión de túnel.
  - **IP dinámica + Autenticación de dirección de correo electrónico (FQDN DE USUARIO)**: este router tiene una dirección IP dinámica y no tiene un nombre de host de DNS dinámico. Especifique una **dirección de correo electrónico** para usarla en la autenticación.

    Si ambos routers tienen direcciones IP dinámicas (como las conexiones PPPoE), no elija **IP dinámica + Dirección de correo electrónico** para las dos gateways. Para la gateway remota, elija **Dirección IP** e **IP por DNS resuelta**.

- **Tipo de grupo de seguridad local**: permite seleccionar una única dirección **IP**, una **subred** o un **rango IP** (dirección) en una subred.
  - **Dirección IP**: especifique un dispositivo que pueda usar este túnel. Especifique la **dirección IP** del dispositivo.
  - **Subred**: permite que todos los dispositivos de una subred utilicen el túnel VPN. Especifique la **dirección IP** de la subred y la **máscara de subred**.

**Configuración de grupo remoto**

Especifique los ajustes para la opción Configuración de grupo remoto de este router:

- **Tipo de gateway de seguridad remota**: método de identificación del router para establecer el túnel VPN. La gateway de seguridad remota es el otro router. Al menos uno de los routers debe tener una dirección IP estática o un nombre de host de DNS dinámico para poder establecer una conexión.
  - **Solo IP**: dirección IP de WAN estática. Si conoce la dirección IP del router VPN remoto, elija **Dirección IP** y especifique la dirección. Si no conoce la dirección IP del router VPN remoto, seleccione **IP por DNS resuelta** y escriba el nombre de dominio del router. Un router Cisco puede obtener la dirección IP de un dispositivo VPN remoto en función del DNS resuelto.
  - **IP + Autenticación de nombre de dominio (FQDN)**: este router tiene una dirección IP estática y un nombre de dominio registrado, por ejemplo, *MiServidor.MiDominio.com*. Si conoce la dirección IP del router VPN remoto, elija **Dirección IP** y especifique la dirección. Si no conoce la dirección IP del router VPN remoto, seleccione **IP por DNS resuelta** y escriba el nombre de dominio del router. Los routers Cisco pueden obtener la dirección IP de un dispositivo VPN remoto en función del DNS resuelto.
  - **IP + Autenticación de dirección de correo electrónico (FQDN DE USUARIO)**: este router tiene una dirección IP estática y el usuario puede utilizar una dirección de correo electrónico para la autenticación. Si conoce la dirección IP del router VPN remoto, elija **Dirección IP** y especifique la dirección IP. Si no conoce la dirección IP del router VPN remoto, seleccione **IP por DNS resuelta** y escriba el nombre de dominio real del router. Los routers Cisco pueden obtener la dirección IP de un dispositivo VPN remoto en función del DNS resuelto.

- **IP dinámica + Autenticación de nombre de dominio (FQDN)**: este router tiene una dirección IP dinámica y un nombre de host de DNS dinámico registrado (ofrecido por proveedores como DynDNS.com). Especifique un valor en **Nombre de dominio** para usarlo en la autenticación. El nombre de dominio se puede usar solo para una conexión de túnel.
- **IP dinámica + Autenticación de dirección de correo electrónico (FQDN DE USUARIO)**: este router tiene una dirección IP dinámica y no tiene un nombre de host de DNS dinámico. Especifique una **dirección de correo electrónico** para usarla en la autenticación.
  Si ambos routers tienen direcciones IP dinámicas (como las conexiones PPPoE), *no* elija **IP dinámica + Dirección de correo electrónico** para las dos gateways. Para la gateway remota, elija **Dirección IP** o **IP por DNS resuelta**.

- **Tipo de grupo de seguridad local**: recursos LAN que pueden usar este túnel. El Grupo de seguridad local es para los recursos LAN de este router. El Grupo de seguridad remoto es para los recursos LAN del otro router.
  - **Dirección IP**: especifique un dispositivo que pueda usar este túnel. Especifique la **dirección IP** del dispositivo.
  - **Subred**: permite que todos los dispositivos de una subred utilicen el túnel VPN. Especifique la **dirección IP** de la subred y la **máscara de subred**.

**Configuración de IPSec**

Para que el cifrado sea correcto, los dos extremos de un túnel VPN deben coincidir en los métodos de cifrado, descifrado y autenticación. Especifique exactamente los mismos ajustes para los dos routers.

Especifique los ajustes para la fase 1 y la fase 2. En la fase 1 se establecen las claves precompartidas para crear un canal de comunicación autenticado y seguro. En la fase 2, los pares IKE utilizan el canal seguro para negociar las asociaciones de seguridad en nombre de otros servicios como IPsec. Hay que especificar los mismos ajustes cuando se configure el otro router para este túnel.

- **Grupo DH, fase 1/ fase 2**: DH (Diffie-Hellman) es un protocolo de intercambio de claves. Hay tres grupos de longitudes de claves principales diferentes: Grupo 1: 768 bits, Grupo 2: 1024 bits y Grupo 5: 1536 bits. Para conseguir una mayor velocidad y un menor nivel de seguridad, elija la opción **Grupo 1**. Para conseguir una velocidad menor y un mayor nivel de seguridad, elija la opción **Grupo 5**. El Grupo 1 está seleccionado de manera predeterminada.

- **Cifrado, fase 1/fase 2**: método de cifrado para esta fase, que puede ser DES, 3DES, AES-128, AES-192 o AES-256. El método determina la longitud de la clave usada para cifrar o descifrar los paquetes ESP. Se recomienda usar AES-256 porque es más seguro.
- **Autenticación, fase 1/fase 2**: método de autenticación para esta fase, que puede ser MD5 o SHA1. El método de autenticación determina la forma en que se validan los paquetes de encabezado ESP (Encapsulating Security Payload, carga de seguridad encapsulada). MD5 es un algoritmo de hash unidireccional que produce un resumen de 128 bits. SHA1 es un algoritmo de hash unidireccional que produce un resumen de 160 bits. Se recomienda usar SHA1 porque es más seguro. Los dos extremos del túnel VPN deben utilizar el mismo método de autenticación.
- **Vigencia de SA, fase 1/fase 2:** tiempo durante el cual un túnel VPN está activo en esta fase. El valor predeterminado para la fase 1 es de 28800 segundos. El valor predeterminado para la fase 2 es de 3600 segundos.
- **Seguridad perfecta hacia delante**: cuando se habilita PFS (Perfect Forward Secrecy, seguridad perfecta hacia delante), la negociación de IKE de fase 2 generará un nuevo material de clave para el cifrado y la autenticación del tráfico de IP, de forma que los hackers que utilicen la fuerza bruta para romper las claves de cifrado no puedan obtener las claves IPsec futuras. Si desea habilitar esta función, active la casilla; en caso contrario, desactívela. Se recomienda utilizar esta función.
- **Clave precompartida**: clave precompartida que se debe usar para autenticar el par IKE remoto. Se pueden especificar hasta 30 caracteres del teclado o valores hexadecimales, por ejemplo, Mi_@123 o 4d795f40313233 (los caracteres ' ' " \ no se pueden utilizar). Ambos extremos del túnel VPN deben usar la misma clave precompartida. Se recomienda encarecidamente cambiar la clave precompartida de forma periódica para maximizar la seguridad de la VPN.
- **Complejidad de clave precompartida mínima**: active la casilla **Habilitar** para activar el Medidor de seguridad de clave precompartida.
- **Medidor de seguridad de clave precompartida**: al habilitar la opción Complejidad de clave precompartida mínima, este medidor indica el nivel de seguridad de la clave precompartida. Al especificar una clave precompartida, aparecen barras de colores. La escala de colores va desde el rojo (débil) hasta el verde (segura) pasando por el amarillo (aceptable).

**SUGERENCIA** Especifique una clave precompartida compleja que tenga más de ocho caracteres, letras en mayúscula y minúscula, números y símbolos como -*^+=.

## Ajustes avanzados para IKE con clave precompartida e IKE con certificado

Para la mayoría de los usuarios, los ajustes básicos son suficientes. Sin embargo, los usuarios avanzados pueden hacer clic en **Avanzado** para mostrar los ajustes avanzados. Si cambia los ajustes avanzados en un router, también deberá cambiarlos en el otro router.

- **Modo agresivo**: se pueden aplicar dos modos de negociación SA de IKE, que son el Modo principal y el Modo agresivo. Si la seguridad de la red es el aspecto prioritario, se recomienda aplicar el Modo principal. Si la velocidad de la red es el aspecto prioritario, se recomienda aplicar el Modo agresivo. Active esta casilla para habilitar el Modo agresivo o déjela desactivada si desea usar el Modo principal.

  Si el Tipo de gateway de seguridad remota es uno de los tipos de *IP dinámica*, hay que utilizar el Modo agresivo. La casilla está activada automáticamente. Este ajuste no se puede cambiar.

- **Comprimir (compatible con el protocolo de compresión de carga útil de IP [IPComp])**: un protocolo que reduce el tamaño de los datagramas IP. Active la casilla para que el router pueda proponer la compresión al iniciar una conexión. Si el retransmisor rechaza esta propuesta, el router no aplicará la compresión. Cuando el router es el retransmisor, acepta la compresión, incluso si esta no está habilitada. Si habilita esta función para este router, también tendrá que habilitarla en el router en el otro extremo del túnel.

- **Mantener activo**: intenta restablecer la conexión VPN en caso de que se produzca alguna interrupción.

- **Algoritmo de hash de AH**: el protocolo AH (Authentication Header, encabezado de autenticación) describe el formato del paquete y los estándares predeterminados para la estructura del paquete. Cuando AH es el protocolo de seguridad, la protección se extiende al encabezado IP para comprobar la integridad de todo el paquete. Active la casilla para usar esta función y seleccionar un método de autenticación: MD5 o SHA1. MD5 genera un resumen de 128 bits para autenticar los datos del paquete. SHA1 genera un resumen de 160 bits para autenticar los datos del paquete. Ambos extremos del túnel deben usar el mismo algoritmo.

- **Difusión de NetBIOS**: difunde los mensajes utilizados para la resolución de nombres en las redes Windows para identificar los recursos, por ejemplo, equipos, impresoras y servidores de archivos. Estos mensajes los utilizan algunas aplicaciones de software y funciones de Windows, por ejemplo, el Entorno de red. El tráfico de difusión LAN normalmente no se reenvía a través de un túnel VPN. Sin embargo, se puede activar esta casilla para permitir que las difusiones de NetBIOS procedentes de un extremo del túnel se difundan de nuevo hasta el otro extremo.
- **NAT Traversal**: NAT (Network Address Translation, conversión de direcciones de red) permite a los usuarios que tengan direcciones de LAN privadas acceder a los recursos de Internet utilizando una dirección IP públicamente enrutable como dirección de origen. Sin embargo, para el tráfico entrante, la gateway de NAT no tiene un método automático para convertir la dirección IP pública a un destino concreto de la LAN privada. Este problema impide que se realicen correctamente los intercambios de IPsec. Si el router VPN está detrás de una gateway de NAT, active esta casilla para habilitar la opción NAT Traversal. Hay que utilizar el mismo ajuste en los dos extremos del túnel.
- **Detección de par inactivo (DPD)**: envía periódicamente mensajes de saludo y confirmación (HELLO/ACK) para comprobar el estado del túnel VPN. Esta función debe estar habilitada en ambos extremos del túnel VPN. Especifique el intervalo entre los mensajes HELLO/ACK en el campo **Intervalo**.
- **Autenticación ampliada**: utiliza un nombre de usuario de host IPsec y una contraseña para autenticar los clientes de VPN. También puede utilizar la base de datos de usuarios hallada en Administración de usuarios. Tanto el host IPSec como el dispositivo perimetral deben admitir la autenticación ampliada. Para usar el **host IPsec**, haga clic en el botón de opción y especifique un valor en los campos **Nombre de usuario** y **Contraseña**. Para usar la opción **Dispositivo perimetral**, haga clic en el botón de opción y seleccione la base de datos en el menú desplegable. Para agregar o editar la base de datos, haga clic en **Agregar/Editar** para mostrar la ventana Administración de usuarios.

- **Copia de seguridad de túnel**: cuando DPD determina que el par remoto no está disponible, esta función permite que el router restablezca el túnel VPN usando una dirección IP alternativa para el par remoto o una interfaz WAN local alternativa. Active la casilla para habilitar esta función y especifique los siguientes ajustes. Esta función está disponible solo si está habilitada la opción de detección de par inactivo.
  - **Dirección IP de copia de seguridad remota**: dirección IP alternativa para el par remoto. También puede volver a especificar la dirección IP de WAN que se haya especificado previamente para la gateway remota.
  - **Interfaz local**: interfaz WAN que se debe usar para restablecer la conexión.
  - **Tiempo de inactividad para túnel VPN de respaldo**: cuando el router se inicia y el túnel principal no se conecta durante el periodo de tiempo especificado, se utiliza el túnel de respaldo. El tiempo de inactividad predeterminado es de 30 segundos.
- **Dividir DNS**: envía algunas de las solicitudes DNS a un servidor DNS y otras solicitudes DNS a otro servidor DNS, en función de los nombres de dominio especificados. Cuando el router reciba una solicitud de resolución de direcciones procedente de un cliente, el router inspecciona el nombre de dominio. Si coincide con uno de los nombres de dominio del ajuste Dividir DNS, la solicitud se pasa al servidor DNS especificado. De lo contrario, la solicitud se pasa al servidor DNS que está especificado en los ajustes de la interfaz WAN.

  **Servidor DNS 1** y **Servidor DNS 2**: dirección IP del servidor DNS que se debe usar para los dominios especificados. Si lo desea, puede especificar un servidor DNS secundario en el campo **Servidor DNS 2**.

  **Nombre de dominio 1** a **Nombre de dominio 4**: especifique los nombres de dominio para los servidores DNS. Las solicitudes para estos dominios se pasan a los servidores DNS especificados.

# De cliente a gateway

Esta función crea un nuevo túnel VPN que permite a los teletrabajadores y a aquellos que viajan por negocios acceder a la red usando software cliente de VPN de terceros, como TheGreenBow.

Configure un túnel VPN para un usuario remoto, una VPN de grupo para varios usuarios remotos o una Easy VPN:

- **Túnel**: crea un túnel para un único usuario remoto. El número del túnel se genera de forma automática.
- **VPN de grupo**: crea un túnel para un grupo de usuarios, por lo que se elimina la necesidad de configurar usuarios individuales. Todos los usuarios remotos pueden usar la misma clave precompartida para conectarse con el dispositivo hasta alcanzar el número máximo de túneles admitidos. El router admite hasta dos grupos VPN. El número del grupo se genera de forma automática.
- **Easy VPN**: permite a los usuarios remotos conectarse con este dispositivo usando un cliente de VPN de Cisco (también conocido como *Cisco Easy VPN Client*), que está disponible en el CD del producto:
  - La versión 5.0.07 es compatible con Windows 7 (32 y 64 bits), Windows Vista (32 y 64 bits) y Windows XP (32 bits)
  - La versión 4.9 es compatible con Mac OS X 10.4 y 10.5.
  - La versión 4.8 es compatible con Linux basado en Intel.

  Para configurar una Easy VPN, configure una contraseña de grupo en esta página y agregue un nombre de usuario y una contraseña para cada usuario del cliente de VPN de Cisco en la Tabla de administración de usuarios, incluida en la sección **Administración de usuarios**. Al agregar un usuario, el grupo Unassigned (Sin asignar) debería estar seleccionado. Los otros grupos se usan para la VPN SSL.

### Configuración de un túnel o una VPN de grupo

Especifique la siguiente información:

- **Nombre de túnel**: nombre descriptivo del túnel. Para un único usuario, puede especificar el nombre de usuario o la ubicación. Si se trata de una VPN de grupo, se puede especificar la ubicación o la función empresarial del grupo. Esta descripción es de referencia. No es necesario que concuerde con el nombre utilizado en el otro extremo del túnel.
- **Interfaz**: puerto WAN.
- **Modo de creación de claves**: elija el método de administración de claves:
  - **Manual**: permite generar la clave personalmente, pero no habilita la negociación de claves. La administración manual de claves se utiliza en entornos estáticos pequeños o con el fin de solucionar problemas. Especifique los ajustes necesarios.
  - **IKE** (Internet Key Exchange) **con clave precompartida**: use este protocolo para configurar una SA (Security Association) para el túnel. (este es el ajuste recomendado). Si selecciona **VPN de grupo**, esta es la única opción disponible.
  - **IKE con certificado**: se usa un certificado para autenticar el par de IKE remoto.
- **Habilitar**: active esta opción para habilitar esta VPN.

### Configuración de grupo local

Especifique la siguiente información:

- **Tipo de gateway de seguridad local**: método de identificación del router para establecer el túnel VPN. La gateway de seguridad remota es el otro router. Al menos uno de los routers debe tener una dirección IP estática o un nombre de host de DNS dinámico para poder establecer una conexión.
  - **Solo IP**: dirección IP de WAN estática. Si conoce la dirección IP del router VPN remoto, elija **Dirección IP** y especifique la dirección. Si no conoce la dirección IP del router VPN remoto, seleccione **IP por DNS resuelta** y escriba el nombre de dominio del router. Un router Cisco puede obtener la dirección IP de un dispositivo VPN remoto en función del DNS resuelto.

- **IP + Autenticación de nombre de dominio (FQDN)**: este dispositivo tiene una dirección IP estática y un nombre de dominio registrado, por ejemplo, *MiServidor.MiDominio.com*. Si conoce la dirección IP del router VPN remoto, elija **Dirección IP** y especifique la dirección. Si no conoce la dirección IP del router VPN remoto, seleccione **IP por DNS resuelta** y escriba el nombre de dominio del router. Los routers Cisco pueden obtener la dirección IP de un dispositivo VPN remoto en función del DNS resuelto.
- **IP + Autenticación de dirección de correo electrónico (FQDN DE USUARIO)**: este dispositivo tiene una dirección IP estática y utiliza una dirección de correo electrónico para la autenticación. Si conoce la dirección IP del router VPN remoto, elija **Dirección IP** y especifique la dirección IP. Si no conoce la dirección IP del router VPN remoto, seleccione **IP por DNS resuelta** y escriba el nombre de dominio real del router. Los routers Cisco pueden obtener la dirección IP de un dispositivo VPN remoto en función del DNS resuelto.
- **IP dinámica + Autenticación de nombre de dominio (FQDN)**: este router tiene una dirección IP dinámica y un nombre de host de DNS dinámico registrado (ofrecido por proveedores como DynDNS.com). Especifique un valor en **Nombre de dominio** para usarlo en la autenticación. El nombre de dominio se puede usar solo para una conexión de túnel.
- **IP dinámica + Autenticación de dirección de correo electrónico (FQDN DE USUARIO)**: este router tiene una dirección IP dinámica y no tiene un nombre de host de DNS dinámico. Especifique una **dirección de correo electrónico** para usarla en la autenticación.

  Si ambos routers tienen direcciones IP dinámicas (como las conexiones PPPoE), no elija IP dinámica + Dirección de correo electrónico para las dos gateways. Para la gateway remota, elija **Dirección IP** e **IP por DNS resuelta**.

- **Tipo de grupo de seguridad local**: especifique los recursos LAN que pueden acceder a este túnel.
  - **Dirección IP**: elija esta opción para que solo un dispositivo LAN pueda acceder al túnel VPN. A continuación, especifique la dirección IP del equipo. Solo este dispositivo puede usar este túnel VPN.
  - **Subred**: elija esta opción (que es la predeterminada) para permitir que todos los dispositivos de una subred puedan acceder al túnel VPN. Especifique la máscara y la dirección IP de la subred.

### Configuración de cliente remoto para un único usuario

Especifique el método para identificar al cliente para establecer el túnel VPN. Las siguientes opciones están disponibles para una VPN de usuario único o de tipo *túnel*:

- **Solo IP**: el cliente de VPN remoto tiene una dirección IP de WAN estática. Si conoce la dirección IP del cliente, elija **Dirección IP** y especifique la dirección. Si no conoce la dirección IP del cliente, seleccione **IP por DNS resuelta** y escriba el nombre de dominio del cliente en Internet. El router obtiene la dirección IP del cliente de la VPN remota usando el DNS resuelto. La dirección IP del cliente de la VPN remota se muestra en la sección Estado de VPN en la página Resumen.
- **IP + Autenticación de nombre de dominio (FQDN)**: el cliente tiene una dirección IP estática y un nombre de dominio registrado. Especifique también un valor en **Nombre de dominio** para usarlo en la autenticación. El nombre de dominio se puede usar solo para una conexión de túnel.

  Si conoce la dirección IP del cliente de la VPN remota, elija **Dirección IP** y especifique la dirección. Si no conoce la dirección IP del cliente de la VPN remota, seleccione **IP por DNS resuelta** y escriba el nombre de dominio real del cliente en Internet. El router obtiene la dirección IP del cliente de la VPN remota usando el DNS resuelto. La dirección IP del cliente de la VPN remota se mostrará en la sección Estado de VPN en la página Resumen.
- **IP + Autenticación de dirección de correo electrónico (FQDN DE USUARIO)**: el cliente tiene una dirección IP estática y el usuario puede utilizar cualquier dirección de correo electrónico para la autenticación. La dirección IP de WAN actual aparece automáticamente. Especifique cualquier **dirección de correo electrónico** para usarla en la autenticación.

  Si conoce la dirección IP del cliente de la VPN remota, elija **Dirección IP** y especifique la dirección. Si no conoce la dirección IP del cliente de la VPN remota, seleccione **IP por DNS resuelta** y escriba el nombre de dominio real del cliente en Internet. El dispositivo obtiene la dirección IP de un cliente de la VPN remota usando el DNS resuelto. La dirección IP del dispositivo de la VPN remota se muestra en la sección Estado de VPN en la página Resumen.
- **IP dinámica + Autenticación de nombre de dominio (FQDN)**: el cliente tiene una dirección IP dinámica y un nombre de host de DNS dinámico registrado (suministrado por proveedores como DynDNS.com). Especifique un valor en **Nombre de dominio** para usarlo en la autenticación. El nombre de dominio se puede usar solo para una conexión de túnel.

- **IP dinámica + Autenticación de dirección de correo electrónico (FQDN DE USUARIO)**: el cliente tiene una dirección IP dinámica y no tiene un nombre de host de DNS dinámico. Especifique cualquier **dirección de correo electrónico** para usarla en la autenticación.

**Configuración de un cliente remoto para un grupo**

Especifique el método para identificar a los clientes para establecer el túnel VPN. Las siguientes opciones están disponibles para las VPN de grupo:

- **Autenticación de nombre de dominio (FQDN)**: identifica al cliente mediante un nombre de dominio registrado. Especifique un valor en **Nombre de dominio** para usarlo en la autenticación. El nombre de dominio se puede usar solo para una conexión de túnel.
- **Autenticación de dirección de correo electrónico (FQDN DE USUARIO)**: identifica al cliente mediante la dirección de correo electrónico para la autenticación. Especifique la dirección en los campos proporcionados.
- **Cliente VPN Microsoft XP/2000**: el software cliente es el cliente VPN Microsoft XP/2000 integrado.

**Configuración de IPSec**

Para que el cifrado sea correcto, los dos extremos de un túnel VPN deben coincidir en los métodos de cifrado, descifrado y autenticación. Especifique exactamente los mismos ajustes para los dos routers.

Especifique los ajustes para la fase 1 y la fase 2. En la fase 1 se establecen las claves precompartidas para crear un canal de comunicación autenticado y seguro. En la fase 2, los pares IKE utilizan el canal seguro para negociar las asociaciones de seguridad para otros servicios como IPsec. Hay que especificar los mismos ajustes cuando se configuren otros routers para este túnel.

- **Grupo DH, fase 1/ fase 2**: DH (Diffie-Hellman) es un protocolo de intercambio de claves. Hay tres grupos de longitudes de claves principales diferentes: Grupo 1: 768 bits, Grupo 2: 1024 bits y Grupo 5: 1536 bits. Para conseguir una mayor velocidad y un menor nivel de seguridad, elija la opción **Grupo 1**. Para conseguir una velocidad menor y un mayor nivel de seguridad, elija la opción **Grupo 5**. El Grupo 1 está seleccionado de manera predeterminada.
- **Cifrado, fase 1/fase 2**: método de cifrado para esta fase, que puede ser DES, 3DES, AES-128, AES-192 o AES-256. El método determina la longitud de la clave usada para cifrar o descifrar los paquetes ESP. Se recomienda usar AES-256 porque es más seguro.

- **Autenticación, fase 1/fase 2**: método de autenticación para esta fase, que puede ser MD5 o SHA1. El método de autenticación determina la forma en que se validan los paquetes de encabezado ESP (Encapsulating Security Payload, carga de seguridad encapsulada). MD5 es un algoritmo de hash unidireccional que produce un resumen de 128 bits. SHA1 es un algoritmo de hash unidireccional que produce un resumen de 160 bits. Se recomienda usar SHA1 porque es más seguro. Los dos extremos del túnel VPN deben utilizar el mismo método de autenticación.
- **Vigencia de SA, fase 1/fase 2:** tiempo durante el cual un túnel VPN está activo en esta fase. El valor predeterminado para la fase 1 es de 28800 segundos. El valor predeterminado para la fase 2 es de 3600 segundos.
- **Seguridad perfecta hacia delante**: cuando se habilita PFS (Perfect Forward Secrecy, seguridad perfecta hacia delante), la negociación de IKE de fase 2 generará un nuevo material de clave para el cifrado y la autenticación del tráfico de IP, de forma que los hackers que utilicen la fuerza bruta para romper las claves de cifrado no puedan obtener las claves IPsec futuras. Si desea habilitar esta función, active la casilla; en caso contrario, desactívela. Se recomienda utilizar esta función.
- **Complejidad de clave precompartida mínima**: active la opción **Habilitar** para activar el Medidor de seguridad de clave precompartida.
- **Clave precompartida**: clave precompartida que se debe usar para autenticar el par IKE remoto. Se pueden especificar hasta 30 caracteres del teclado o valores hexadecimales, por ejemplo, Mi_@123 o 4d795f40313233. Ambos extremos del túnel VPN deben usar la misma clave precompartida. Se recomienda cambiar la clave precompartida de forma periódica para maximizar la seguridad de la VPN.
- **Medidor de seguridad de clave precompartida**: al habilitar la opción Complejidad de clave precompartida mínima, este medidor indica el nivel de seguridad de la clave precompartida. Al especificar una clave precompartida, aparecen barras de colores. La escala de colores va desde el rojo (débil) hasta el verde (segura) pasando por el amarillo (aceptable).

**SUGERENCIA** Especifique una clave precompartida compleja que tenga más de ocho caracteres, letras en mayúscula y minúscula, números y símbolos como -*^+= (los caracteres ' ' " \ no se pueden utilizar).

## Ajustes avanzados para IKE con clave precompartida e IKE con certificado

Para la mayoría de los usuarios, los ajustes básicos son suficientes. Sin embargo, los usuarios avanzados pueden hacer clic en **Avanzado** para mostrar los ajustes avanzados. Si cambia los ajustes avanzados en un router, también deberá cambiarlos en el otro router.

- **Modo agresivo**: se pueden aplicar dos modos de negociación SA de IKE, que son el Modo principal y el Modo agresivo. Si la seguridad de la red es el aspecto prioritario, se recomienda aplicar el Modo principal. Si la velocidad de la red es el aspecto prioritario, se recomienda aplicar el Modo agresivo. Active esta casilla para habilitar el Modo agresivo o déjela desactivada si desea usar el Modo principal.
  Si el **Tipo de gateway de seguridad remota** es uno de los tipos de *IP dinámica*, hay que utilizar el Modo agresivo. La casilla está activada automáticamente. Este ajuste no se puede cambiar.
- **Comprimir (compatible con el protocolo de compresión de carga útil de IP [IPComp])**: un protocolo que reduce el tamaño de los datagramas IP. Active la casilla para que el router pueda proponer la compresión al iniciar una conexión. Si el retransmisor rechaza esta propuesta, el router no aplicará la compresión. Cuando el router es el retransmisor, acepta la compresión, incluso si esta no está habilitada. Si habilita esta función para este router, también tendrá que habilitarla en el router en el otro extremo del túnel.
- **Mantener activo**: intenta restablecer la conexión VPN en caso de que se produzca alguna interrupción.
- **Algoritmo de hash de AH**: el protocolo AH (Authentication Header, encabezado de autenticación) describe el formato del paquete y los estándares predeterminados para la estructura del paquete. Cuando AH es el protocolo de seguridad, la protección se extiende al encabezado IP para comprobar la integridad de todo el paquete. Active la casilla para usar esta función y seleccionar un método de autenticación: MD5 o SHA1. MD5 genera un resumen de 128 bits para autenticar los datos del paquete. SHA1 genera un resumen de 160 bits para autenticar los datos del paquete. Ambos extremos del túnel deben usar el mismo algoritmo.

- **Difusión de NetBIOS**: difunde los mensajes utilizados para la resolución de nombres en las redes Windows para identificar los recursos, por ejemplo, equipos, impresoras y servidores de archivos. Estos mensajes los utilizan algunas aplicaciones de software y funciones de Windows, por ejemplo, el Entorno de red. El tráfico de difusión LAN normalmente no se reenvía a través de un túnel VPN. Sin embargo, se puede activar esta casilla para permitir que las difusiones de NetBIOS procedentes de un extremo del túnel se difundan de nuevo hasta el otro extremo.
- **NAT Traversal**: NAT (Network Address Translation, conversión de direcciones de red) permite a los usuarios que tengan direcciones de LAN privadas acceder a los recursos de Internet utilizando una dirección IP públicamente enrutable como dirección de origen. Sin embargo, para el tráfico entrante, la gateway de NAT no tiene un método automático para convertir la dirección IP pública a un destino concreto de la LAN privada. Este problema impide que se realicen correctamente los intercambios de IPsec. Si el router VPN está detrás de una gateway de NAT, active esta casilla para habilitar la opción NAT Traversal. Hay que utilizar el mismo ajuste en los dos extremos del túnel.
- **Intervalo de detección de par inactivo**: método para detectar un par inactivo de intercambio de claves por red (IKE, Internet Key Exchange). El método usa patrones de tráfico de IPsec para minimizar la cantidad de mensajes. El intervalo de control mínimo en la Detección de pares inactivos de VPN es de 10 segundos.
- **Autenticación ampliada**: permite especificar un nombre de usuario y una contraseña para autenticar las solicitudes de túnel IPSec entrantes, además de una clave precompartida o un certificado.
  - **Host IPsec**: indica que se use un **host IPsec** para la autenticación ampliada.
    **Nombre de usuario**: nombre de usuario para la autenticación.
    **Contraseña**: contraseña de autenticación.
  - **Dispositivo perimetral**: proporciona una dirección IP para el solicitante del túnel entrante (después de la autenticación) a partir del rango de IP virtual configurado en la ventana **Resumen**. En el menú desplegable, seleccione el dispositivo. Para agregar o editar el dominio del dispositivo, haga clic en **Agregar/Editar** para mostrar la ventana **Administración de usuarios**.
- **Modo de configuración**: proporciona una dirección IP para el solicitante del túnel entrante (después de la autenticación) a partir del rango de IP virtual configurado en la ventana VPN > **Resumen**.

# FlexVPN (spoke)

FlexVPN utiliza IKEv2 basado en estándares abiertos como tecnología de seguridad y ofrece altos niveles de seguridad. FlexVPN se creó para simplificar la implementación de VPN y abordar la complejidad de usar varias soluciones. Dado que es un ecosistema unificado, abarca todos los tipos de VPN: acceso remoto, trabajador remoto, sitio a sitio, movilidad, servicios de seguridad administrada, etc.

**Añadir un nuevo túnel FlexVPN**

Para añadir un túnel nuevo, configure lo siguiente:

- **Nombre del túnel**: escriba un nombre para el túnel FlexVPN.
- **Interfaz**: seleccione el puerto WAN que usará para este túnel de la lista desplegable.
- **Habilitar**: seleccione esta opción para habilitar el túnel o anule la selección para deshabilitarlo. De manera predeterminada, el túnel FlexVPN está habilitado.

**Configuración de spoke**

Introduzca los ajustes de Configuración de spoke para este router:

- **Tipo de gateway de seguridad de spoke**: seleccione una opción para identificar el router a fin de establecer el túnel FlexVPN de la lista desplegable.
  - **IP solamente**: este router tiene una dirección IP de WAN estática. La dirección IP de WAN aparece automáticamente.
  - **IP + autenticación de nombre de dominio (FQDN)**: este dispositivo tiene una dirección IP estática y un nombre de dominio registrado, como MiServidor.MiDominio.com. También debe escribir el **Nombre de dominio** que se usará para la autenticación. El nombre de dominio puede usarse solamente para una conexión de túnel.
  - **IP + autenticación de dirección de correo electrónico (USER FQDN)**: este dispositivo tiene una dirección IP estática y se usa una dirección de correo electrónico para la autenticación. La dirección IP de WAN aparece automáticamente. Escriba la **Dirección de correo electrónico** que se usará para la autenticación.

- **IP dinámica + autenticación de nombre de dominio (FQDN)**: este router tiene una dirección IP dinámica y un nombre de host de DNS dinámico registrado (disponible de proveedores como DynDNS.com). Escriba un **Nombre de dominio** que se usará para la autenticación. El nombre de dominio puede usarse solamente para una conexión de túnel.

- **IP dinámica + autenticación de dirección de correo electrónico (USER FQDN)**: este router tiene una dirección IP dinámica y no tiene un nombre de host de DNS dinámico. Escriba una **Dirección de correo electrónico** que se usará para la autenticación.
- **Nombre de dominio**: escriba un nombre de dominio.
- **Dirección IP de GRE**: dirección IP de la interfaz virtual (GRE).
- **Obtener del hub**: el hub asigna la dirección IP de GRE.
- **Configurar de manera estática**: configuración manual de la dirección IP de GRE.
- **Complejidad mínima de clave previamente compartida**: seleccione la casilla **Habilitar** para habilitar el Medidor de seguridad de clave previamente compartida.
- **Clave previamente compartida**: clave previamente compartida usada para autenticar el IKE de spoke. Puede escribir hasta 30 caracteres del teclado o valores hexadecimales, como Mi_@123 o 4d795f40313233 (no se admiten ' ' " \). Ambos extremos del túnel FlexVPN deben usar la misma clave previamente compartida. Se recomienda encarecidamente cambiar la clave previamente compartida de manera periódica para aumentar al máximo la seguridad de FlexVPN.
- **Medidor de seguridad de la clave previamente compartida**: cuando se habilita la Complejidad mínima de clave previamente compartida, este medidor indica la seguridad de la clave previamente compartida. A medida que escribe la clave previamente compartida, aparecen barras de colores. La escala varía entre rojo (débil), amarillo (aceptable) y verde (segura).

**Red spoke**

La opción Red spoke permite que todos los dispositivos de la red spoke usen el túnel FlexVPN. Para añadir una nueva red spoke, haga clic en **Añadir** y escriba la dirección IP de subred y la máscara de subred.

**Configuración de hub**

Introduzca los ajustes de Configuración de hub para este router:

- **Tipo de gateway de seguridad del hub**: es el método para identificar el router a fin de establecer el túnel FlexVPN. Seleccione una de las siguientes opciones:
  - **IP solamente**: dirección IP de WAN estática. Si conoce la dirección IP del hub, seleccione **Dirección IP** y escríbala. Si no conoce la dirección IP del hub, seleccione **IP mediante resolución de DNS** y escriba el nombre de dominio del router. Un router de Cisco puede obtener la dirección IP del hub mediante la resolución de DNS.
  - **IP + autenticación de nombre de dominio (FQDN)**: este router tiene una dirección IP estática y un nombre de dominio registrado, como MiServidor. MiDominio.com. Si conoce la dirección IP del hub, seleccione **Dirección IP** y escríbala. Si no conoce la dirección IP del hub, seleccione **IP mediante resolución de DNS** y escriba el nombre de dominio del router. Los routers de Cisco pueden obtener la dirección IP del hub mediante la resolución de DNS.
  - **IP + autenticación de dirección de correo electrónico (USER FQDN)**: este router tiene una dirección IP estática y se usa una dirección de correo electrónico para la autenticación. Si conoce la dirección IP del hub, seleccione **Dirección IP** y escríbala. Si no conoce la dirección IP del hub, seleccione **IP mediante resolución de DNS** y escriba el nombre real de dominio del router. Los routers de Cisco pueden obtener la dirección IP del hub mediante la resolución de DNS.
- **Complejidad mínima de clave previamente compartida**: seleccione **Habilitar** para habilitar el Medidor de seguridad de clave previamente compartida.
- **Clave previamente compartida**: clave previamente compartida usada para autenticar el IKE del hub. Puede escribir hasta 30 caracteres del teclado o valores hexadecimales, como Mi_@123 o 4d795f40313233 (no se admiten ' ' " \). Ambos extremos del túnel FlexVPN deben usar la misma clave previamente compartida. Se recomienda encarecidamente cambiar la clave previamente compartida de manera periódica para aumentar al máximo la seguridad de FlexVPN.
- **Medidor de seguridad de la clave previamente compartida**: cuando se habilita la Complejidad mínima de clave previamente compartida, este medidor indica la seguridad de la clave previamente compartida. A medida que escribe la clave previamente compartida, aparecen barras de colores. La escala varía entre rojo (débil), amarillo (aceptable) y verde (segura).

### Configuración de IPsec

Para que la encriptación tenga éxito, los dos extremos del túnel FlexVPN deben acordar los métodos de encriptación, desencriptación y autenticación. Escriba exactamente los mismos datos en ambos routers.

Escriba los datos para la Fase 1 y la Fase 2. La Fase 1 establece las claves previamente compartidas para crear un canal seguro de comunicación autenticada. En la Fase 2, los pares de IKE usan el canal seguro para negociar las asociaciones de seguridad en nombre de otros servicios, como IPsec. Asegúrese de escribir los mismos datos cuando configure otro router para este túnel.

- **Grupo DH de Fase 1 y Fase 2**: DH (Diffie-Hellman) es un protocolo de intercambio de claves. Hay tres grupos diferentes de longitudes de clave principales: el grupo 1 (768 bits), el grupo 2 (1024 bits) y el grupo 5 (1536 bits).
  Si busca más velocidad y menos seguridad, escoja el **Grupo 1**. Si busca menos velocidad y más seguridad, escoja el Grupo 5. El Grupo 2 está seleccionado de forma predeterminada.
- **Encriptación de Fase 1 y Fase 2**: el método de encriptación para esta fase. Puede ser DES, 3DES, AES-128, AES-192 o AES-256. El método determina la longitud de la clave que se usa para encriptar o desencriptar paquetes ESP. Se recomienda AES-256 porque es más seguro.
- **Autenticación de Fase 1 y Fase 2**: el método de autenticación para esta fase. Puede ser MD5 o SHA1. El método de autenticación determina cómo se validan los paquetes de encabezado de ESP (protocolo de carga útil de seguridad de encapsulamiento). MD5 es un algoritmo de hash unidireccional que produce una síntesis de 128 bits. SHA1 es un algoritmo de hash unidireccional que produce una síntesis de 160 bits. Se recomienda SHA1 porque es más seguro. Asegúrese de que ambos extremos del túnel VPN usen el mismo método de autenticación.
- **Duración de SA de Fase 1 y Fase 2**: el tiempo que permanece activo un túnel VPN en esta fase. El valor predeterminado para la Fase 1 es de 28 800 segundos. El valor predeterminado para la Fase 2 es de 3600 segundos.

### Configuración avanzada

Para la mayoría de los usuarios, es suficiente con la configuración básica. Si decide modificar la configuración avanzada de un router, también hágalo en el otro.

- **Mantener conexión**: intenta restablecer la conexión VPN si se interrumpe.

- **Detección de par inactivo (DPD)**: envía mensajes HELLO/ACK periódicos para comprobar el estado del túnel FlexVPN. Es posible especificar el intervalo entre los mensajes HELLO/ACK en el campo **Intervalo**.
- **Respaldo de túnel**: cuando la DPD determina que el par remoto no está disponible, esta función habilita el router para restablecer el túnel FlexVPN usando una dirección IP alternativa para el par remoto o una interfaz WAN local alternativa. Seleccione la casilla para habilitar esta función e introduzca los siguientes ajustes. Esta función está disponible solamente si se habilita la Detección de pares inactivos.
  - **Dirección IP de hub**: dirección IP alternativa para el par remoto; otra opción es volver a escribir la dirección IP de WAN que ya se definió para el gateway remoto.
  - **Interfaz de spoke**: interfaz WAN que se usa para restablecer la conexión.
  - **Tiempo de espera para el túnel de respaldo de VPN**: cuando el router se inicia y el túnel principal no se conecta después de transcurrido este tiempo, se usa el túnel de respaldo. El tiempo de espera predeterminado es de 30 segundos

# Paso a través de VPN

Paso a través de VPN permite a los clientes de VPN pasar a través de este router y conectarse a un punto de terminación de la VPN. Esta opción está habilitada de forma predeterminada.

Para habilitar la función Paso a través de VPN, active la opción **Habilitar** para los protocolos permitidos:

- **IPSec Passthrough**: IPSec (Internet Protocol Security, seguridad del protocolo Internet) es un conjunto de protocolos utilizados para implementar el intercambio seguro de paquetes en la capa IP.
- **PPTP Passthrough**: el protocolo PPTP (Point-to-Point Tunneling Protocol, protocolo de tunelización punto a punto) permite tunelizar el protocolo PPP (Point-to-Point Protocol, protocolo punto a punto) a través de una red IP.
- **L2TP Passthrough**: L2TP (Layer 2 Tunneling Protocol, protocolo de tunelización de capa 2) es el método utilizado para habilitar las sesiones punto a punto utilizando Internet en la capa 2.

# Servidor PPTP

Se pueden habilitar hasta 10 túneles de VPN de PPTP (Point-to-Point Tunneling Protocol, protocolo de tunelización de punto a punto) para los usuarios que ejecuten el software cliente de PPTP. Por ejemplo, en Windows XP o 2000, un usuario abre el panel Conexiones de red para crear una nueva conexión. En el asistente, el usuario selecciona la opción para crear una conexión con el lugar de trabajo usando una conexión de red privada virtual. El usuario debe conocer la dirección IP de WAN de este dispositivo. Para obtener más información, consulte la documentación o los archivos de ayuda del sistema operativo.

Para habilitar el servidor PPTP y permitir los túneles VPN de PPTP, active la casilla **Habilitar** y especifique el rango:

**Inicio de rango** y **Fin de rango**: rango de direcciones de LAN que se debe asignar a los clientes de VPN de PPTP. El rango de direcciones IP de la LAN para los clientes de VPN de PPTP debe estar fuera del rango de DHCP normal del router.

La opción **Estado del túnel PPTP** permite ver la cantidad de **Túneles usados** y de **Túneles disponibles.**

La **Tabla de conexiones** muestra los túneles que están en uso.

# 10

# OpenVPN

OpenVPN es una técnica de red privada virtual (VPN) para crear conexiones seguras entre puntos o sitios en configuraciones de routing o puente e instalaciones de acceso remoto. Usa un protocolo de seguridad personalizado que utiliza SSL/TLS para el intercambio de claves.

OpenVPN les permite a los pares autenticarse entre sí usando certificados o un nombre de usuario y una contraseña. Cuando se utiliza en una configuración de múltiples clientes a servidor, permite que el servidor envíe un certificado de autenticación para cada cliente usando la autoridad de firma y certificado.

## Resumen

Esta función permite ver información general sobre la configuración del túnel OpenVPN. El dispositivo admite hasta 50 cuentas OpenVPN.

El campo **Número de túnel de OpenVPN** permite ver la cantidad de **Túneles usados**, **Túneles disponibles**, **Túneles habilitados** y **Túneles definidos**.

**Tabla de configuración del servidor**

La Tabla de configuración del servidor permite ver las entradas creadas en **OpenVPN** > **OpenVPN Servidor**.

- **Habilitar**: seleccione esta casilla para habilitar el servidor OpenVPN o anule la selección para deshabilitarla.
- **Autenticación**: contraseña o contraseña + certificado.
- **Protocolo**: protocolo requerido y número de puerto.
- **Encriptación**: el método de encriptación para esta fase. Puede ser NULL, DES, 3DES, AES128, AES-192 o AES-256. El método determina la longitud de la clave que se usa para encriptar o desencriptar paquetes.
- **Grupo de direcciones del cliente**: proporciona la dirección IP del cliente de este grupo.

## Servidor OpenVPN

**Estado de identificación de cuenta de OpenVPN**

La Tabla de configuración de la identificación de cuenta permite ver las entradas creadas en **OpenVPN** > **Cuenta OpenVPN.** Haga clic en **Añadir** para agregar una cuenta OpenVPN.

- **Habilitar**: seleccione esta casilla para habilitar una cuenta OpenVPN existente o anule la selección para deshabilitarla.

Especifique administradores para añadir o modificar la configuración del servidor OpenVPN.

Para añadir un servidor OpenVPN, introduzca los siguientes ajustes y haga clic en **Guardar**.

**Configuración básica**

- **Habilitar**: seleccione esta casilla para habilitar el servidor OpenVPN o anule la selección para deshabilitarla.

# Cuenta OpenVPN

Especifique administradores para añadir o modificar los usuarios del cliente OpenVPN.

Para añadir una cuenta OpenVPN, introduzca los siguientes ajustes y haga clic en **Guardar**.

- **Habilitar**: seleccione esta casilla para habilitar la cuenta OpenVPN o anule la selección para deshabilitarla.
- **Autenticación**: la contraseña.
- **Servidor OpenVPN**: nombre o dirección IP del servidor OpenVPN.
- **Nombre de usuario**: nombre de usuario del cliente OpenVPN.
- **Contraseña**: contraseña del cliente OpenVPN.

# 11

# Administración de certificados

Un certificado digital certifica que una clave pública es propiedad del firmante del certificado. Esto permite que los demás (partes que confían) puedan confiar en las firmas o en las afirmaciones efectuadas mediante la clave privada correspondiente a la clave pública certificada. Mediante este modelo de relaciones de confianza, una CA (Certificate Authority, autoridad de certificación) es un tercero de confianza en el que confían tanto el firmante (propietario) del certificado como la parte que confía en el certificado. Las CA están presentes en muchos esquemas PKI (Public Key Infrastructure, infraestructura de clave pública).

La función Administración de certificados se utiliza para generar e instalar certificados SSL.

## Mi certificado

Se pueden agregar hasta 50 certificados autofirmados o autorizados por terceros. También se pueden crear certificados usando el **Generador de certificados** o importarlos desde un equipo o un dispositivo USB.

Los navegadores no confían de forma inherente en los certificados SSL autofirmados. Aunque estos certificados se pueden usar para el cifrado, es posible que los navegadores muestren mensajes de advertencia en los que se indica al usuario que el certificado en cuestión no lo ha emitido ninguna entidad en la que el usuario haya decidido confiar.

Los usuarios también pueden conectarse sin tener un certificado instalado en el equipo. El usuario ve una advertencia de seguridad cuando se conecta al túnel VPN, pero puede continuar sin esta medida adicional de protección.

Para configurar un certificado como el principal, haga clic en el botón de opción del certificado que desee y haga clic en **Seleccionar como certificado principal**.

Para mostrar la información del certificado, haga clic en el icono **Detalles**.

### Procedimiento para exportar o mostrar un certificado o una clave privada

El certificado de cliente permite al cliente conectarse a la VPN. Para exportar o mostrar un certificado o una clave privada:

**PASO 1** Haga clic en el icono que proceda: **Exportar certificado para el cliente**, **Exportar certificado para el administrador** o **Exportar clave privada**. Aparece la ventana Descarga de archivo.

**Exportar certificado para el cliente**: certificado de cliente que le permite conectarse a la VPN.

**Exportar certificado para el administrador**: contiene la clave privada y se puede exportar una copia para que actúe como archivo de copia de seguridad. Por ejemplo, antes de restablecer el dispositivo a los ajustes predeterminados, puede exportar el certificado. Después de reiniciar el dispositivo, importe este archivo para restaurar el certificado.

**Exportar clave privada**: determinadas aplicaciones de software de cliente de VPN requieren una credencial con una clave privada, un certificado de CA y un certificado por separado.

**PASO 2** Haga clic en **Abrir** para mostrar la clave. Haga clic en **Guardar** para guardar la clave.

### Importación de un certificado autofirmado o de terceros

Una CSR (Certificate Signing Request, solicitud de firma de certificado) que se genere externamente no se puede autorizar ni firmar. Para agregar una CSR externa, hay que usar una **Autorización de CSR**.

Para importar un certificado:

**PASO 1** Haga clic en **Agregar**.

**PASO 2** Seleccione **Autorizado por terceros** o **Autofirmado**.

**PASO 3** Seleccione **Importar de PC** o **Importar de dispositivo USB**.

**PASO 4** Busque el **certificado de la autoridad de certificación** (solo terceros).

**PASO 5** Busque el **certificado y la clave privada** (terceros o autofirmados).

**PASO 6** Haga clic en **Guardar**.

# .Certificado IPSec de confianza

IPSec se utiliza en el intercambio de generación de claves y datos de autenticación, así como en el protocolo de establecimiento de claves, el algoritmo de cifrado o el mecanismo de validación y autenticación segura de las transacciones en línea con certificados SSL.

Para mostrar la información del certificado, haga clic en el icono **Detalles**.

Para exportar o mostrar un certificado, haga clic en el icono **Exportar certificado**. Se muestra una ventana emergente en la que puede **abrir** el certificado para inspeccionarlo o bien **guardarlo** en un equipo.

Para importar un certificado de terceros, haga clic en **Agregar** e importe el certificado:

**PASO 1** Seleccione el **certificado de la autoridad de certificación**.

**PASO 2** Seleccione **Importar de PC** o **Importar de dispositivo USB**.

**PASO 3** Busque el **certificado** (terceros o autofirmado).

**PASO 4** Haga clic en **Guardar**.

# Certificado de OpenVPN

Admite los métodos de autenticación de OpenVPN en función de los certificados.

Para abrir esta página, seleccione **Administración de certificados > Certificado de OpenVPN** en el árbol de navegación.

Para mostrar la información del certificado, haga clic en el icono **Detalles**.

Para crear el nuevo certificado para el servidor de OpenVPN o el cliente de OpenVPN, haga clic en **Agregar** y pase a la página **Administración de certificados > Generador de certificados**.

# Generador de certificados

El Generador de solicitudes de certificados recopila información y genera un archivo de clave privada y una solicitud de certificado. Puede elegir generar un certificado con firma automática o una Solicitud de firma de certificado (CSR) para que firme una autoridad certificadora externa. También puede elegir generar un certificado para el servidor de OpenVPN o el cliente de OpenVPN. Cuando la configuración se guarda, la CSR o el certificado con firma automática generados se muestran debajo de **Mi certificado**, el certificado para el servidor de OpenVPN o el cliente de OpenVPN se muestra debajo del certificado de OpenVPN.

Para generar un certificado:

**PASO 1** Ingrese los siguientes parámetros:

- **Tipo**: tipo de solicitud de certificado.
- **Nombre del país**: país de origen.
- **Nombre del estado o la provincia**: estado o provincia (opcional).
- **Nombre de la localidad**: municipalidad (opcional).
- **Nombre de la organización**: organización (opcional).
- **Nombre de la unidad organizacional**: subconjunto de la organización.
- **Nombre común**: nombre común de la organización.
- **Dirección de correo electrónico**: dirección de correo electrónico de contacto (opcional).
- **Longitud de la clave de cifrado**: longitud de la clave.
- **Duración válida**: cantidad de días que el certificado tiene validez.
- **Autoridad de certificación raíz**: elija una de las autoridades de certificación raíz para crear el certificado para el servidor de OpenVPN o el cliente de OpenVPN.

**PASO 2** Haga clic en **Guardar**. Aparecerá la ventana **Mi certificado** o Certificado de OpenVPN.

# Autorización de CSR

Una CSR es un certificado de identidad digital generado mediante un generador de certificados. Un certificado no está completo hasta que lo firma una CA. Este dispositivo puede funcionar como una CA para firmar o autorizar una CSR que se haya generado externamente mediante la opción Administración de certificados > Autorización de CSR. Una vez que este dispositivo firma una CSR generada externamente, la CSR firmada se convierte en un certificado de confianza y se muestra en la ventana **.Certificado IPSec de confianza**. Para restaurar la configuración predeterminada del dispositivo, incluidos los certificados predeterminados, use la ventana **Ajustes predeterminados**.

Para firmar un certificado:

**PASO 1** Haga clic en **Explorar** para identificar la CSR.

**PASO 2** Para seleccionar la clave privada correspondiente para autorizar y firmar la CSR, seleccione el certificado para asociarlo con la solicitud mediante el menú desplegable **Mi certificado**.

**PASO 3** Haga clic en **Guardar**.

# 12

# Registro

Los registros reflejan el estado del sistema, ya sea utilizando traps o de forma periódica.

## Registro del sistema

Permite configurar alertas y registros de SMS (Short Message Service, servicio de mensajes cortos).

**Configuración de la función de envío de SMS del registro del sistema**

Para configurar el enlace para el registro, lleve a cabo los siguientes pasos:

**PASO 1** Haga clic en **Habilitar**.

**PASO 2** Seleccione **USB1** o **USB2** para enviar el registro a través de los puertos USB.

**PASO 3** Seleccione la opción **Número de marcado 1**, **Número de marcado 2** (o las dos opciones) y especifique el número de teléfono al que desee llamar.

**PASO 4** Haga clic en **Prueba** para probar el enlace.

**PASO 5** Especifique cuándo se debe enviar el registro:

- Cuando se active un enlace.
- Cuando se desactive un enlace.
- Cuando se produzca un error en la autenticación.
- Cuando se reinicie el sistema.

**PASO 6** Haga clic en **Guardar**.

### Configuración de los servidores del registro del sistema

Para habilitar un servidor, haga clic en **Habilitar** y escriba un nombre en el campo **Servidor Syslog**.

### Configuración de las notificaciones por correo electrónico

Para configurar las notificaciones por correo electrónico, active la opción **Habilitar** y cumplimente la siguiente información:

- **Servidor de correo**: nombre o dirección IP del servidor de correo.
- **Autenticación**: tipo de autenticación para iniciar sesión en un servidor de correo.
  - **Ninguno**: no se exige ninguna autenticación.
  - **Inicio de sesión sencillo**: autenticación en formato sin cifrar.
  - **TLS**: protocolo de autenticación de conexión segura (por ejemplo, Gmail utiliza la opción de autenticación TLS en el puerto 587).
  - **SSL**: protocolo de autenticación de conexión segura (por ejemplo, Gmail utiliza la opción de autenticación SSL en el puerto 465).
- **Puerto SMTP**: número del puerto SMTP (Simple Mail Transfer Protocol, protocolo simple de transferencia de correo).
- **Nombre de usuario**: nombre del usuario del correo electrónico. Por ejemplo:
  Servidor de correo: smtp.gmail.com
  Autenticación: SSL
  Puerto SMTP: 465
  Nombre de usuario: xxxxx@gmail.com
  Contraseña: yyyyyy
- **Contraseña**: contraseña del correo electrónico.
- **Enviar correo electrónico a 1** y (opcional) **2**: dirección de correo electrónico. Por ejemplo, Enviar correo electrónico a: `zzz@empresa.com`.
- **Longitud de la cola de registro**: número de entradas de registro que se deben crear antes de enviar una notificación. Por ejemplo, *10* entradas.
- **Umbral de tiempo de registro**: tiempo que debe transcurrir entre las notificaciones del registro. Por ejemplo, *10* minutos.

- **Alerta de tiempo real**: evento que desencadena una notificación inmediata.
- **Alerta por correo electrónico cuando se acceda a contenido bloqueado/filtrado**: correo electrónico de alerta que se envía cuando se intenta acceder un dispositivo que está bloqueado o filtrado.
- **Alerta por correo electrónico de ataque de hacker**: correo electrónico de alerta que se envía cuando un hacker intenta obtener acceso mediante un ataque DoS (Denial-Of-Service, denegación de servicio).

Para enviar el registro por correo electrónico de forma inmediata, haga clic en **Enviar registro ahora**.

**Configuración de los registros**

Seleccione qué eventos se deben producir para que se generen entradas en el registro:

- **Desbordamiento de Syn**: la velocidad con la que se reciben solicitudes de conexiones TCP es superior a la capacidad del dispositivo para procesarlas.
- **Simulación de IP**: paquetes IP con direcciones IP de origen aparentemente falsificadas que se envían con el propósito de ocultar la identidad del emisor o suplantar la identidad de otro sistema informático.
- **Intento de inicio de sesión no autorizado**: se ha rechazado el intento para iniciar sesión en la red.
- **Ping de la muerte**: detección de un ping malintencionado o con una estructura incorrecta que se ha enviado a un equipo. Un ping tiene normalmente 32 bytes de tamaño (u 84 bytes si tenemos en cuenta el encabezado del protocolo de Internet [IP]). Tradicionalmente, muchos sistemas informáticos no admitían un paquete de ping con un tamaño superior al tamaño del paquete IPv4 máximo (65 535 bytes). El hecho de enviar un ping de un tamaño más grande podía generar un error en el equipo de destino.
- **Win Nuke**: ataque de denegación de servicio remoto que afecta a los sistemas operativos Microsoft Windows 95, Microsoft Windows NT y Microsoft Windows 3.1x.
- **Directivas de denegación**: acceso denegado en función de las directivas configuradas.
- **Inicio de sesión autorizado**: un usuario autorizado ha iniciado sesión en la red.

- **Mensajes de error del sistema**: se han registrado mensajes de error del sistema.
- **Directivas de permiso**: un usuario autorizado ha iniciado sesión en la red haciendo uso de las directivas configuradas.
- **Kernel**: todos los mensajes del kernel del sistema.
- **Cambios de configuración**: ocasiones en las que se ha modificado la configuración del dispositivo.
- **IPSec y VPN de PPTP**: estado de desconexión, conexión y negociación del túnel VPN.
- **VPN SSL**: estado de desconexión, conexión y negociación del túnel VPN SSL.
- **Red**: indica si las interfaces WAN o DMZ están conectadas o desconectadas.

**Información adicional (botones de registro)**

Si el navegador web muestra una advertencia sobre la ventana emergente, indique que se permita el contenido bloqueado. Haga clic en **Actualizar** para actualizar los datos.

Haga clic en los siguientes botones para ver más información:

- **Ver registro del sistema**: muestra el **registro del sistema**. Para especificar un registro, seleccione el filtro en el menú desplegable.

  Las entradas del registro incluyen la fecha y la hora del evento, el tipo de evento y un mensaje. El mensaje especifica el tipo de directiva, por ejemplo, una regla de acceso, la dirección IP de la LAN del origen (SRC) y la dirección MAC.
- **Tabla de registro de salida**: información de paquetes salientes.
- **Tabla de registro entrante**: información de paquetes entrantes.
- **Borrar registro ahora**: haga clic en esta opción para borrar el registro sin enviarlo por correo electrónico únicamente si no desea volver a ver la información en el futuro.

# Estadísticas del sistema

Se muestra información detallada acerca de los puertos y los dispositivos conectados.

# Procesos

Se muestra información detallada acerca de los procesos en ejecución.

# 13

# Administración de usuarios

La página Administración de usuarios permite controlar el acceso de los usuarios y los dominios. Se usa principalmente para PPTP, el cliente Cisco VPN (también conocido como EasyVPN).

Para agregar o modificar un dominio:

**PASO 1** Haga clic en **Agregar** (o seleccione una entrada y haga clic en **Editar**).

**PASO 2** Elija un valor en **Tipo de autenticación** y especifique la información necesaria:

- **Local Data Base** (Base de datos local): permite autenticarse en una base de datos local.
  - **Dominio**: el nombre de dominio que los usuarios seleccionan para iniciar sesión.
- **Radius (PAP, CHAP, MSCHAP, MSCHAPv2)**: permite autenticarse en un servidor RADIUS utilizando los protocolos PAP (Password Authentication Protocol, protocolo de autenticación de contraseña), CHAP (Challenge Handshake Authentication Protocol, protocolo de autenticación por desafío mutuo), MSCHAP (Microsoft Challenge Handshake Authentication Protocol, protocolo de autenticación por desafío mutuo de Microsoft) o MSCHAPv2, (Microsoft Challenge Handshake Authentication Protocol Version 2, protocolo de autenticación por desafío mutuo de Microsoft, versión 2).
  - **Dominio**: el nombre de dominio que los usuarios seleccionan para iniciar sesión.
  - **Servidor Radius**: dirección IP del servidor RADIUS.
  - **Contraseña de Radius**: *secreto* de autenticación.

- Active Directory: autenticación de Windows Active Directory. Tenga en cuenta que la autenticación de Active Directory es la más propensa a errores. Si no puede autenticarse usando Active Directory, consulte el procedimiento de solución de problemas que figura al final de esta sección.
  - **Dominio**: el nombre de dominio que los usuarios seleccionan para iniciar sesión.
  - **Dirección de servidor AD**: dirección IPv4 del servidor de Active Directory.
  - **Nombre de dominio AD**: nombre de dominio del servidor de Active Directory.
- **LDAP**: Lightweight Directory Access Protocol, protocolo ligero de acceso al directorio.
  - **Dominio**: el nombre de dominio que los usuarios seleccionan para iniciar sesión.
  - **Dirección de servidor LDAP**: dirección IPv4 del servidor LDAP.
  - **Nombre de DN base de LDAP**: base de búsqueda para las consultas LDAP. Un ejemplo de cadena de base de búsqueda es `CN=Users,DC=yourdomain,DC=com`.

**PASO 3** Haga clic en **Aceptar**.

---

Para agregar o modificar un usuario, haga clic en **Agregar** (o seleccione una entrada y haga clic en **Editar**) y especifique la siguiente información:

- **Nombre de usuario**: nombre que utiliza el usuario para iniciar sesión en el portal de VPN SSL.
- **Contraseña**: contraseña que se utiliza para la autenticación.
- **Grupo**: El grupo Unassigned (Sin asignar) contiene usuarios de VPN PPTP y de EasyVPN. El grupo Administrador tiene solo un usuario. El nombre de usuario predeterminado del grupo Administrador es **cisco**.
- **Dominio**: nombre del dominio incluido en la Tabla de administración de dominios.

# 14

# Filtrado web

El filtrado web puede brindarle protección contra el acceso a sitios web inadecuados basada en el mecanismo de operación que se describe a continuación. Esta característica solo se encuentra disponible en los modelos RV320-WB y RV325-WB.

**STEP 1** Si la URL entrante está en la **Lista de exclusión** y el valor del índice de **Reputación web** no es inferior a 40, la URL es segura y está permitida. Viceversa.

**STEP 2** Si la URL entrante no está en la **Lista de exclusión**, verifique si se encuentra en la **Lista de bloqueo**. Si está en la **Lista de bloqueo**, la URL está bloqueada. Si no está en la **Lista de bloqueo**, verifique si se encuentra en la **Lista blanca**.

**STEP 3** Si la URL entrante está incluida en la **Lista blanca**, la URL está permitida. Si no lo está, verifique la categoría web.

**STEP 4** Si la URL pertenece a los elementos seleccionados de la categoría, está bloqueada. Si no lo hace, verifique la **Reputación web**.

**STEP 5** Si el valor del índice de reputación no es inferior a 40, está permitida. Viceversa.

**Filtrado web:** para aplicar siempre el filtrado web, haga clic en **Always On** (Siempre activado). Para aplicar el filtrado web de acuerdo con programaciones, haga clic en **Scheduled** (Programado). Para deshabilitar el filtrado web, haga clic en **Always Off** (Siempre desactivado) y en **Save** (Guardar).

**Reputación web:** marque **Web Reputation** (Reputación web) para habilitar el análisis de reputación web.

**Categorías:** haga clic en **Categories** (Categorías); se abrirá la página Web Filter Category (Categoría de filtrado web). Elija entre High (Alto), Medium (Mediano), Low (Bajo) o Custom (Personalizado) para definir rápidamente el tipo de filtrado. También puede elegir los elementos de las categorías Contenido para adultos, Empresa/inversión, Entretenimiento, Ilegales/cuestionables, Recursos de TI, Estilo de vida/cultura, Otros y Seguridad. Las URL entrantes que pertenecen a los elementos seleccionados están bloqueadas. Haga clic en **Save** (Guardar) y en **Back** (Atrás) para ir a la página Web Filter (Filtro web).

**Excepciones:** haga clic en **Exceptions** (Excepciones); se abrirá la página de **White List** (Lista blanca), **Block List** (Lista de bloqueo) y **Exclusion List** (Lista de exclusión). En el campo de cada lista, seleccione el **Type** (Tipo) de mecanismo de filtrado del menú desplegable e ingrese el Valor para agregar/editar un elemento. Haga clic en **Save** (Guardar) y en **Back** (Atrás) para ir a la página Web Filter (Filtro web).

- Haga clic en **Add** (Agregar) e ingrese el valor de los campos.
  - **Name** (Nombre): el nombre de la programación.
  - **Description** (Descripción): describa la programación.
  - Indique las fechas en las que desea que se implemente la programación.
  - **Start** (Inicio): la hora de inicio de la programación.
  - **End** (Finalización): la hora de finalización de la programación.
  - **Active** (Activo): marque esta opción para activar la programación.
  - Haga clic en **Save** (Guardar) para guardar la configuración.

# Cisco Web Filtering Service Supplemental End User License Agreement

This Supplemental End User License Agreement (“SEULA”) contains additional terms and conditions that grant the right to use the Cisco Small Business Web Filtering Service and its associated software (collectively, the “Service”) under the End User License Agreement (“EULA”) between you and Cisco (collectively, the “Terms”). Capitalized terms used in this SEULA but not defined will have the meanings assigned to them in the EULA. To the extent that there is a conflict between the terms and conditions of the EULA and this SEULA, the terms and conditions of this SEULA will take precedence.

In addition to the limitations set forth in the EULA on your access and use of the Service, you agree to comply at all times with the terms and conditions provided in this SEULA. ACCESSING AND USING THE SERVICE CONSTITUTES ACCEPTANCE OF THE TERMS, AND YOU ARE BINDING YOURSELF AND THE BUSINESS ENTITY THAT YOU REPRESENT (COLLECTIVELY, “END USER”) TO THE TERMS. END USER MUST CAREFULLY READ AND ACCEPT ALL OF THE TERMS BEFORE CISCO WILL PROVIDE YOU ACCESS TO THE SERVICE. IF YOU DO NOT

AGREE TO ALL OF THE TERMS, YOU SHOULD CLICK THE “DECLINE” BUTTON WHERE PROMPTED AND DO NOT ACCESS OR USE THE SERVICE. IF YOU AGREE TO ALL OF THE TERMS YOU SHOULD CLICK THE “ACCEPT” BUTTON WHERE PROMPTED.

These Terms are effective on the date of End User’s acceptance. Upon termination of these Terms, End User shall no longer be eligible to use the Service.

1. SCOPE OF THE SERVICE

1.1 These Terms describe the terms and conditions of your use of the Service.

1.2 Service Changes. Cisco reserves the right, at its sole discretion and from time to time, to modify the Service, or parts thereof, including, but not limited to, terminating the availability of a given feature or functionality. Some material Service changes may include a requirement that End User agree to the changed Terms. If End User does not agree with a change in the Service, or a modification of the Terms reflecting such change to the Services, either party may terminate these Terms pursuant to Section 3 (Term and Termination) and End User will no longer have access to the Service.

1.3 Third Party Service. End User understands and agrees that the Service is being provided by one or more third parties on behalf of Cisco (collectively, “Service Provider”), and that if Service Provider stops providing the Service for any reason, End User will no longer have access to the Service. End User may contact Cisco for more information in such event.

2. THE SERVICE

2.1 Service. Subject to End User’s compliance with the Terms, Cisco shall provide End User the Service for use on your Cisco device in accordance with the Service datasheet(s) available at: http://www.cisco.com/c/en/us/products/routers/smallbusiness-rv-series-routers/datasheet-listing.html

3. TERM AND TERMINATION

3.1 Cisco may terminate these Terms immediately upon notice: (i) if End User breaches any provision of these Terms and fails to remedy such breach within thirty (30) days after written notification by Cisco to End User of such breach; or (ii) in the event that Cisco determines, at its sole discretion, to discontinue the Service. Upon termination as specified in these Terms, (a) all rights and licenses of End User hereunder shall terminate, and (b) End User access to the Service shall terminate.

3.2 Cisco may at any time terminate these Terms for convenience, for any reason, or for no reason at all, by providing End User with thirty (30) days prior notice of termination via posting an end of sale notice at: http://www.cisco.com/c/en/us/products/routers/small-business-rv-series-routers/eos-eol-notice-listing.html

3.3 End User may terminate these Terms upon thirty (30) days prior written notice to Cisco if End User does not agree to a change of scope or content made by Cisco in accordance with Section 1.

4. OWNERSHIP AND LICENSE

4.1 Ownership. End User agrees that Cisco and/or Service Provider own all right, title and interest, including intellectual property rights in and to the Service.

4.2 License. Subject to the terms and conditions of these Terms, Cisco grants to End User a limited, non-exclusive, non-transferable license to use the Service on the Cisco device.

5. DATA USAGE AND PROTECTION

5.1 Collection. The Service may collect and send to the Cisco and/or Service Provider the following data: (a) your IP address; (b) your Cisco device model and serial numbers and (c) your Internet search requests (including, but not limited to, full URLs, Internet domains and destination web server IP addresses) (collectively, “Your Data”). End User represents and warrants that End User owns or has all necessary rights to Your Data, and acknowledges that Cisco and Service Provider do not test or screen Your Data, other than what is necessary to provide the Service. Cisco and Service Provider take no responsibility and assumes no liability for Your Data. End User shall be solely responsible and liable for Your Data.

5.2 Transfer. By using the Service, End User agrees and consents to the collection, use, processing and storage of Your Data and any other personal data according to the Terms and the Cisco Privacy Statement (available at: http://www.cisco.com/web/siteassets/legal/privacy.html). To the extent that there is a conflict between the terms and conditions of the Cisco Privacy Statement and the Terms, the terms and conditions of the Terms will take precedence. In performance of the Services, Cisco and/or Service Provider may transfer Your Data to its locations in the United States and/or other jurisdictions. By agreeing to the Terms or using the Service, End User agrees to such transfer of Your Data. Please note that Your Data may not be subject to the same controls as Your current location. End User consents to the uses described above, including but not limited to having Your Data transferred to and processed in the United States and other jurisdictions.

5.3 End User further agrees and consents that Cisco and/or Service Provider may use Your Data to improve the Services and related services from Cisco and/or Service Provider, and may aggregate Your Data in a manner which does not identify End User. Cisco and/or Service Provider may share such aggregate information with third parties.

6. LIMITED WARRANTY AND DISCLAIMER

NOTHING IN THESE TERMS SHALL AFFECT THE WARRANTIES PROVIDED WITH ANY HARDWARE PURCHASED OR SOFTWARE LICENSED FROM CISCO BY END USER. ANY AND ALL SERVICES PROVIDED HEREUNDER ARE PROVIDED ON AN "AS IS" AND "AS AVAILABLE" BASIS. ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS, AND WARRANTIES INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OR CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE (EVEN IF THE PURPOSE IS KNOWN TO CISCO), SATISFACTORY QUALITY, AGAINST INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE, ARE HEREBY EXCLUDED

TO THE GREATEST EXTENT ALLOWED BY APPLICABLE LAW. END USER'S SOLE AND EXCLUSIVE REMEDY FOR BREACH OF WARRANTY SHALL BE, AT CISCO'S OPTION, RE-PERFORMANCE OF THE SERVICE; OR TERMINATION OF THE SERVICE.

IN NO EVENT DOES CISCO OR SERVICE PROVIDER WARRANT THAT THE SERVICE WILL BE UNINTERRUPTED, SECURE OR ERROR FREE.

NEITHER CISCO NOR SERVICE PROVIDER SHALL BE LIABLE FOR ANY FAILURE TO ACHIEVE ANY SERVICE LEVEL AGREEMENT FOR THE SERVICE.

END USER EXPRESSLY ACKNOWLEDGES AND AGREES THAT IT IS SOLELY RESPONSIBLE FOR YOUR DATA AND ANY OTHER DATA UPLOADED TO OR DOWNLOADED USING THE SERVICE. IN NO EVENT SHALL CISCO OR SERVICE PROVIDER BE LIABLE FOR THE ACCURACY OR COMPLETENESS OF THE INFORMATION PROVIDED IN CONNECTION WITH THE SERVICE.

CISCO'S (AND SERVICE PROVIDER'S) TOTAL LIABILITY TO END USER IN CONNECTION WITH CLAIMS ARISING UNDER THESE TERMS SHALL BE LIMITED TO THE MONEY, IF ANY, PAID BY END USER FOR THE SERVICE. THIS LIMITATION OF LIABILITY IS CUMULATIVE AND NOT PER INCIDENT (I.E., THE EXISTENCE OF TWO OR MORE CLAIMS WILL NOT ENLARGE THIS LIMIT).

EXCEPT FOR END USER'S BREACH OF SECTION 4 (OWNERSHIP AND LICENSE), IN NO EVENT SHALL EITHER PARTY, ITS RESPECTIVE AFFILIATES, OFFICERS, DIRECTORS, EMPLOYEES, AGENTS OR SUPPLIERS BE LIABLE FOR ANY SPECIAL, INCIDENTAL, INDIRECT OR CONSEQUENTIAL DAMAGES, OR LOST REVENUE, LOST PROFITS, OR LOST OR DAMAGED DATA, WHETHER ARISING IN CONTRACT, TORT (INCLUDING NEGLIGENCE), OR OTHERWISE, EVEN IF SUCH PARTY HAS BEEN INFORMED OF THE POSSIBILITY THEREOF.

7. GENERAL

7.1 Indemnification. End User hereby indemnifies and holds Cisco harmless from any claim, loss, damage, liability and expense, including reasonable court costs and attorney's fees, resulting from any claim (i) arising out of the acts of End User, its employees or its agents or (ii) arising in connection with Your Data. This shall not limit Cisco's obligations, subject to these Terms, to provide the Service. All financial obligations associated with End User's business are the sole responsibility of End User.

7.2 Third Party Services. Cisco reserves the right to subcontract the provision of all or part of the Service to a third party.

7.3 Force Majeure. Cisco shall not be liable for any delay or failure in performance whatsoever resulting from acts beyond its reasonable control. Such acts shall include, but not be limited to delays attributed to delays of common carriers, acts of God, earthquakes, labor disputes, shortages of supplies, actions of governmental entities, riots, war, acts or threatened acts of terrorism, fire, epidemics and similar occurrences.

7.4 No Waiver. No waiver of rights under these Terms by either party shall constitute a subsequent waiver of this or any other right under these Terms.

7.5 Survival. The following sections shall survive the termination of these Terms: Sections 3 (Term and Termination), 4 (Ownership and License), 5 (Data Usage and Protection), 6 (Limited Warranty and Disclaimer) and 7 (General).

# 15

# Recursos adicionales

| Soporte | |
|---|---|
| Comunidad de soporte de Cisco | www.cisco.com/go/smallbizsupport |
| Soporte y recursos de Cisco | www.cisco.com/go/smallbizhelp |
| Contactos de soporte telefónico | www.cisco.com/en/US/support/tsd_cisco_small_business_support_center_contacts.html |
| Descargas de firmware de Cisco | www.cisco.com/cisco/software/navigator.html?i=!ch<br>Seleccione un enlace para descargar firmware de productos de Cisco. No es necesario iniciar sesión. |
| Solicitud de código abierto de Cisco | www.cisco.com/go/smallbiz_opensource_request |
| Central de partners de Cisco (inicio de sesión del partner requerido) | www.cisco.com/web/partners/sell/smb |
| **Documentación de productos** | |
| Routers y cortafuegos de Cisco | www.cisco.com/go/smallbizrouters |

Para conocer los resultados de las pruebas relacionadas con EU Lot 26, consulte www.cisco.com/go/eu-lot26-results.

**Cisco y el logotipo de Cisco son marcas comerciales o registradas de Cisco Systems, Inc. o de sus filiales en Estados Unidos y en otros países. Para ver una lista de las marcas comerciales de Cisco, visite esta URL: www.cisco.com/go/trademarks. Las marcas comerciales de terceros a las que se hace referencia en esta documentación pertenecen a sus respectivos propietarios. El uso del término "partner" (o sus equivalentes) no implica una relación de sociedad entre Cisco y cualquier otra empresa. (1110R)**

**Copyright © 2014**

Revisión: 9 de abril de 2014 78-21283-01B0

# 15

# Recursos adicionales