IBM i
Versión 7.2

# *Seguridad*
# *Red privada virtual*

IBM i
Versión 7.2

# *Seguridad*
# *Red privada virtual*

**Nota**

Antes de utilizar esta información y el producto al que da soporte, lea la información en la sección “Avisos” en la página 91.

Este documento puede contener referencias al código interno bajo licencia (LIC). El código interno bajo licencia es código de máquina cuya licencia se obtiene bajo los términos del Acuerdo de licencia de IBM para código de máquina.

# Contenido


**Red privada virtual . . . . . 1**
Novedades de IBM i 7.2 . . . . . 1
Archivo PDF de la red privada virtual . . . . . 2
Conceptos de VPN . . . . . 2
Protocolos de IP Security . . . . . 2
Cabecera de autenticación . . . . . 4
Carga útil de seguridad encapsulada . . . . 5
AH y ESP combinados . . . . . 7
Algoritmos criptográficos mejorados . . . . 7
Gestión de claves . . . . . 9
IKE versión 2 . . . . . 11
Renovación de clave IKE_SA . . . . . 12
Búsqueda URL de certificados . . . . . 12
Layer 2 Tunnel Protocol . . . . . 13
Conversión de direcciones de red para VPN . . 13
IPSec (compatible con NAT) con UDP . . . . 15
Compresión de IP . . . . . 16
VPN y filtrado IP . . . . . 16
Conexiones VPN sin filtros de políticas . . . 17
IKE implícito . . . . . 17
Escenarios: VPN . . . . . 18
Escenario: conexión básica entre sucursales . . . 18
Cómo completar las hojas de trabajo de planificación . . . . . 20
Configuración de VPN en el sistema A . . . 21
Configuración de VPN en el sistema C . . . 22
Inicio de VPN . . . . . 22
Prueba de una conexión . . . . . 23
Escenario: conexión básica de empresa a empresa 23
Cómo completar las hojas de trabajo de planificación . . . . . 25
Configuración de VPN en el sistema A . . . 25
Configuración de VPN en el sistema C . . . 26
Activación de las normas de paquetes . . . 27
Inicio de una conexión. . . . . 27
Prueba de una conexión . . . . . 27
Escenario: protección de un túnel voluntario L2TP con IPSec . . . . . 28
Configuración de VPN en el sistema A . . . 29
Configuración de un perfil de conexión PPP y una línea virtual en el sistema A . . . . . 32
Aplicación del grupo de claves dinámicas `l2tptocorp` al perfil PPP `toCorp` . . . . . 33
Configuración de VPN en el sistema B . . . 33
Configuración de un perfil de conexión PPP y una línea virtual en el sistema B . . . . . 33
Activación de las normas de paquetes . . . 34
Escenario: VPN compatible con el cortafuegos . . 35
Cómo completar las hojas de trabajo de planificación . . . . . 37
Configuración de VPN en la pasarela B . . . 38
Configuración de VPN en el sistema E . . . 39
Inicio de una conexión. . . . . 40
Prueba de la conexión . . . . . 41
Escenario: conexión VPN con usuarios remotos 41
Ejecución de las hojas de trabajo de planificación para la conexión VPN de la sucursal al personal de ventas remoto . . . 41
Configuración de un perfil de terminador L2TP del sistema A . . . . . 42
Inicio del perfil de conexión de receptor . . . 43
Configuración de una conexión VPN en el sistema A para clientes remotos. . . . . 44
Activación de las normas de filtros . . . . 44
Configuración de VPN en el cliente Windows 45
Prueba de una conexión VPN entre puntos finales . . . . . 46
Escenario: utilización de la conversión de direcciones de red para VPN . . . . . 46
Planificación de VPN . . . . . 48
Requisitos de configuración de VPN . . . . . 48
Cómo determinar qué tipo de VPN se va a crear 49
Cómo completar las hojas de trabajo de planificación de VPN . . . . . 49
Hoja de trabajo de planificación para conexiones dinámicas . . . . . 49
Hoja de trabajo de planificación para conexiones manuales . . . . . 51
Configuración de VPN . . . . . 52
Configuración de las conexiones VPN con el asistente Nueva conexión. . . . . 53
Configuración de políticas de seguridad de VPN 53
Configuración de una política de intercambio de claves de Internet . . . . . 53
Configuración de una política de datos . . . 54
Configuración de una conexión VPN segura . . 55
Parte 1: Configurar un grupo de claves dinámicas . . . . . 55
Parte 2: configurar una conexión de claves dinámicas . . . . . 56
Configuración de una conexión manual . . . . 56
Configuración de una conexión dinámica . . . 57
Configuración de normas de paquetes VPN . . 57
Configurar la norma de filtro anterior a IPSec 58
Configuración de una norma de filtro de políticas . . . . . 59
Definición de una interfaz para las normas de filtrado VPN . . . . . 61
Activación de las normas de paquetes VPN . 61
Configuración de la confidencialidad de flujo de tráfico . . . . . 62
Configuración del número de secuencia ampliado 63
Configuración de llenar desde paquete . . . . 63
Configuración de VPN NPF para VIPA . . . . 63
Diferencias de configuración de IKEv2 . . . . 64
Inicio de una conexión VPN . . . . . 64
Gestión de VPN . . . . . 65
Establecimiento de los atributos predeterminados de las conexiones . . . . . 65
Restablecimiento de conexiones en estado de error. . . . . 65

Visualización de la información de errores . . . 66
Visualización de los atributos de las conexiones activas . . . . . 66
Visualización de las anotaciones de trabajo del servidor VPN. . . . . 67
Visualización de los atributos de las asociaciones de seguridad . . . . . 67
Detención de una conexión VPN . . . . . 67
Supresión de objetos de configuración de VPN 67
Resolución de problemas de VPN . . . . . 68
Iniciación a la resolución de problemas de VPN 68
Otros aspectos a comprobar . . . . . 69
Errores de configuración de VPN habituales y cómo solucionarlos . . . . . 69
Mensaje de error de VPN: TCP5B28 . . . . 70
Mensaje de error de VPN: Elemento no encontrado . . . . . 70
Mensaje de error de VPN: EL PARÁMETRO PINBUF NO ES VÁLIDO. . . . . 70
Mensaje de error de VPN: Elemento no encontrado, Servidor de claves remoto... . . . 71
Mensaje de error de VPN: No ha sido posible actualizar el objeto . . . . . 71
Mensaje de error de VPN: no ha sido posible cifrar la clave... . . . . 72
Mensaje de error de VPN: CPF9821 . . . . 72
Error de VPN: Todas las claves están en blanco . . . . . 73
Error VPN: La conexión ha habilitado el estado después de que lo haya detenido. . . 73
Error VPN: Se ha producido una anomalía al desactivar las normas de filtro activas . . . 73
Error de VPN: El grupo de conexión de claves de una conexión cambia . . . . . 73
Resolución de problemas de VPN con el diario QIPFILTER . . . . . 74
Habilitación del diario QIPFILTER. . . . . 74
Utilización del diario QIPFILTER . . . . . 74
Campos de diario QIPFILTER . . . . . 75
Resolución de problemas de VPN con el diario QVPN . . . . . 76
Habilitación del diario QVPN . . . . . 77
Utilización del diario QVPN. . . . . 77
Campos de diario QVPN . . . . . 78
Resolución de problemas de VPN con de las anotaciones de trabajo VPN . . . . . 79
Mensajes de error habituales del gestor de conexiones VPN . . . . . 80
Resolución de problemas de VPN con el rastreo de comunicaciones . . . . . 86
Información relacionada para VPN . . . . . 88

**Avisos . . . . . 91**
Información de la interfaz de programación . . . 93
Marcas registradas . . . . . 93
Términos y condiciones . . . . . 93

# Red privada virtual

Una red privada virtual (VPN) permite a su empresa ampliar de forma segura la intranet privada a través de la infraestructura existente de una red pública como Internet. Con VPN, su empresa puede controlar el tráfico de la red a la vez que proporciona características de seguridad importantes, como por ejemplo la autenticación y la privacidad de datos.

Puede configurar VPN con IBM® Navigator for i, la interfaz gráfica de usuario (GUI) para IBM i. Permite crear un camino de extremo a extremo entre cualquier combinación de host y pasarela. VPN utiliza métodos de autenticación, algoritmos de cifrado y otras precauciones para asegurar que los datos enviados entre ambos puntos finales de conexión están protegidos.

VPN se ejecuta bajo la capa de red del modelo de pila de comunicaciones por capas TCP/IP. En particular, VPN utiliza la infraestructura abierta IPSec (IP Security Architecture). IPSec ofrece funciones de seguridad de base para Internet y asimismo, facilita bloques de construcción flexibles, a partir de los cuales puede crear redes privadas virtuales seguras y robustas.

VPN también soporta las soluciones VPN de L2TP (Layer 2 Tunnel Protocol). Las conexiones L2TP, también denominadas líneas virtuales, ofrecen acceso a los usuarios remotos a bajo precio, al permitir que un servidor de red de la empresa gestione las direcciones IP asignadas a sus usuarios remotos. Además, las conexiones L2TP ofrecen un acceso seguro a su sistema o red cuando los proteja con IPSec.

Es importante que sea consciente del efecto que una VPN creará en toda su red. Es esencial realizar una buena planificación e implementación para que los resultados sean satisfactorios. Revise estos temas para asegurar que sabe cómo funcionan las VPN y cómo debe utilizarlas:

## Novedades de IBM i 7.2

Conozca la información nueva o con modificaciones de la colección de temas Redes privadas virtuales.

### IKE Versión 2

Se han añadido mejoras al soporte de IKE versión 2.

- Soporte de negociación IpSec compatible con NAT en IKEv2.
- Renovación de clave de IKE_SA.
- Autenticación con Algoritmo de firma digital de curva elíptica (ECDSA).
- Búsqueda URL de certificados.
- Algoritmos criptográficos mejorados para atributos de asociaciones de seguridad de Política de intercambio de claves y Política de datos.

### Reglas de filtro y mandatos de VPN

Existen nuevos mandatos para cargar y descargar reglas de filtro y para gestionar las conexiones VPN.

- LODIPFTR - cargar y descargar reglas de filtro.
- STRVPNCNN – iniciar conexión VPN.
- ENDVPNCNN - finalizar conexión VPN.
- CPYVPNCFGF - exportación e importación XML de configuraciones VPN.

### Cómo ver las novedades o los cambios

Como ayuda para ver los lugares donde se efectuaron cambios técnicos, este Information Center utiliza:
- La imagen » para marcar el lugar donde empieza la información nueva o cambiada.
- La imagen « para marcar el lugar donde acaba la información nueva o cambiada.

En los archivos PDF, puede que observe barras de revisión (|) en el margen izquierdo de la información nueva o cambiada.

Para encontrar otra información acerca de las novedades o cambios de este release, consulte el Memorándum para los usuarios.

## Archivo PDF de la red privada virtual

Puede ver e imprimir un archivo PDF de esta información.

Para ver o descargar la versión PDF de este documento, seleccione Red privada virtual (VPN) .

### Guardar archivos PDF

Para guardar un archivo PDF en su estación de trabajo para visualizarlo o imprimirlo:
1. Pulse con el botón derecho del ratón el enlace PDF en el navegador.
2. Pulse la opción que guarda el PDF localmente.
3. Navegue hasta el directorio en el que desea guardar el PDF.
4. Pulse **Guardar**.

### Cómo descargar Adobe Reader

Para poder ver o imprimir archivos PDF, debe instalar Adobe Reader en su sistema. Puede bajar una copia desde el sitio Web de Adobe (www.adobe.com/products/acrobat/readstep.html) .

## Conceptos de VPN

Es importante que tenga al menos un conocimiento básico de las tecnologías VPN estándares antes de implementar una conexión VPN.

La VPN (red privada virtual) utiliza varios protocolos TCP/IP importantes para proteger el tráfico de datos. Para comprender mejor el funcionamiento de las conexiones VPN, deberá estar familiarizado con estos protocolos y conceptos, y la forma en que VPN los utiliza:

## Protocolos de IP Security

IP Security (IPSec) proporciona una base estable y duradera para proporcionar seguridad de capa de red.

IPSec soporta todos los algoritmos criptográficos que se utilizan hoy en día y también puede ajustarse a algoritmos nuevos, más potentes que vayan surgiendo. El protocolo IPSec cubre las siguientes cuestiones de seguridad principales:

**Autenticación de origen de datos**
Verifica que cada datagrama ha sido originado por el remitente indicado.

**Integridad de datos**
Verifica que el contenido de un datagrama no se ha cambiado por el camino, ni deliberadamente ni debido a errores aleatorios.

**Confidencialidad de datos**
Oculta el contenido de un mensaje, normalmente mediante cifrado.

**Protección de reproducción**
Impide que un agresor pueda interceptar un datagrama y reproducirlo posteriormente.

**Gestión automatizada de claves criptográficas y asociaciones de seguridad**
Permite utilizar la política VPN en toda la red con poca o ninguna configuración manual.

VPN utiliza dos protocolos IPSec para proteger los datos mientras fluyen a través de la VPN: AH (cabecera de autenticación) y EPS (carga útil de seguridad encapsulada). La otra parte de la habilitación de IPSec es el protocolo IKE (intercambio de claves de Internet) o la gestión de claves. Mientras que IPSec cifra los datos, IKE soporta la negociación automatizada de SA (asociaciones de seguridad) y la generación y la renovación automatizadas de claves criptográficas.

**Nota:** Algunas configuraciones de VPN pueden tener una vulnerabilidad de seguridad dependiendo de cómo se configure IPSec. La vulnerabilidad afecta a las configuraciones en las que IPsec está configurado para utilizar la Carga útil de seguridad encapsulada (ESP) en modalidad de túnel con confidencialidad (cifrado), pero sin protección de la integridad (autenticación) o Cabecera de autenticación (AH). La configuración predeterminada cuando se selecciona ESP siempre incluye un algoritmo de autenticación que proporciona la protección de la integridad. Por lo tanto, a menos que se elimine el algoritmo de autenticación en la transformación ESP, las configuraciones de VPN estarán protegidas contra esta vulnerabilidad. La configuración de VPN de IBM Universal Connection no se ve afectada por esta vulnerabilidad.

Para comprobar si esta vulnerabilidad de seguridad afecta a su sistema, siga estos pasos:

1. En IBM Navigator for i, expanda **Red** > **Políticas IP** > **Red privada virtual** y pulse **Políticas de seguridad IP**.
2. Pulse con el botón derecho del ratón en **Políticas de datos** y seleccione **Abrir**.
3. Pulse con el botón derecho del ratón en la política de datos que desee comprobar y seleccione **Propiedades**.
4. Pulse la pestaña **Proposiciones**.
5. Seleccione una de las proposiciones de protección de datos que utilizan el protocolo ESP y pulse **Editar**.
6. Pulse la pestaña **Transformaciones**.
7. Seleccione en la lista algunas de las transformaciones que utilizan el protocolo ESP y seleccione **Editar**.
8. Compruebe que el algoritmo de autenticación tenga un valor distinto a **Ninguno**.

IETF (Internet Engineering Task Force) define formalmente IPSec en la RFC (Request for Comment) 4301, *Security Architecture for the Internet Protocol*. Puede visualizar esta RFC en Internet, en el siguiente sitio Web: http://www.rfc-editor.org.

Los principales protocolos IPSec se listan a continuación:

**Conceptos relacionados**:

"Gestión de claves" en la página 9
Una VPN dinámica ofrece seguridad adicional para las comunicaciones mediante el protocolo IKE (intercambio de claves de Internet) para la gestión de claves. IKE permite a los servidores VPN de cada extremo de la conexión negociar nuevas claves a intervalos determinados.

**Información relacionada**:

http://www.rfc-editor.org

## Cabecera de autenticación

El protocolo de cabecera de autenticación (AH) ofrece autenticación del origen de los datos, integridad de los datos y protección contra la reproducción. Sin embargo, AH no ofrece confidencialidad de datos, lo que significa que todos los datos se enviarán como texto legible.

AH asegura la integridad de los datos mediante la suma de comprobación que genera un código de autenticación de mensajes, como por ejemplo MD5. Para asegurar la autenticación del origen de los datos, AH incluye una clave compartida secreta en el algoritmo que utiliza para la autenticación. Para asegurar la protección contra la reproducción, AH utiliza un campo de números de secuencia dentro de la cabecera AH. Es importante observar que, a menudo, estas tres funciones distintas se concentran y se conocen como autenticación. En términos más sencillos, AH asegura que no se han manipulado los datos mientras se dirigían a su destino final.

A pesar de que AH autentica el datagrama IP en la mayor medida posible, el destinatario no puede predecir los valores de ciertos campos de la cabecera IP. AH no protege estos campos, conocidos como campos mutables. Sin embargo, AH siempre protege la carga útil del paquete IP.

IETF (Internet Engineering Task Force IETF) define formalmente AH en la RFC (Request for Comment) 4302, *IP Autentication Header*. Puede visualizar esta RFC en Internet, en el siguiente sitio Web: http://www.rfc-editor.org.

### Formas de utilizar AH

Puede aplicar AH de dos formas: modalidad de transporte o modalidad de túnel. En la modalidad de transporte, la cabecera IP del datagrama se encuentra en la parte más externa de la cabecera IP, seguida de la cabecera AH y, a continuación, la carga útil del datagrama. AH autentica el datagrama entero, a excepción de los campos mutables. Sin embargo, la información que contiene el datagrama se transporta como texto legible y, por lo tanto, está sujeto a lecturas. La modalidad de transporte necesita menos actividad general del proceso que la modalidad de túnel, pero no proporciona tanta seguridad.

La modalidad de túnel crea una nueva cabecera IP y la utiliza como parte más externa de la cabecera IP del datagrama. La cabecera AH continúa en la nueva cabecera IP. El datagrama original (tanto la cabecera IP como la carga útil original) aparece en último lugar. AH autentica el datagrama entero, por lo tanto, el sistema que responde puede detectar si el datagrama ha cambiado por el camino.

Si ambos extremos de una asociación de seguridad hay una pasarela, utilice la modalidad de túnel. En la modalidad de túnel, las direcciones de origen y destino de la parte más externa de la cabecera IP no tienen necesariamente que ser iguales que las direcciones de la cabecera IP original. Por ejemplo, dos pasarelas de seguridad pueden operar un túnel AH para autenticar todo el tráfico entre las redes que conectan. De hecho, esta es una configuración muy habitual.

La principal ventaja de utilizar esta modalidad de túnel es que esta modalidad protege totalmente el datagrama IP encapsulado. Además, la modalidad de túnel hace posible utilizar direcciones privadas.

### ¿Por qué AH?

En muchos casos, sus datos sólo necesitan autenticación. Aunque el protocolo ESP (carga útil de seguridad encapsulada) puede realizar la autenticación, AH no afecta al rendimiento de su sistema como lo hace ESP. Otra ventaja de utilizar AH es que ésta autentica el datagrama entero. ESP, no obstante, no autentica la parte inicial de la cabecera IP o cualquier otra información que preceda a la cabecera ESP.

Además, para poder poner en vigor ESP hay que disponer de algoritmos criptográficos de 128 KB. La criptografía de 128 KB está restringida en algunas regiones, mientras que AH no está regulada y puede utilizarse libremente en todo el mundo.

### Utilización de ESN con AH

Si utiliza el protocolo AH, puede habilitar el Número de secuencia ampliado (ESN). ESN permite transmitir grandes volúmenes de datos a una gran velocidad sin necesidad de volver a aplicar las claves. La conexión VPN utiliza números de secuencia de 64 bits, en lugar de números de 32 bits a través de IPSec. La utilización de números de secuencia de 64 bits permite disponer de más tiempo antes de volver a aplicar las claves, lo que evita que se agoten los números de secuencia y minimiza el uso de recursos del sistema.

### ¿Qué algoritmos utiliza AH para proteger la información?

AH utiliza algoritmos conocidos como **HMAC (códigos de autenticación de mensajes con valores hash)**.
| Específicamente, la VPN utiliza HMAC-MD5, HMAC-SHA, HMAC-SHA-256,HMAC-SHA384,
| HMAC-SHA512, o AES-XCBC-MAC. Cada uno de los algoritmos utiliza datos de entrada de longitud variable y una clave secreta para generar datos de salida de longitud fija (llamado valor hash o MAC). Si los valores hash de dos mensajes coinciden, es probable que los mensajes sean idénticos.

IETF (Internet Engineering Task Force IETF) define formalmente los algoritmos en la RFC (Request for Comments):

- HMAC-MD5 en la RFC 2085, *HMAC-MD5 IP Authentication with Replay Prevention*
- HMAC-SHA en la RFC 2404, *The use of HMAC-SHA-1-96 within ESP and AH*
- | HMAC-SHA_256,HMAC-SHA-384, y HMAC-SHA-512 en RFC 4868, *Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec*
- AES-XCBC-MAC en la RFC 3566, *The AES-XCBC-MAC-96 Algorithm and Its Use With IPsec*

Puede consultar estas RFC en Internet, en el siguiente sitio Web: http://www.rfc-editor.org.

**Conceptos relacionados**:

"Carga útil de seguridad encapsulada"
El protocolo ESP (carga útil de seguridad encapsulada) ofrece confidencialidad de datos y, de forma opcional, ofrece autenticación del origen de los datos, comprobación de la integridad y protección contra la reproducción.

"Algoritmos criptográficos mejorados" en la página 7
| Los algoritmos criptográficos soportados en la selección VPN para atributos de asociaciones de seguridad de Política de intercambio de claves y Política de datos.

**Información relacionada**:

http://www.rfc-editor.org

## Carga útil de seguridad encapsulada

El protocolo ESP (carga útil de seguridad encapsulada) ofrece confidencialidad de datos y, de forma opcional, ofrece autenticación del origen de los datos, comprobación de la integridad y protección contra la reproducción.

La diferencia entre ESP y el protocolo AH (cabecera de autenticación) es que ESP ofrece cifrado, mientras que ambos protocolos ofrecen autenticación, comprobación de la integridad y protección contra la reproducción. Con ESP, ambos sistemas de comunicación utilizarán una clave compartida para cifrar y descifrar los datos que intercambian.

Si decide utilizar tanto el cifrado como la autenticación, el sistema que responde autentica el paquete en primer lugar y, a continuación, si el primer paso tiene éxito, el sistema procede con el descifrado. Este tipo de configuración reduce la actividad general de proceso y asimismo reduce la vulnerabilidad frente a ataques de denegación de servicio.

### Hay dos formas de utilizar ESP

Puede aplicar ESP de dos formas: modalidad de transporte o modalidad de túnel. En la modalidad de transporte, la cabecera ESP sigue a la cabecera IP del datagrama IP original. Si el datagrama ya dispone de una cabecera IPSec, la cabecera ESP precederá a ésta. La cola ESP y datos de autenticación opcionales siguen a la carga útil.

La modalidad de transporte no autentica o cifra la cabecera IP, que podría dejar en evidencia la información de direccionamiento al alcance de posibles agresores mientras el datagrama está en tránsito. La modalidad de transporte necesita menos actividad general del proceso que la modalidad de túnel, pero no proporciona tanta seguridad. En la mayoría de los casos, los hosts utilizan la ESP en modalidad de transporte.

La modalidad de túnel crea una nueva cabecera IP y la utiliza como parte más externa de la cabecera IP del datagrama, seguido de la cabecera ESP y, a continuación, el datagrama original (tanto la cabecera IP como la carga útil original). La cola de ESP y datos de autenticación opcionales se añaden a la carga útil. Cuando utilice el cifrado y la autenticación, la ESP protegerá completamente el datagrama original porque ahora se habrán convertido en los datos de la carga útil del nuevo paquete ESP. ESP, sin embargo, no protege la nueva cabecera IP. Las pasarelas deben utilizar la ESP en modalidad de túnel.

### ¿Qué algoritmos utiliza ESP para proteger la información?

ESP utiliza una clave simétrica que utilizan ambas partes comunicantes para cifrar y descifrar los datos que intercambian. El remitente y el destinatario deben estar de acuerdo sobre la clave para que pueda tener lugar una comunicación segura entre ambos. VPN utiliza DES (estándar de cifrado de datos), triple
| DES (3DES), AES (estándar de cifrado avanzado) o AES-CBC y AES-CTR para el cifrado.

Si elige el algoritmo AES para el cifrado, puede habilitar el Número de secuencia ampliado (ESN). ESN permite transmitir grandes volúmenes de datos a una gran velocidad. La conexión VPN utiliza números de secuencia de 64 bits, en lugar de números de 32 bits a través de IPSec. La utilización de números de secuencia de 64 bits permite disponer de más tiempo antes de volver a aplicar las claves, lo que evita que se agoten los números de secuencia y minimiza el uso de recursos del sistema.

IETF (Internet Engineering Task Force IETF) define formalmente los algoritmos en la RFC (Request for Comments):

- DES en la RFC (Request for Comment) 1829, *The ESP DES-CBC Transform*
- 3DES en la RFC 1851, *The ESP Triple DES Transform*.
- AES-CBC en la RFC 3602, *The AES-CBC Cipher Algorithm and Its Use with IPsec*
- | AES-CTR en la RFC 3686, *Using Advanced Encryption Standard (AES) Counter Mode with IPSec*
  | *Encapsulating Security Payload (ESP)*

Puede consultar estas y otras RFC en Internet, en la siguiente dirección Web: http://www.rfc-editor.org.

| ESP utiliza los algoritmos HMAC-MD5, HMAC-SHA, HMAC-SHA-256, HMAC-SHA-384,
| HMAC-SHA-512, y AES-XCBC-MAC para ofrecer funciones de autenticación. Cada uno de los algoritmos utiliza datos de entrada de longitud variable y una clave secreta para generar datos de salida de longitud fija (llamado valor hash o MAC). Si los valores hash de dos mensajes coinciden, es probable que los mensajes sean idénticos.

IETF (Internet Engineering Task Force IETF) define formalmente los algoritmos en la RFC (Request for Comments):

- HMAC-MD5 en la RFC 2085, *HMAC-MD5 IP Authentication with Replay Prevention*
- HMAC-SHA en la RFC 2404, *The use of HMAC-SHA-1-96 within ESP and AH*

| • HMAC-SHA_256,HMAC-SHA-384, y HMAC-SHA-512 en RFC 4868, *Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec*
• AES-XCBC-MAC en la RFC 3566, *The AES-XCBC-MAC-96 Algorithm and Its Use With IPsec*

Puede consultar estas RFC en Internet, en la siguiente dirección Web: http://www.rfc-editor.org.

| ESP utiliza AES-CCM y AES-GCM para proporcionar cifrado y autenticación. No puede seleccionarse un
| algoritmo de autenticación si se elige uno de estos algoritmos "combinados".
| • AES-CCM en la RFC 4309, *Using Advanced Encryption Standard (AES) CCM mode with IPSec Encapsulating Security Payload (ESP)*
| • AES-GCM en la RFC 4106, *The Use of Galios/Counter Mode (GCM) in IPSec Encapsulating Security Payload (ESP)*

| ESP utiliza AES-GMAC (Galios Message Authentication Code) para proporcionar autenticación, pero no
| cifrado.
| • AES-GMAC en la RFC 4543, *The Use of Galios Message Authentication Code (GMAC) in IPSec ESP and AH.*

**Conceptos relacionados**:

"Cabecera de autenticación" en la página 4
El protocolo de cabecera de autenticación (AH) ofrece autenticación del origen de los datos, integridad de los datos y protección contra la reproducción. Sin embargo, AH no ofrece confidencialidad de datos, lo que significa que todos los datos se enviarán como texto legible.

"Algoritmos criptográficos mejorados"
| Los algoritmos criptográficos soportados en la selección VPN para atributos de asociaciones de seguridad de Política de intercambio de claves y Política de datos.

**Información relacionada**:

http://www.rfc-editor.org

## AH y ESP combinados

VPN permite combinar AH y ESP para conexiones de host a host en modalidad de transporte.

La combinación de estos protocolos protege todo el datagrama IP. A pesar de que la combinación de ambos protocolos ofrece más seguridad, la actividad general de proceso que conlleva puede pesar más que el beneficio.

## Algoritmos criptográficos mejorados

| Los algoritmos criptográficos soportados en la selección VPN para atributos de asociaciones de seguridad de Política de intercambio de claves y Política de datos.

Política de intercambio de claves:

- Cifrado
  - 3DES-CBC
  | - AES-CBC (128, 192 y 256 bits)
  | - AES-CTR (128, 192 y 256 bits)
- Hash/PRF
  - SHA
  - HMAC-SHA-256
  | - HMAC-SHA-384
  | - HMAC-SHA-512
  - AES-XCBC-MAC (HASH 96 bits; PRF 128 bits)
- Diffie-Hellman
  - Grupo 1

- Grupo 2
- Grupo 14
- Grupo 19 (ECP de 256)
- Grupo 20 (ECP de 384)
- Grupo 24

Política de datos:

- Autenticación
  - SHA
  - HMAC-SHA-256
  - HMAC-SHA-384
  - HMAC-SHA-512
  - AES-XCBC-MAC
- Diffie-Hellman para PFS
  - Grupo 1
  - Grupo 2
  - Grupo 14
  - Grupo 19 (ECP de 256 bits)
  - Grupo 20 (ECP de 384 bits)
  - Grupo 24
- Cifrado
  - 3DES-CBC
  - AES-CBC (128, 192 y 256 bits)
  - AES-CTR (128, 192 y 256 bits)
  - AES-CCM (128, 192 y 256 bits)
  - AES-GCM (128, 192 y 256 bits)
  - AES-GMAC (128, 192 y 256 bits)

Además de los algoritmos criptográficos mejorados soportados, se resta énfasis a los algoritmos siguientes. Siguen estando soportados, pero la tendencia es utilizarlos menos.

- Hash
  - MD5
- Cifrado
  - DES
  - RC4
  - RC5

IETF (Internet Engineering Task Force IETF) define formalmente los algoritmos en la RFC (Request for Comments):

- AES-CBC en la RFC 3602, *The AES-CBC Cipher Algorithm and Its Use with IPsec*
- AES-XCBC-MAC en la RFC 3566, *The AES-XCBC-MAC-96 Algorithm and Its Use With IPsec*
- HMAC-SHA_256, HMAC-SHA-384 y HMAC-SHA-512 en la RFC 4868, *Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec*
- HMAC-MD5 en la RFC 2085, *HMAC-MD5 IP Authentication with Replay Prevention*
- DES en la RFC (Request for Comment) 1829, *The ESP DES-CBC Transform*
- Grupos DH 19 y 20 en la RFC 4754, *IKE and IKEV2 Authentication Using the Elliptical Curve Digital Signature Algorithm (ECDSA)*

| • AES-CTR en la RFC 3686, *Using Advanced Encryption (AES) Counter Mode with IPSec Encapsulating Security Payload (ESP)*
| • AES-CCM en la RFC 4309, *Using Advanced Encryption Standard (AES) CCM mode with IPSec Encapsulating Security Payload (ESP)*
| • AES-GCM en la RFC 4106, *The Use of Galios/Counter Mode (GCM) in IPSec Encapsulating Security Payload (ESP)*
| • AES-GMAC en la RFC 4543, *The Use of Galios Message Authentication Mode (GMAC) in IPSec ESP and AH*

Puede consultar estas RFC en Internet, en la siguiente dirección Web: http://www.rfc-editor.org.

**Conceptos relacionados**:

"Cabecera de autenticación" en la página 4
El protocolo de cabecera de autenticación (AH) ofrece autenticación del origen de los datos, integridad de los datos y protección contra la reproducción. Sin embargo, AH no ofrece confidencialidad de datos, lo que significa que todos los datos se enviarán como texto legible.

"Carga útil de seguridad encapsulada" en la página 5
El protocolo ESP (carga útil de seguridad encapsulada) ofrece confidencialidad de datos y, de forma opcional, ofrece autenticación del origen de los datos, comprobación de la integridad y protección contra la reproducción.

## Gestión de claves

Una VPN dinámica ofrece seguridad adicional para las comunicaciones mediante el protocolo IKE (intercambio de claves de Internet) para la gestión de claves. IKE permite a los servidores VPN de cada extremo de la conexión negociar nuevas claves a intervalos determinados.

Después de cada negociación satisfactoria, los servidores VPN regeneran las claves que protegen la conexión, de forma que resulte más difícil para un agresor capturar información de la conexión. Adicionalmente, si utiliza el secreto progresivo perfecto, los agresores no podrán deducir las futuras claves en base a información de claves anterior.

El gestor de claves de VPN es la implementación de IBM del protocolo de intercambio de claves de Internet (IKE). El gestor de claves soporta la negociación automática de las SA (asociaciones de seguridad), así como la regeneración y renovación automática de claves criptográficas.

Una **SA (Asociación de seguridad)** contiene información necesaria para utilizar los protocolos IPSec. Por ejemplo, una SA identifica el tipo de algoritmo, la longitud y el tiempo de vida de una clave, las partes participantes y las modalidades de encapsulación.

Las claves criptográficas, como implica su nombre, bloquean o protegen la información hasta que ésta alcanza de forma segura su destino final.

**Nota:** La generación de sus claves de forma segura es el factor más importante al establecer una conexión privada y segura. Si sus claves están comprometidas, sus esfuerzos de autenticación y cifrado, no importa lo duros que sean, serán inútiles.

**Fases de la gestión de claves**

El gestor de claves de VPN utiliza dos fases distintas en su implementación.

**Fase 1** La fase 1 establece un secreto principal a partir del cual se derivan las claves criptográficas ulteriores para proteger el tráfico de datos del usuario. Esto es cierto incluso aunque no exista todavía protección de seguridad entre ambos puntos finales. VPN utiliza la modalidad de firma RSA, la modalidad de firma ECDSA, o claves precompartidas para autenticar las negociaciones de la fase 1, así como para establecer las claves que protegen los mensajes IKE que fluyen durante las negociaciones de la fase 2 subsiguientes.

Una *clave precompartida* es una serie no trivial de 128 caracteres como máximo. Ambos extremos de una conexión deben ponerse de acuerdo sobre la clave precompartida. La ventaja de la utilización de claves precompartidas es la simplicidad, la desventaja es que un secreto compartido debe comunicarse por otros canales, por ejemplo a través del teléfono o de correo certificado, antes de las negociaciones IKE. Debe tratar la clave precompartida como si fuera una contraseña.

La autenticación de la *Firma RSA* ofrece una mayor seguridad que las claves precompartidas porque esta modalidad utiliza certificados digitales para la autenticación. Debe configurar sus certificados digitales a través del Gestor de certificados digitales. VPN no tiene ningún límite para las longitud de clave de RSA que admite. Los certificados que utilice deben provenir de autoridades certificadoras en las que confíen ambos servidores de claves.

Las *Firmas ECDSA* son más pequeñas que las Firmas RSA de una potencia de cifrado similar, dando una mejora en la eficiencia de comunicación. Las Firmas ECDSA dan soporte a tres longitudes de clave, ECDSA-256, ECDSA-384 y ECDSA-521. Debe configurar sus certificados digitales a través del Gestor de certificados digitales. Los certificados que utilice deben provenir de autoridades certificadoras en las que confíen ambos servidores de claves. Las Firmas ECDSA no están soportadas en IKEv1.

**Fase 2** No obstante, la fase 2 negocia las asociaciones de seguridad y las claves que protegen los intercambios de datos reales de la aplicación. Recuerde que hasta este punto no se han enviado realmente datos de aplicación. La fase 1 protege los mensajes IKE de la fase 2.

Una vez que las negociaciones de la fase 2 han terminado, la VPN establece una conexión dinámica segura a través de la red y entre los puntos finales definidos para la conexión. Todos los datos que fluyen a través de la VPN se entregan con el grado de seguridad y eficiencia acordado por los servidores de claves durante los procesos de negociación de la fase 1 y la fase 2.

En general, las negociaciones de la fase 1 se llevan a cabo una vez al día, mientras que las negociaciones de fase 2 se renuevan cada 60 minutos o incluso cada 5 minutos. Las velocidades de renovación elevadas aumentan la seguridad de los datos, pero disminuyen el rendimiento del sistema. Utilice tiempos de vida de clave breves para proteger sus datos más delicados.

Al crear una VPN dinámica mediante IBM Navigator for i, debe definir una política IKE para permitir las negociaciones de la fase 1 y una política de datos para controlar las negociaciones de la fase 2. Opcionalmente, puede utilizar el asistente Nueva conexión. El asistente crea automáticamente cada uno de los objetos de configuración que VPN necesita para funcionar correctamente, incluyendo una política IKE y una política de datos.

## Lectura recomendada

Si desea leer más acerca del protocolo y la gestión de claves IKE (intercambio de claves de Internet), revise estos RFC (Request for Comments) de IETF (Internet Engineering Task Force):

**IKEv1**

- RFC 2407, *The Internet IP Security Domain of Interpretation for ISAKMP*
- RFC 2408, *Internet Security Association and Key Management Protocol (ISAKMP)*
- RFC 2409, *The Internet Key Exchange (IKE)*

Estas RFC están soportadas actualmente para IKEv1.

Puede consultar estas RFC en Internet, en el siguiente sitio Web: http://www.rfc-editor.org.

**Conceptos relacionados**:

"Escenario: VPN compatible con el cortafuegos" en la página 35
En este escenario, una gran empresa de seguros desea establecer una VPN entre una pasarela en Chicago y un host en Minneapolis, donde ambas redes están detrás de un cortafuegos.

"Protocolos de IP Security" en la página 2
IP Security (IPSec) proporciona una base estable y duradera para proporcionar seguridad de capa de red.

"IKE versión 2"
IKE versión 2 es una mejora del protocolo de intercambio de claves de Internet.

**Tareas relacionadas**:

"Configuración de una política de intercambio de claves de Internet" en la página 53
La política de intercambio de claves de Internet (IKE) define qué nivel de autenticación y de protección de cifrado utilizará IKE durante las negociaciones de fase 1.

"Configuración de una política de datos" en la página 54
Una política de datos define el nivel de autenticación o cifrado con que se protegen los datos que fluyen a través de la VPN.

**Información relacionada**:

http://www.rfc-editor.org

## IKE versión 2

IKE versión 2 es una mejora del protocolo de intercambio de claves de Internet.

IKE versión 2 (IKEv2) ha sido desarrollado por IETF con RFC4306. IKEv2 mejora la función de negociar el intercambio de claves dinámico y la autenticación de los sistemas de negociación para VPN.

IKEv2 también simplifica los flujos de intercambio de claves e introduce medidas para arreglar ambigüedades y vulnerabilidades inherentes a IKEv1.

- IKEv2 proporciona un flujo de mensajes más simple para las negociaciones de intercambio de claves.
- IKEv2 proporciona opciones para renovar la clave de IKE_SA sin volver a autenticar.
- Con IKEv2, los tiempos de vida de clave para IKE_SA y CHILD_SA se gestionan independientemente del sistema igual.
- IKEv2 es la base para futuras mejoras en el protocolo de intercambio de claves.

Tanto el protocolo IKEv1 como el protocolo IKEv2 operan en dos fases. Las diferencias entre los dos protocolos incluyen:

- La primera fase de IKEv2 es IKE_SA, que consta del par de mensajes IKE_SA_INIT. Los atributos de la fase IKE_SA se definen en la Política de intercambio de claves.
- La segunda fase de IKEv2 es CHILD_SA. El primer CHILD_SA es el par de mensajes IKE_AUTH. Se pueden enviar más pares de mensajes CHILD_SA para mensajes informativos y de renovación de claves. Los atributos de CHILD_SA se definen en la Política de datos.

IKEv2 proporciona un intercambio más eficaz y simple.

- La fase 1 de IKEv1 tiene dos intercambios posibles: modalidad principal y modalidad agresiva. Con la modalidad principal, las negociaciones de la fase 1 y la fase 2 están en dos fases separadas. La modalidad principal de la fase 1 utiliza seis mensajes para completarse; la fase 2 en modalidad rápida utiliza tres mensajes.
- IKEv2 combina estas modalidades en una secuencia de cuatro mensajes. IKE_SA se negocia y se autentica y luego CHILD_SA se negocia y se generan claves en cuatro mensajes. La renovación de clave posterior de CHILD_SA se consigue en dos mensajes.

A pesar de estos cambios, el resultado básico de las dos versiones es el mismo. IKEv1 y IKEv2 negocian una asociación de seguridad para proteger los datos entre dos puntos finales.

## Lectura recomendada

Para obtener más información acerca del protocolo y la gestión de claves IKE (intercambio de claves de Internet), revise estos RFC (Request for Comments) de IETF (Internet Engineering Task Force):

**IKEv2**

- RFC 4306, *The Internet Key Exchange (IKEv2) Protocol*
- RFC 5996, *The Internet key Exchange Protocol Version 2* (soportado en IBM i 7.2 solamente).

Estas RFC están soportadas actualmente para IKEv2.

Puede consultar estas RFC en Internet, en el siguiente sitio Web: http://www.rfc-editor.org.

**Conceptos relacionados**:

"Gestión de claves" en la página 9
Una VPN dinámica ofrece seguridad adicional para las comunicaciones mediante el protocolo IKE (intercambio de claves de Internet) para la gestión de claves. IKE permite a los servidores VPN de cada extremo de la conexión negociar nuevas claves a intervalos determinados.

"Diferencias de configuración de IKEv2" en la página 64
Comparación entre la configuración de IKEv1 e IKEv2.

"Resolución de problemas de VPN con de las anotaciones de trabajo VPN" en la página 79
Si encuentra problemas con las conexiones VPN, se recomienda siempre que analice las anotaciones de trabajo. De hecho, hay varias anotaciones de trabajo que contienen mensajes de error y otra información relacionada con un entorno VPN.

## Renovación de clave IKE_SA

La renovación de clave IKE_SA permite a IKE_SA experimentar una renovación de clave sin volver a autenticar.

La renovación de clave IKE_SA se realiza como un intercambio independiente cuando una parte determina que IKE_SA ha caducado. Se renueva una clave IKE_SA nueva a tiempo para el intento de renovar CHILD_SA.

Para habilitar la renovación de clave IKE_SA, siga estos pasos:

- Expanda **Red** > **Todas las tareas** > **Políticas IP** > **Red privada virtual**.
- Pulse **Propiedades**.
- Marque el recuadro **Habilitar renovación de clave IKE_SA para IKEv2** para activar la renovación de clave IKE_SA.

**Nota:** El recuadro **Habilitar renovación de clave IKE_SA para IKEv2** no está seleccionado de forma predeterminada. Si se determina que un IKE_SA siempre debe autenticarse por motivos de seguridad, el recuadro **Habilitar renovación de clave IKE_SA para IKEv2** deberá permanecer sin marcar.

## Búsqueda URL de certificados

La búsqueda URL de certificados permite a los socios de negociaciones de IKE enviar un enlace de URL a un certificado que se utiliza para autenticar el intercambio.

La finalidad de la búsqueda URL de certificados es ahorrar ancho de banda en la carga útil de las negociaciones IKE. IKEv2 sólo da soporte a iguales enviando búsqueda URL de certificados. Para habilitar este soporte y requerir que los iguales siempre envíen el certificado completo durante la autenticación de IKE_SA, siga estos pasos:

- Expanda **Red** > **Todas las tareas** > **Políticas IP** > **Red privada virtual**.
- Pulse **Propiedades**.
- Marque el recuadro **Permitir búsqueda HTTP de los certificados enviados por sistemas remotos** para activar la búsqueda URL de certificados.

## Layer 2 Tunnel Protocol

Las conexiones L2TP (Layer 2 Tunneling Protocol), también denominadas líneas virtuales, ofrecen acceso a los usuarios remotos a bajo precio, al permitir que un sistema de red de la empresa gestione las direcciones IP asignadas a sus usuarios remotos. Además, las conexiones L2TP ofrecen un acceso seguro a su sistema o red cuando las utilice conjuntamente con IPSec (IP Security).

L2TP soporta dos modalidades de túnel: el túnel voluntario y el túnel obligatorio. La diferencia más importante entre ambos es el punto final. En el túnel voluntario, el túnel termina en el cliente remoto mientras que el túnel obligatorio termina en el proveedor de servicios de Internet (ISP).

Con un **túnel obligatorio** L2TP, un host remoto inicia la conexión con su ISP. A continuación, ISP establece una conexión L2TP entre el usuario remoto y la red de la empresa. A pesar de que el ISP establece la conexión, deberá decidir cómo proteger el tráfico mediante VPN. Con un túnel obligatorio, ISP debe soportar LT2P.

Con un **túnel voluntario** L2TP, el usuario remoto crea la conexión , normalmente mediante un cliente de túnel L2TP. Como resultado, el usuario remoto envía los paquetes L2TP a su ISP, que los reenvía a la red de la empresa. Con un túnel voluntario, ISP no necesita soportar L2TP. El escenario Proteger un túnel voluntario L2TP con IPSec proporciona un ejemplo de cómo configurar un sistema de una sucursal para que se conecte con la red corporativa mediante un sistema de pasarela con un túnel L2TP protegido por VPN.

Puede ver una presentación visual sobre el concepto de los Túneles voluntarios L2TP protegidos por IPSec. Para ello, se necesita el Conector Flash. También puede utilizar la versión HTML de esta presentación.

L2TP es en realidad una variación de un protocolo de encapsulado IP. El túnel L2TP se crea al encapsular un marco L2TP dentro de un paquete UDP (Protocolo de datagramas de usuario), que, a su vez, está encapsulado en un paquete IP. Las direcciones de origen y destino de este paquete IP definen los puntos finales de conexión. Debido a que el protocolo de encapsulado exterior es IP, puede aplicar los protocolos IPSec al paquete IP compuesto. De esta forma, se protegen los datos que fluyen dentro del túnel L2TP. A continuación, puede aplicar directamente la cabecera de autenticación (AH), la carga útil de seguridad encapsulada (ESP) y el protocolo de intercambio de claves de Internet (IKE).

**Conceptos relacionados**:

"Escenario: protección de un túnel voluntario L2TP con IPSec" en la página 28
En este escenario, aprenderá a configurar una conexión entre el host de una sucursal y una oficina central que utiliza L2TP protegido por IPSec. La sucursal tiene una dirección IP asignada dinámicamente, mientras que la oficina central tiene una dirección IP estática direccionable globalmente.

## Conversión de direcciones de red para VPN

VPN proporciona una forma de realizar la conversión de direcciones de red, denominada NAT VPN. NAT VPN se diferencia de la NAT tradicional en que aquélla convierte las direcciones antes de aplicarlas a los protocolos IKE e IPSec. Consulte este tema para obtener más información.

NAT (conversión de direcciones de red) toma sus direcciones IP privadas y las convierte en direcciones IP públicas. De esta forma, facilita la conservación de direcciones públicas valiosas y, al mismo tiempo, permite a los hosts de su red acceder a los servicios y hosts remotos a través de Internet (u otras redes públicas).

Además, si utiliza direcciones IP privadas, estas pueden entrar en conflicto con direcciones IP entrantes parecidas. Por ejemplo: desea comunicarse con otra red y ambas redes utilizan direcciones 10.*.*.*.; las direcciones entrarán en conflicto y todos los paquetes se desactivarán. Si aplica NAT a sus direcciones salientes, podrá solucionar este problema. Sin embargo, si el tráfico de datos está protegido por una VPN, la NAT convencional no funcionará porque modifica las direcciones IP en las SA (asociaciones de

seguridad) que VPN necesita para funcionar. Para evitar este problema, VPN ofrece su propia versión de la conversión de direcciones de red, denominada NAT VPN. VPN NAT realiza conversiones de direcciones antes de la validación SA, asignando una dirección a la conexión cuando ésta se inicia. Esta dirección permanece asociada a la conexión hasta que ésta se suprime.

**Nota:** FTP no soporta VPN NAT actualmente.

**¿Cómo utilizar VPN NAT?**

Hay dos tipos distintos de VPN NAT que necesita considerar antes de empezar. Son los siguientes:

**VPN NAT para evitar conflictos entre direcciones IP**

Este tipo de VPN NAT permite evitar todos los conflictos posibles entre direcciones IP que se producen al configurar una conexión VPN entre redes o sistemas con esquemas de direccionamiento similares. Un escenario habitual es aquel en que ambas empresas desean crear conexiones VPN utilizando uno de los rangos de direcciones IP privadas designados. Por ejemplo, 10.*.*.*. La forma en que deberá configurar este tipo de VPN NAT depende de si su sistema es el iniciador o el contestador de la conexión VPN. Cuando el sistema es el iniciador de la conexión, puede convertir las direcciones locales en direcciones compatibles con la dirección de la conexión VPN asociada. Cuando el sistema es el contestador de la conexión, puede convertir las direcciones remotas VPN de su socio en direcciones compatibles con su esquema de direccionamiento local. Configure este tipo de conversión de direcciones sólo para las conexiones dinámicas.

**VPN NAT para ocultar direcciones locales**

Este tipo de VPN NAT se utiliza ante todo para ocultar la dirección IP real de su sistema local, mediante la conversión de su dirección en otra dirección, que se hace disponible públicamente. Al configurar VPN NAT, puede especificar que cada dirección IP conocida públicamente se convierta a su dirección de una agrupación de direcciones ocultas. Esto también permite equilibrar la carga de tráfico de una dirección individual a través de direcciones múltiples. VPN NAT para direcciones locales precisa que el sistema actúe como contestador de las conexiones.

Utilice VPN NAT para ocultar direcciones locales si responde afirmativamente a estas preguntas:

1. ¿Tiene uno o varios sistemas a los que quiera que accedan las personas mediante una VPN?
2. ¿Necesita ser flexible con las direcciones IP reales de sus sistemas?
3. ¿Tiene una o varias direcciones IP globalmente direccionables?

El escenario Utilizar la conversión de direcciones de red para VPN proporciona un ejemplo de cómo configurar VPN NAT para ocultar direcciones locales en el modelo IBM i.

Para obtener instrucciones paso a paso acerca de cómo configurar VPN NAT en el sistema, consulte la ayuda en línea disponible en la interfaz VPN de IBM Navigator for i.

**Conceptos relacionados**:

"Escenario: utilización de la conversión de direcciones de red para VPN" en la página 46
En este escenario, la empresa desea intercambiar datos sensibles con uno de sus asociados comerciales mediante VPN. Para preservar mejor la privacidad de la estructura de red de la empresa, ésta también utilizará VPN NAT para ocultar la dirección IP privada del sistema que utiliza para alojar las aplicaciones a las que el asociado comercial tiene acceso.

"Hoja de trabajo de planificación para conexiones manuales" en la página 51
Complete esta hoja de trabajo para configurar una conexión manual.

# IPSec (compatible con NAT) con UDP

La encapsulación UDP permite que el tráfico IPSec pase a través de un dispositivo NAT convencional. Consulte este tema para obtener más información acerca de sus características y las razones por las que debe utilizarla para las conexiones VPN.

## El problema: la NAT convencional interrumpe VPN

La conversión de direcciones de red (NAT) permite ocultar las direcciones IP privadas no registradas detrás de un conjunto de direcciones IP registradas. Esto ayuda a proteger la red interna de las redes externas. NAT también ayuda a reducir el problema del agotamiento de direcciones IP, dado que un pequeño conjunto de direcciones registradas puede representar a muchas direcciones privadas.

Desgraciadamente, la NAT convencional no funciona en los paquetes IPSec debido a que, cuando el paquete pasa por un dispositivo NAT, la dirección origen del paquete cambia, invalidando con ello el paquete. Cuando esto ocurre, el terminal receptor de la conexión VPN descarta el paquete y las negociaciones de la conexión VPN fallan.

## La solución: encapsulación UDP

En una nutshell, la encapsulación UDP envuelve un paquete IPSec dentro de una cabecera IP/UDP nueva pero duplicada. La dirección de la cabecera IP nueva se convierte cuando pasa a través del dispositivo NAT. A continuación, cuando el paquete alcanza su destino, el terminal receptor elimina la cabecera adicional dejando el paquete IPSec original, que ahora pasará todas las demás validaciones.

Sólo puede aplicar la encapsulación UDP a las VPN que vayan a utilizar IPSec ESP en modalidad de túnel o en modalidad de transporte. Además, el sistema sólo puede actuar como cliente de una encapsulación UDP. Es decir, sólo puede *iniciar* tráfico encapsulado UDP.

Los gráficos que figuran a continuación muestran el formato de un paquete ESP encapsulado mediante UDP en modalidad de túnel:

**Datagrama IPv4 original:**


**Después de aplicar IPSec ESP en modalidad de túnel:**


**Después de aplicar la encapsulación UDP:**


Los gráficos que figuran a continuación muestran el formato de un paquete ESP encapsulado UDP en modalidad de transporte:

**Datagrama IPv4 original:**


**Después de aplicar IPSec ESP en modalidad de transporte:**


**Después de aplicar la encapsulación UDP:**


Una vez que el paquete se ha encapsulado, el sistema lo envía a su VPN asociada a través del puerto UDP 4500. Normalmente, las VPN asociadas realizan las negociaciones IKE a través del puerto 500. No obstante, cuando IKE detecta NAT durante la negociación de claves, los paquetes IKE posteriores se envían a través del puerto origen 4500, puerto destino 4500. Esto también significa que el puerto 4500 no puede estar restringido por ninguna norma de filtro aplicable. El terminal receptor de la conexión puede determinar si el paquete es un paquete IKE o un paquete encapsulado UDP debido a que los 4 primeros bytes de la carga útil de UDP se establecen en cero en un paquete IKE. Para que funcione correctamente, ambos terminales de la conexión deben soportar la encapsulación UDP.

**Conceptos relacionados**:

"Escenario: VPN compatible con el cortafuegos" en la página 35
En este escenario, una gran empresa de seguros desea establecer una VPN entre una pasarela en Chicago y un host en Minneapolis, donde ambas redes están detrás de un cortafuegos.

## Compresión de IP

El protocolo de Compresión de la carga útil IP (IPComp) reduce el tamaño de los datagramas IP comprimiéndolos para incrementar el rendimiento de la comunicación entre dos asociados.

El objetivo es aumentar el rendimiento de la comunicación general cuando ésta se produce a través de enlaces lentos o congestionados. IPComp no ofrece ninguna seguridad y debe utilizarse junto con una transformación AH o ESP cuando la comunicación se produce a través de una conexión VPN.

IETF (Internet Engineering Task Force IETF) define formalmente IPComp en la RFC (Request for Comments) 2393, *IP Protocolo de compresión de carga útil (IPComp)*. Puede visualizar esta RFC en Internet, en el siguiente sitio Web: http://www.rfc-editor.org.

**Información relacionada**:

http://www.rfc-editor.org

## VPN y filtrado IP

El filtrado IP y VPN están estrechamente relacionados. De hecho, la mayoría de conexiones VPN requieren normas de filtro para funcionar correctamente. Este tema proporciona información acerca de los filtros necesarios para VPN, y también acerca de otros conceptos de filtrado relacionados con VPN.

La mayoría de conexiones VPN requieren normas de filtro para funcionar correctamente. Las normas de filtro necesarias dependen del tipo de conexión VPN que esté configurando y del tipo de tráfico que desee controlar. En general, cada conexión tendrá un filtro de políticas. El filtro de políticas define qué direcciones, protocolos y puertos pueden utilizar la VPN. Además, las conexiones que soportan el

protocolo IKE (intercambio de claves de Internet) tienen generalmente normas escritas explícitamente para permitir el proceso IKE a través de la conexión. VPN puede generar estas normas automáticamente. Siempre que sea posible, permita que VPN genere los filtros de políticas automáticamente. Esto no sólo ayudará a eliminar errores, sino que también eliminará la necesidad de configurar las normas como un paso independiente mediante el editor de normas de paquetes de IBM Navigator for i.

Por supuesto, existen excepciones. Consulte los temas siguientes para obtener información acerca de otros conceptos y técnicas menos comunes del filtrado y de VPN que pueden aplicarse a su situación particular:

**Conceptos relacionados**:

"Configuración de normas de paquetes VPN" en la página 57
Si está creando una conexión por primera vez, permita que VPN genere automáticamente las normas de paquetes VPN. Puede llevarlo a cabo utilizando el asistente Nueva conexión o las páginas de propiedades de VPN para configurar la conexión.

## Conexiones VPN sin filtros de políticas

Si los puntos finales de conexión de la VPN son direcciones IP específicas y simples y desea iniciar la VPN sin tener que escribir ni activar normas de filtro en el sistema, puede configurar un filtro de políticas dinámico.

Una norma de filtro de políticas define qué direcciones, protocolos y puertos puede utilizar una VPN y dirige el tráfico apropiado a través de la conexión. En algunos casos, puede que desee configurar una conexión que no requiera una norma de filtro de políticas. Por ejemplo, puede que tenga normas de paquetes que no son de VPN cargadas en la interfaz que la conexión VPN va a utilizar, y por tanto, en lugar de desactivar las normas activas en esa interfaz, decide configurar la VPN de forma que el sistema gestione todos los filtros dinámicamente para la conexión. El filtro de políticas para este tipo de conexión se conoce como **filtro de políticas dinámico**. Para poder utilizar un filtro de políticas dinámico para la conexión VPN, deben cumplirse la totalidad de las siguientes condiciones:

- Sólo el sistema local puede iniciar la conexión.
- Los puntos finales de datos de la conexión deben ser sistemas únicos. Es decir, no pueden ser una subred ni un rango de direcciones.
- No puede cargarse ninguna norma de filtro de políticas para la conexión.

Si la conexión cumple estos criterios, puede configurarla para que no requiera un filtro de políticas. Cuando se inicie la conexión, el tráfico entre los puntos finales de datos fluirá a través de ella independientemente de que haya otras normas de paquetes cargadas en el sistema.

Para obtener instrucciones paso a paso acerca de cómo configurar una conexión para que no requiera un filtro de políticas, consulte la ayuda en línea de VPN.

## IKE implícito

Para que se produzcan negociaciones de intercambio de claves de Internet (IKE) para la VPN, debe permitir el tráfico IP de los datagramas UDP a través del puerto 500. Sin embargo, si en el sistema no existen normas de filtro específicamente escritas para permitir el tráfico IKE, el sistema permitirá implícitamente el flujo de tráfico IKE.

Para establecer una conexión, la mayoría de las VPN requieren que se produzcan negociaciones IKE para que pueda producirse el proceso IPSec. IKE utiliza el puerto conocido 500 y, por tanto, para que IKE funcione correctamente, debe permitir el tráfico IP de los datagramas UDP a través del puerto 500. Si en el sistema no existen normas de filtro específicamente escritas para permitir el tráfico IKE, el tráfico IKE se permite implícitamente. Sin embargo, las normas escritas específicamente para el tráfico del puerto 500 de UDP se manejan en función de lo definido en las normas de filtro activas.

# Escenarios: VPN

Revise estos escenarios para familiarizarse con los detalles técnicos y de configuración relacionados con cada uno de estos tipos de conexión básica.

**Conceptos relacionados**:

Escenario de QoS: resultados seguros y previsibles (VPN y QoS)

**Información relacionada**:

OS/400 V5R1 Virtual Private Networks: Remote Access to the IBM e(logo)server iSeries Server with Windows 2000 VPN Clients, REDP0153

AS/400 Internet Security: Implementing AS/400 Virtual Private Networks, SG24-5404-00

AS/400 Internet Security Scenarios: A Practical Approach, SG24-5954-00

# Escenario: conexión básica entre sucursales

En este escenario, su empresa desea establecer una VPN entre las subredes de dos departamentos remotos a través de un par de modelos IBM i que actúan como pasarelas VPN.

## Situación

Supongamos que su empresa desea minimizar los costes de comunicación entre sus propias sucursales. Actualmente, su empresa utiliza frame relay o líneas alquiladas, pero desea explorar otras posibilidades de transmisión de datos confidenciales internos que resulte menos costosa, más segura y globalmente accesible. Sacando partido a Internet, puede establecer fácilmente una red privada virtual (VPN) que satisfaga las necesidades de su empresa.

Su empresa y su sucursal precisan de una protección VPN en Internet, pero no en sus respectivas intranets. Debido a que considera fiables las intranets, la mejor solución es crear una VPN de pasarela a pasarela. En este caso, ambas pasarelas están conectadas directamente a la red de intervención. En otras palabras, son sistemas de *frontera* o *borde*, que no están protegidos mediante un cortafuegos. Este ejemplo sirve como introducción útil a los pasos que conlleva establecer una configuración de VPN básica. Cuando el escenario hace referencia al término *Internet*, alude a la red de intervención existente entre dos pasarelas VPN, que podría ser la propia red privada de la empresa o la Internet pública.

**Importante:** Este escenario muestra las pasarelas de seguridad del modelo IBM i conectadas directamente a Internet. Se ha prescindido de un cortafuegos para simplificar el escenario. Esto no implica que el empleo de un cortafuegos sea innecesario. De hecho, deberá considerar los riesgos de seguridad que supone cualquier conexión a Internet.

## Ventajas

Este escenario comporta las siguientes ventajas:

- La utilización de Internet o una intranet existente reduce el coste de las líneas privadas entre subredes remotas.
- La utilización de Internet o una intranet existente reduce la complejidad que comporta la instalación y mantenimiento de líneas privadas y el equipo asociado.
- La utilización de Internet permite conectar las ubicaciones remotas prácticamente a cualquier otro lugar del mundo.
- La utilización de la VPN ofrece a los usuarios acceso a todos los sistemas y recursos de ambos lados de la conexión de la misma forma que si estuvieran utilizando una línea alquilada o una conexión WAN (red de área amplia).
- La utilización de un cifrado estándar y de métodos de autenticación asegura una protección de la información delicada que pasa de una ubicación a otra.

- El intercambio de las claves cifradas de forma dinámica y regular simplifica la configuración y minimiza el riesgo de que éstas puedan descodificarse y que pueda violarse la seguridad.
- La utilización de direcciones IP privadas en cada subred remota hace innecesario asignar a cada cliente valiosas direcciones públicas de IP.

## Objetivos

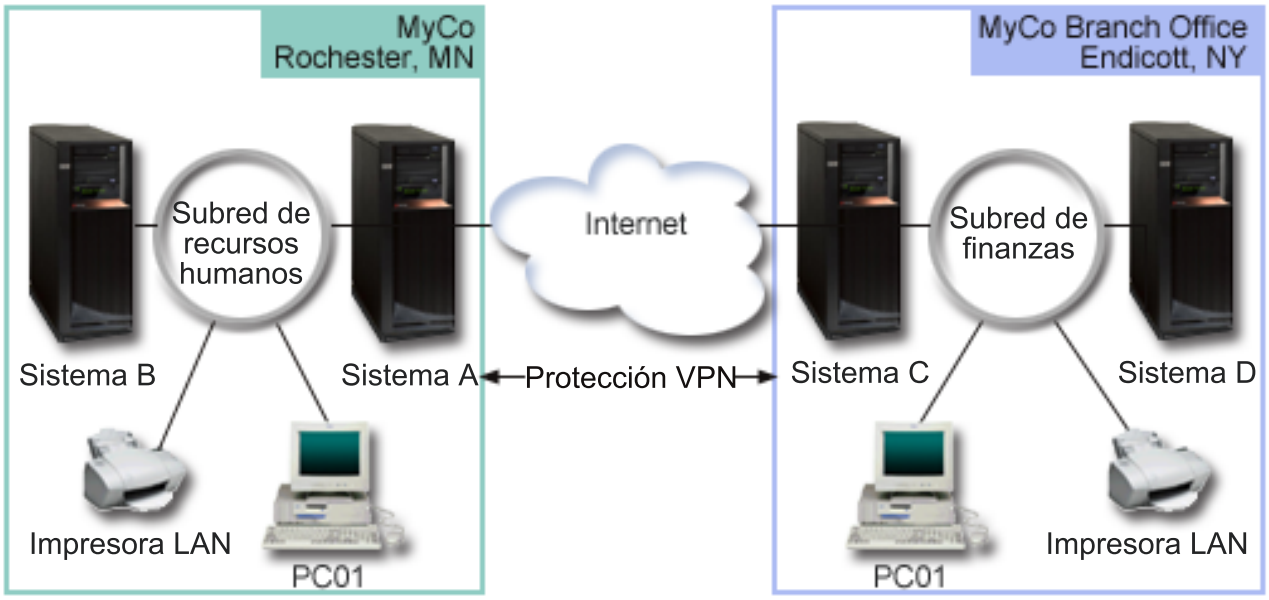
En este escenario, MyCo, Inc. desea establecer una VPN entre las subredes de sus departamentos de Recursos Humanos y Finanzas mediante un par de modelos IBM i. Ambos sistemas actuarán como pasarelas de VPN. En términos de configuraciones de VPN, una pasarela realiza la gestión de claves y aplica IPSec a los datos que fluyen por el túnel. Las pasarelas no son los puntos finales de datos de la conexión.

Los objetivos de este escenario son los siguientes:

- La VPN debe proteger todo el tráfico de datos entre la subred del departamento de Recursos Humanos y la subred del departamento de Finanzas.
- El tráfico de datos no necesita protección VPN una vez ha llegado a la subred de alguno de los departamentos.
- Todos los clientes y hosts de cada red tienen acceso total a la red de los demás, incluyendo todas las aplicaciones.
- Los sistemas de la pasarela pueden comunicarse entre sí y acceder a las aplicaciones del otro.

## Detalles

La siguiente ilustración muestra las características de la red de MyCo.




**Departamento de Recursos Humanos**

- El Sistema A actúa como pasarela VPN del Departamento de Recursos Humanos.
- La subred es 10.6.0.0 con la máscara 255.255.0.0. Esta subred representa el punto final de datos a través del túnel de la VPN del sitio de MyCo en Rochester.
- El sistema A se conecta a Internet mediante la dirección IP 204.146.18.227. Este es el punto final de conexión. Es decir, el sistema A realiza la gestión de claves y aplica IPSec a los datagramas IP entrantes y salientes.

- El sistema A se conecta a la subred con la dirección IP 10.6.11.1.
- El sistema B es un sistema de producción de la subred de Recursos Humanos que ejecuta aplicaciones TCP/IP estándares.

**Departamento de Finanzas**

- El Sistema C actúa como pasarela VPN del Departamento de Finanzas.
- La subred es 10.196.8.0 con la máscara 255.255.255.0. Esta subred representa el punto final de datos a través del túnel de la VPN del sitio de MyCo en Endicott.
- El sistema C se conecta con Internet mediante la dirección IP 208.222.150.250. Este es el punto final de conexión. Es decir, el sistema C realiza la gestión de claves y aplica IPSec a los datagramas IP entrantes y salientes.
- El sistema C se conecta a la subred con la dirección IP 10.196.8.5.

## Tareas de configuración

Debe completar cada una de estas tareas para configurar la conexión entre sucursales que se ha descrito en este escenario:

**Nota:** Antes de iniciar estas tareas, verifique el direccionamiento de TCP/IP para asegurar que los sistemas de ambas pasarelas pueden comunicarse entre sí a través de Internet. Con esto se asegura de que los hosts de cada subred efectúen el direccionamiento correctamente hacia las pasarelas respectivas para poder acceder a la subred remota.

**Conceptos relacionados**:

Direccionamiento de TCP/IP y equilibrio de cargas de trabajo

**Información relacionada**:

AS/400 Internet Security Scenarios: A Practical Approach, SG24-5954-00

## Cómo completar las hojas de trabajo de planificación

Las listas de comprobación de planificación ilustran el tipo de información que necesita para empezar a configurar la VPN. Todas las respuestas de la lista de comprobaciones de los prerrequisitos deben ser SÍ antes de poder proseguir con la configuración de la VPN.

**Nota:** Estas hojas de trabajo son aplicables al sistema A; repita el proceso para el sistema C, invirtiendo las direcciones IP de la forma necesaria.

*Tabla 1. Requisitos del sistema*

| Lista de comprobación de los prerrequisitos | Respuestas |
|---|---|
| ¿Está instalada la opción Digital Certificate Manager? | Sí |
| ¿Se ha iniciado el servidor HTTP (para dar soporte a IBM Navigator for i)? | Sí |
| ¿Está instalado IBM TCP/IP Connectivity Utilities para i? | Sí |
| ¿Ha establecido en 1 el valor del sistema de retener datos de seguridad del servidor (QRETSVRSEC *SEC)? | Sí |
| ¿Está configurado TCP/IP en el sistema (incluyendo las interfaces IP, rutas IP, el nombre del host local IP y el nombre de dominio local IP)? | Sí |
| ¿Se ha establecido la comunicación normal TCP/IP entre los puntos finales? | Sí |
| ¿Ha aplicado los últimos arreglos temporales de programa (PTF)? | Sí |
| Si el túnel de la VPN atraviesa los cortafuegos o direccionadores que utilizan el filtrado de paquetes IP, ¿soportan las normas de filtro del cortafuegos o direccionador los protocolos AH y ESP? | Sí |
| ¿Están configurados los cortafuegos o los direccionadores para permitir los protocolos IKE (UDP puerto 500), AH y ESP? | Sí |

*Tabla 1. Requisitos del sistema (continuación)*

| Lista de comprobación de los prerrequisitos | Respuestas |
|---|---|
| ¿Están configurados los cortafuegos para habilitar el reenvío de IP? | Sí |

*Tabla 2. Configuración de VPN*

| Necesita esta información para configurar la VPN | Respuestas |
|---|---|
| ¿Qué tipo de conexión está creando? | de pasarela a pasarela |
| ¿Cómo se denominará el grupo de claves dinámicas? | HRgw2FINgw |
| ¿Qué tipo de seguridad y rendimiento del sistema necesita para proteger las claves? | equilibrado |
| ¿Utiliza certificados para autenticar la conexión? Si no es así, ¿cuál es la clave precompartida? | No topsecretstuff |
| ¿Cuál es el identificador del servidor de claves local? | Dirección IP: 204.146.18.227 |
| ¿Cuál es el identificador del punto final de datos local? | Subred: 10.6.0.0<br>Máscara: 255.255.0.0 |
| ¿Cuál es el identificador del servidor de claves remoto? | Dirección IP: 208.222.150.250 |
| ¿Cuál es el identificador del punto final de datos remoto? | Subred: 10.196.8.0<br>Máscara: 255.255.255.0 |
| ¿Qué puertos y protocolos desea permitir fluir a través de la conexión? | Cualquiera |
| ¿Qué tipo de seguridad y rendimiento del sistema necesita para proteger sus datos? | equilibrado |
| ¿A qué interfaces se aplica la conexión? | TRLINE |

## Configuración de VPN en el sistema A

Complete estas tareas para configurar el sistema A

Utilice los siguientes pasos y la información de sus hojas de trabajo para configurar la VPN en el sistema A:

1. En IBM Navigator for i, expanda **Red** > **Políticas IP** > **Red privada virtual**.
2. Pulse **Conexiones seguras** para abrir el panel **Conexiones**.
3. Pulse **Acciones** > **Conexión nueva** para iniciar el asistente Conexión nueva.
4. Revise la página de **Bienvenida** para obtener información acerca de los objetos que crea el asistente.
5. Pulse **Siguiente** para ir a la página **Nombre de la conexión**.
6. En el campo **Nombre**, especifique `HRgw2FINgw`.
7. Opcional: Especifique una descripción para este grupo de conexión.
8. Pulse **Siguiente** para ir a la página **Escenario de la conexión**.
9. Seleccione **Conectar su pasarela a otra pasarela**.
10. Pulse **Siguiente** para ir a la página **Política de intercambio de claves de Internet**.
11. Seleccione **Crear una nueva política** y, a continuación, seleccione **Equilibrar seguridad y rendimiento**.
12. Pulse **Siguiente** para ir a la página **Certificado para punto final de conexión local**.
13. Seleccione **No** para indicar que no utilizará certificados para autenticar la conexión.
14. Pulse **Siguiente** para ir a la página **Servidor de claves local**.
15. Seleccione **Dirección IP de Versión 4** en el campo **Tipo de identificador**.
16. Seleccione `204.146.18.227` en el campo **Dirección IP**.
17. Pulse **Siguiente** para ir a la página **Servidor de claves remoto**.

18. Seleccione **Dirección IP de Versión 4** en el campo **Tipo de identificador**.
19. Especifique `208.222.150.250` en el campo **Identificador**.
20. Especifique `topsecretstuff` en el campo **Clave precompartida**.
21. Pulse **Siguiente** para ir a la página **Punto final de datos local**.
22. Seleccione **Subred IP versión 4** en el campo **Tipo de identificador**.
23. Especifique `10.6.0.0` en el campo **Identificador**.
24. Especifique `255.255.0.0` en el campo **Máscara de subred**.
25. Pulse **Siguiente** para ir a la página **Punto final de datos remoto**.
26. Seleccione **Subred IP versión 4** en el campo **Tipo de identificador**.
27. Especifique `10.196.8.0` en el campo **Identificador**.
28. Especifique `255.255.255.0` en el campo **Máscara de subred**.
29. Pulse **Siguiente** para ir a la página **Servicios de datos**.
30. Acepte los valores predeterminados y, a continuación, pulse **Siguiente** para ir a la página **Política de datos**.
31. Seleccione **Crear una nueva política** y, a continuación, seleccione **Equilibrar seguridad y rendimiento**.
32. Pulse **Siguiente** para ir a la página **Interfaces aplicables**.
33. Seleccione **TRLINE** en la tabla **Línea**.
34. Pulse **Siguiente** para ir a la página **Resumen**. Revise los objetos que creará el asistente para asegurar que son correctos.
35. Pulse **Finalizar** para completar la configuración.
36. Cuando aparezca el panel **Activar filtros de políticas**, seleccione **Si, activar los filtros de política generados** y, a continuación, seleccione **Permitir el resto de tráfico**.
37. Pulse **Aceptar** para completar la configuración. Cuando se le solicite, especifique que desea activar las normas en todas las interfaces.

**Tareas relacionadas**:

"Configuración de VPN en el sistema C"
Siga los mismos pasos que para configurar VPN en el sistema A y cambie las direcciones IP según corresponda. Utilice las hojas de trabajo de planificación como guía.

## Configuración de VPN en el sistema C

Siga los mismos pasos que para configurar VPN en el sistema A y cambie las direcciones IP según corresponda. Utilice las hojas de trabajo de planificación como guía.

Cuando termine de configurar la pasarela VPN del departamento de finanzas, el estado de las conexiones será *bajo petición*, lo que significa que la conexión se inicia cuando se envían los datagramas IP que esta conexión VPN debe proteger. El próximo paso consiste en iniciar los servidores VPN, si aún no lo están.

**Tareas relacionadas**:

"Configuración de VPN en el sistema A" en la página 21
Complete estas tareas para configurar el sistema A

## Inicio de VPN

Una vez configurada la conexión VPN en el sistema A y C, debe iniciarla.

Para iniciar la VPN, siga estos pasos:

1. En IBM Navigator for i, expanda **Red** > **Todas las tareas** > **Políticas IP** > **Red privada virtual**.
2. Pulse **Iniciar servidor VPN**.

### Prueba de una conexión

Tras haber finalizado la configuración de ambos sistemas y haber iniciado satisfactoriamente los servidores VPN, pruebe la conectividad para asegurarse de que las subredes remotas pueden comunicarse entre sí.

Para probar la conexión, siga estos pasos:

1. En IBM Navigator for i, expanda **Red** > **Todas las tareas** > **Configuración TCP/IP**.
2. Pulse **Trabajar con Ping**.
3. En el panel **Ping**, especifique `System C` en el campo **Dirección IP o nombre de host**.
4. Pulse **Realizar PING ahora** para verificar la conectividad del sistema A con el sistema C.
5. Pulse **Aceptar** cuando haya finalizado.

## Escenario: conexión básica de empresa a empresa

En este escenario, su empresa desea establecer una VPN entre una estación de trabajo cliente de la división de fabricación y una estación de trabajo cliente del departamento de suministros de un socio comercial.

### Situación

Suponga que es el principal proveedor de un fabricante. Puesto que es decisivo que disponga de los componentes y cantidades específicos en el preciso momento en que la empresa fabricante los necesite, tendrá que conocer siempre el estado del inventario del fabricante y de planificación de la producción. Es posible actualmente que lleve a cabo esta interacción de forma manual y considere que resulta lenta, costosa e incluso inexacta. Desea encontrar una forma más fácil, rápida y efectiva para comunicarse con su empresa fabricante. Sin embargo, debido a la confidencialidad y a la naturaleza sensible en el tiempo de la información que intercambia, el fabricante no desea publicarla en el sitio Web de su empresa o distribuirlo mensualmente en un informe externo. Sacando partido a Internet, puede establecer fácilmente una VPN que satisfaga las necesidades de ambas empresas.

### Objetivos

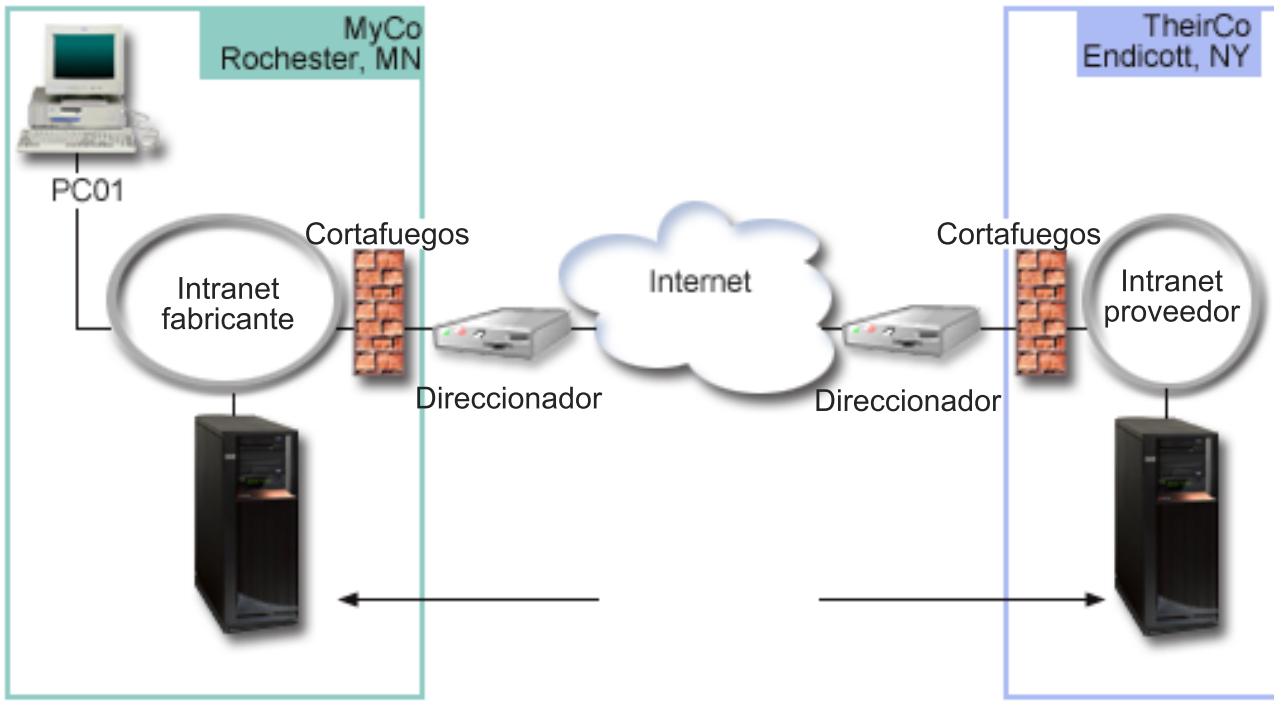
En este escenario, MyCo desea establecer una VPN entre un host de su división de componentes y un host del departamento de manufactura de uno de sus socios comerciales, TheirCo.

Debido a que la información que comparten ambas empresas es altamente confidencial, ésta debe protegerse mientras circula por Internet. Además, los datos no deben fluir como texto legible dentro de las redes de las dos empresas ya que cada una de ellas no considera a la otra de confianza. En otras palabras, ambas empresas necesitan autenticación, integridad y cifrado de extremo a extremo.

**Importante:** La intención de este escenario es introducir, mediante ejemplos, una configuración de VPN simple de host a host. En un entorno de red habitual, también necesitará considerar la configuración de un cortafuegos, los requisitos para la obtención de direcciones IP y el direccionamiento, entre otros.

## Detalles

La siguiente ilustración muestra las características de la red de MyCo y TheirCo:




**Red de suministro de MyCo**

- El sistema A tiene una dirección IP de 10.6.1.1. Este es el punto final de conexión, así como el punto final de datos. Es decir, el sistema A realiza negociaciones IKE y aplica IPsec a los datagramas IP entrantes y salientes y, asimismo, es el origen y destino de los datos que fluyen por la VPN.
- El sistema A se encuentra en la subred 10.6.0.0 con la máscara 255.255.0.0
- Sólo el sistema A puede iniciar la conexión con el sistema C.

**Red de manufactura de TheirCo**

- El sistema C tiene una dirección IP de 10.196.8.6. Este es el punto final de conexión, así como el punto final de datos. Es decir, el sistema C realiza negociaciones IKE y aplica IPsec a los datagramas IP entrantes y salientes y, asimismo, es el origen y destino de los datos que fluyen por la VPN.
- El sistema C se encuentra en la subred 10.196.8.0 con la máscara 255.255.255.0

## Tareas de configuración

Debe completar cada una de estas tareas para configurar la conexión de empresa a empresa descrita en este escenario:

**Nota:** Antes de iniciar estas tareas, verifique el direccionamiento de TCP/IP para asegurar que los sistemas de ambas pasarelas pueden comunicarse entre sí a través de Internet. Con esto se asegura de que los hosts de cada subred efectúen el direccionamiento correctamente hacia las pasarelas respectivas para poder acceder a la subred remota.

**Conceptos relacionados**:

Direccionamiento de TCP/IP y equilibrio de cargas de trabajo

## Cómo completar las hojas de trabajo de planificación

Las listas de comprobación de planificación ilustran el tipo de información que necesita para empezar a configurar la VPN. Todas las respuestas de la lista de comprobaciones de los prerrequisitos deben ser SÍ antes de poder proseguir con la configuración de la VPN.

**Nota:** Estas hojas de trabajo son aplicables al sistema A; repita el proceso para el sistema C, invirtiendo las direcciones IP de la forma necesaria.

*Tabla 3. Requisitos del sistema*

| **Lista de comprobación de los prerrequisitos** | **Respuestas** |
|---|---|
| ¿Está instalada la opción Digital Certificate Manager? | Sí |
| ¿Se ha iniciado el servidor HTTP (para dar soporte a IBM Navigator for i)? | Sí |
| ¿Está instalado IBM TCP/IP Connectivity Utilities para i? | Sí |
| ¿Ha establecido en 1 el valor del sistema de retener datos de seguridad del servidor (QRETSVRSEC *SEC)? | Sí |
| ¿Está configurado TCP/IP en el sistema (incluyendo las interfaces IP, rutas IP, el nombre del host local IP y el nombre de dominio local IP)? | Sí |
| ¿Se ha establecido la comunicación normal TCP/IP entre los puntos finales? | Sí |
| ¿Ha aplicado los últimos arreglos temporales de programa (PTF)? | Sí |
| Si el túnel de la VPN atraviesa los cortafuegos o direccionadores que utilizan el filtrado de paquetes IP, ¿soportan las normas de filtro del cortafuegos o direccionador los protocolos AH y ESP? | Sí |
| ¿Están configurados los cortafuegos o los direccionadores para permitir los protocolos IKE (UDP puerto 500), AH y ESP? | Sí |
| ¿Están configurados los cortafuegos para habilitar el reenvío de IP? | Sí |

*Tabla 4. Configuración de VPN*

| **Necesita esta información para configurar la VPN** | **Respuestas** |
|---|---|
| ¿Qué tipo de conexión está creando? | de pasarela a pasarela |
| ¿Cómo se denominará el grupo de claves dinámicas? | HRgw2FINgw |
| ¿Qué tipo de seguridad y rendimiento del sistema necesita para proteger las claves? | equilibrado |
| ¿Utiliza certificados para autenticar la conexión? Si no es así, ¿cuál es la clave precompartida? | No topsecretstuff |
| ¿Cuál es el identificador del servidor de claves local? | Dirección IP: 204.146.18.227 |
| ¿Cuál es el identificador del punto final de datos local? | Subred: 10.6.0.0<br>Máscara: 255.255.0.0 |
| ¿Cuál es el identificador del servidor de claves remoto? | Dirección IP: 208.222.150.250 |
| ¿Cuál es el identificador del punto final de datos remoto? | Subred: 10.196.8.0<br>Máscara: 255.255.255.0 |
| ¿Qué puertos y protocolos desea permitir fluir a través de la conexión? | Cualquiera |
| ¿Qué tipo de seguridad y rendimiento del sistema necesita para proteger sus datos? | equilibrado |
| ¿A qué interfaces se aplica la conexión? | TRLINE |

## Configuración de VPN en el sistema A

Complete estos pasos para configurar una conexión VPN en el sistema A.

Utilice la información de sus hojas de trabajo de planificación para configurar la VPN en el sistema A de la forma siguiente:

1. En IBM Navigator for i, expanda **Red** > **Políticas IP** > **Red privada virtual**.
2. Pulse **Conexiones seguras** para abrir el panel **Conexiones**.
3. Pulse **Acciones** > **Conexiones nuevas** para iniciar el asistente Conexión nueva.
4. Revise la página de **Bienvenida** para obtener información acerca de los objetos que crea el asistente.
5. Pulse **Siguiente** para ir a la página **Nombre de la conexión**.
6. En el campo **Nombre**, especifique `MyCo2TheirCo`.
7. Opcional: Especifique una descripción para este grupo de conexión.
8. Pulse **Siguiente** para ir a la página **Escenario de la conexión**.
9. Seleccione **Conectar su host a otro host**.
10. Pulse **Siguiente** para ir a la página **Política de intercambio de claves de Internet**.
11. Seleccione **Crear una nueva política** y, a continuación, seleccione **Máxima seguridad, mínimo rendimiento**.
12. Pulse **Siguiente** para ir a la página **Certificado para punto final de conexión local**.
13. Seleccione **Sí** para indicar que utilizará certificados para autenticar la conexión. A continuación, seleccione el certificado que representa el sistema A.

    **Nota:** Si desea utilizar un certificado para autenticar el punto final de conexión local, debe, en primer lugar crear el certificado en Digital Certificate Manager (DCM).
14. Pulse **Siguiente** para ir a la página **Servidor de claves remoto**.
15. Seleccione **Dirección IP de Versión 4** en el campo **Tipo de identificador**.
16. Especifique `10.196.8.6` en el campo **Identificador**.
17. Pulse **Siguiente** para ir a la página **Servicios de datos**.
18. Acepte los valores predeterminados y, a continuación, pulse **Siguiente** para ir a la página **Política de datos**.
19. Seleccione **Crear una nueva política** y, a continuación, seleccione **Máxima seguridad, mínimo rendimiento**.
20. Pulse **Siguiente** para ir a la página **Interfaces aplicables**.
21. Seleccione **TRLINE**.
22. Pulse **Siguiente** para ir a la página **Resumen**. Revise los objetos que creará el asistente para asegurar que son correctos.
23. Pulse **Finalizar** para completar la configuración.
24. Cuando aparezca el recuadro de diálogo **Activar filtros de políticas**, seleccione **No, las normas de paquetes se activarán más tarde** y, a continuación, pulse **Aceptar**.

El siguiente paso es especificar que únicamente el sistema A puede iniciar esta conexión. Para ello, personalice las propiedades del grupo de claves dinámicas, MyCo2TheirCo, que el asistente ha creado:

1. Pulse **Por grupo** en el panel izquierdo de la interfaz VPN; el nuevo grupo de claves dinámicas, MyCo2TheirCo, se visualizará en el panel derecho. Púlselo con el botón derecho del ratón y seleccione **Propiedades**.
2. Vaya a la página **Política** y seleccione la opción **El sistema local inicia la conexión**.
3. Pulse **Aceptar** para guardar los cambios.

## Configuración de VPN en el sistema C

Siga los mismos pasos que para configurar VPN en el sistema A y cambie las direcciones IP según corresponda. Utilice las hojas de trabajo de planificación como guía.

Cuando termine de configurar la pasarela VPN del departamento de finanzas, el estado de las conexiones será *bajo petición*, lo que significa que la conexión se inicia cuando se envían los datagramas IP que esta conexión VPN debe proteger. El próximo paso consiste en iniciar los servidores VPN, si aún no lo están.

## Activación de las normas de paquetes

El asistente de VPN crea automáticamente las normas de paquetes que la conexión requiere para funcionar adecuadamente. Sin embargo, deberá activarlas en ambos sistemas antes de poder iniciar la conexión VPN.

Para activar las normas de paquetes en el sistema A, siga estos pasos:

1. En IBM Navigator for i, expanda **Red** > **Políticas IP**.
2. Pulse **Reglas de paquete** para abrir el panel Reglas de paquete.
3. Pulse **Acciones** y, a continuación, pulse **Activar reglas...**. De esta forma, se abrirá el panel **Activar reglas de paquete**.
4. Seleccione si desea activar sólo las reglas generadas por VPN, sólo los archivos seleccionados, o tanto las reglas generadas por VPN como los archivos seleccionados. Puede elegir la última opción (ambos), por ejemplo, si tiene diversas normas PERMIT y DENY que desea forzar en la interfaz, además de las normas generadas por VPN.
5. Seleccione la interfaz en la que desea activar las normas. En este caso, seleccione **Activar estas reglas en todas las interfaces y todos los identificadores de filtro punto a punto**.
6. Pulse **Aceptar** en el recuadro de diálogo para confirmar que desea verificar y activar las normas en la interfaz o interfaces que ha especificado. Después de pulsar Aceptar, el sistema comprueba si existen errores de sintaxis y semántica en las normas e informa de los resultados en una ventana de mensaje situada en la parte inferior del editor.
7. Repita estos pasos para activar las normas de paquetes en el sistema C.

## Inicio de una conexión

Una vez configurada la conexión VPN, debe iniciarla.

Siga estos pasos para configurar la VPN MyCo2TheirCo desde el sistema A:

1. En IBM Navigator for i, expanda **Red** > **Todas las tareas** > **Políticas IP** > **Red privada virtual**.
2. Si el servidor VPN no está iniciado, pulse **Iniciar servidor VPN**. De esta forma, se iniciará el servidor VPN.
3. Expanda **Red** > **Políticas IP** > **Red privada virtual**.
4. Pulse **Conexiones seguras**.
5. Pulse con el botón derecho del ratón **Todas las conexiones** y seleccione **Abrir** para visualizar una lista de conexiones.
6. Pulse con el botón derecho del ratón **MyCo2TheirCo** y seleccione **Iniciar**.
7. Desde el menú **Visualizar**, seleccione **Renovar**. Si la conexión se inicia satisfactoriamente, el estado debe cambiar de *Desocupado* a *Habilitado*. La conexión tardará unos minutos en iniciarse, por lo tanto, renueve periódicamente la visualización hasta que el estado cambie a *Habilitado*.

## Prueba de una conexión

Tras haber finalizado la configuración de ambos sistemas y haber iniciado satisfactoriamente los servidores VPN, pruebe la conectividad para asegurarse de que las subredes remotas pueden comunicarse entre sí.

Para probar la conexión, siga estos pasos:

1. En IBM Navigator for i, expanda **Red** > **Todas las tareas** > **Configuración TCP/IP**.
2. Pulse **Trabajar con Ping**.
3. En el panel **Ping**, especifique `System C` en el campo **Dirección IP o nombre de host**.
4. Pulse **Realizar PING ahora** para verificar la conectividad del sistema A con el sistema C.

5. Pulse **Aceptar** cuando haya finalizado.

## Escenario: protección de un túnel voluntario L2TP con IPSec

En este escenario, aprenderá a configurar una conexión entre el host de una sucursal y una oficina central que utiliza L2TP protegido por IPSec. La sucursal tiene una dirección IP asignada dinámicamente, mientras que la oficina central tiene una dirección IP estática direccionable globalmente.

### Situación

Suponga que su empresa tiene una pequeña sucursal en otro estado. En todo día laboral, la sucursal necesitará tener acceso a información confidencial en un modelo IBM i dentro de la intranet de la empresa. Su empresa actualmente utiliza una costosa línea alquilada para proporcionar a la sucursal el acceso a la red de la empresa. A pesar de que su empresa desea seguir suministrando un acceso seguro a su intranet, desea reducir los gastos relacionados con la línea alquilada. Esto es posible creando un túnel voluntario L2TP (Layer 2 Tunnel Protocol) que extienda su red corporativa, de forma que la sucursal parezca parte de la subred de su empresa. VPN protege el tráfico de datos a través del túnel L2TP.

Mediante un túnel voluntario L2TP, la sucursal remota establece un túnel directamente con el servidor de red L2TP (LNS) de la red corporativa. La funcionalidad del concentrador de acceso L2TP (LAC) reside en el cliente. El túnel es transparente para el proveedor de servicios de Internet (ISP) del cliente, o sea que ya no se necesita el ISP para soportar L2TP. Si desea conocer mejor los conceptos de L2TP, consulte Layer 2 Tunnel Protocol (L2TP).

**Importante:** Este escenario muestra las pasarelas de seguridad conectadas directamente a Internet. Se ha prescindido de un cortafuegos para simplificar el escenario. Esto no implica que el empleo de un cortafuegos sea innecesario. De hecho, deberá considerar los riesgos de seguridad que supone cualquier conexión a Internet.

### Objetivos

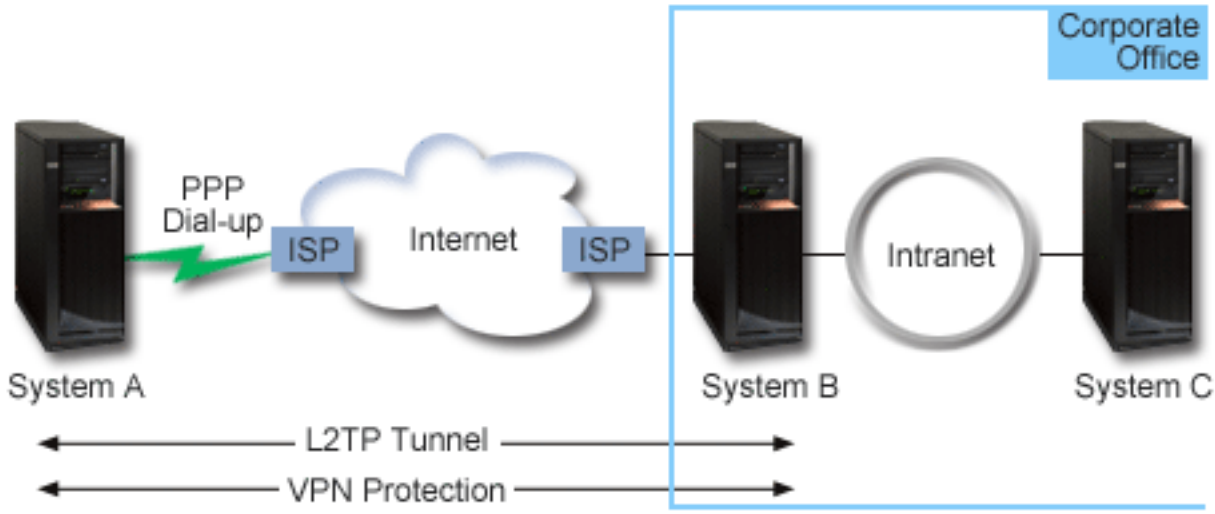
En este escenario, el sistema de una sucursal se conecta con su red corporativa mediante un sistema de pasarela con un túnel L2TP protegido por VPN.

Los objetivos principales de este escenario son los siguientes:

- El sistema de la sucursal siempre inicia la conexión con la oficina central.
- El sistema de la sucursal es el único sistema de la red de la sucursal que necesita acceso a la red de la empresa. En otras palabras, su rol en la red de la sucursal es de host, no de pasarela.
- El sistema de la oficina central es un host en la red de la empresa.

## Detalles

La siguiente ilustración muestra las características de la red de este escenario:




**Sistema A**

- Debe tener acceso a las aplicaciones TCP/IP de todos los sistemas de la red corporativa.
- Recibe las direcciones IP asignadas dinámicamente a través de su ISP.
- Debe estar configurado para que soporte L2TP.

**Sistema B**

- Debe tener acceso a las aplicaciones TCP/IP del sistema A.
- La subred es 10.6.0.0 con la máscara 255.255.0.0. Esta subred representa el punto final de datos a través del túnel de la VPN en el sitio de la empresa.
- Se conecta con Internet mediante la dirección IP 205.13.237.6. Este es el punto final de conexión. Es decir, el sistema B realiza la gestión de claves y aplica IPSec a los datagramas IP entrantes y salientes. El sistema B se conecta a la subred con la dirección IP 10.6.11.1.

En términos de L2TP, el *Sistema A* actúa como iniciador de L2TP, mientras que el *Sistema B* actúa como terminador de L2TP.

## Tareas de configuración

Presuponiendo que la configuración TCP/IP ya existe y funciona, debe completar las siguientes tareas:

**Conceptos relacionados**:

"Layer 2 Tunnel Protocol" en la página 13
Las conexiones L2TP (Layer 2 Tunneling Protocol), también denominadas líneas virtuales, ofrecen acceso a los usuarios remotos a bajo precio, al permitir que un sistema de red de la empresa gestione las direcciones IP asignadas a sus usuarios remotos. Además, las conexiones L2TP ofrecen un acceso seguro a su sistema o red cuando las utilice conjuntamente con IPSec (IP Security).

**Información relacionada**:

AS/400 Internet Security Scenarios: A Practical Approach, SG24-5954-00

## Configuración de VPN en el sistema A

Complete estos pasos para configurar una conexión VPN en el sistema A.

Utilice la información de sus hojas de trabajo de planificación para configurar la VPN en el sistema A de la forma siguiente:

1. **Configurar la política de intercambio de claves de Internet**
   a. En IBM Navigator for i, expanda **Red** > **Políticas IP** > **Red privada virtual**.
   b. Pulse **Políticas de seguridad IP** para abrir el panel **Políticas de seguridad IP**.
   c. Pulse con el botón derecho del ratón **Políticas de intercambio de claves de Internet** y seleccione **Nueva política de intercambio de claves de Internet**.
   d. En la página **Servidor remoto**, seleccione **Dirección IP versión 4** como tipo de identificador y, a continuación, especifique `205.13.237.6` en el campo **Dirección IP**.
   e. En la página **Asociaciones**, seleccione **Clave precompartida** para indicar que esta conexión utiliza una clave precompartida para autenticar esta política.
   f. Especifique la clave precompartida en el campo **Clave**. Debe tratar la clave precompartida como si fuera una contraseña.
   g. Seleccione el **Identificador de clave** para el tipo de identificador del servidor de claves local y, a continuación, especifique el identificador de clave en el campo **Identificador**. Por ejemplo, `thisisthekeyid`. Recuerde que el servidor de claves local tiene una dirección IP asignada dinámicamente que es imposible de conocer de antemano. El sistema B utiliza este identificador para identificar el sistema A cuando éste inicia una conexión.
   h. En la página **Transformaciones**, pulse **Añadir** para añadir las transformaciones que el sistema A propone al sistema B para proteger las claves y especificar si la política IKE utiliza la protección de identidad al iniciar las negociaciones de fase 1.
   i. En la página **Transformación de política IKE**, seleccione **Clave precompartida** para su método de autenticación, **SHA** para el algoritmo hash y algoritmo PRF, y **3DES-CBC** para el algoritmo de cifrado. Haga caducar las claves IKE y después acepte los valores del grupo Diffie-Hellman.
   j. Pulse **Aceptar** para volver a la página **Transformaciones**.
   k. Seleccione **Negociación de modalidad agresiva de IKE (sin protección de identidad)**.

      **Nota:** Si utiliza claves precompartidas y la negociación de modalidad agresiva juntos en la configuración, seleccione contraseñas oscuras de improbable descubrimiento en los ataques que exploran el diccionario. También es recomendable cambiar periódicamente las contraseñas.
   l. Pulse **Aceptar** para guardar los cambios.
2. **Configurar la política de datos**
   a. En IBM Navigator for i, expanda **Red** > **Políticas IP** > **Red privada virtual**.
   b. Pulse **Políticas de seguridad IP** para abrir el panel **Políticas de seguridad IP**.
   c. Pulse con el botón derecho del ratón en **Políticas de datos** y seleccione **Política de datos nueva**
   d. En la página **General**, especifique el nombre de la política de datos. Por ejemplo, `l2tpremoteuser`.
   e. Vaya a la página **Proposiciones**. Una proposición es una colección de protocolos que utilizan los servidores de claves iniciadores y contestadores para establecer una conexión dinámica entre dos puntos finales. Puede utilizar una sola política de datos en varios objetos de conexión. Sin embargo, no todos los servidores de claves VPN remotos deben tener necesariamente las mismas propiedades de política de datos. Por lo tanto, puede añadir varias propuestas a una política de datos. Para establecer una conexión VPN con un servidor de claves remoto, debe haber como mínimo una propuesta que coincida en la política de datos del iniciador y del contestador.
   f. Pulse **Añadir** para añadir una transformación de política de datos.
   g. Seleccione **Transportar** para la modalidad de encapsulado.
   h. Especifique una fecha de caducidad para la clave.
   i. Pulse la pestaña **Transformaciones**.
   j. Pulse **Añadir** para añadir una transformación. Una transformación define los protocolos, algoritmos de autenticación y algoritmos de cifrado que esta política de datos utiliza durante las negociaciones de la fase 2 de IKE. El iniciador de una conexión envía una o varias proposiciones de política de

datos al contestador. El contestador selecciona una proposición coincidente de su política de seguridad asociada para completar la conexión segura.

k. Pulse **Aceptar** para guardar la transformación.

l. Pulse **Aceptar** para guardar la nueva política de datos.

3. **Configurar el grupo de claves dinámicas**

a. Pulse **Conexiones seguras** bajo la interfaz VPN.

b. Pulse con el botón derecho del ratón **Por grupo** y seleccione **Nuevo grupo de claves dinámicas**.

c. En la página **General**, especifique un nombre para el grupo. Por ejemplo, `l2tptocorp`.

d. Seleccione **Protege un túnel L2TP iniciado localmente**.

e. Para el rol del sistema, seleccione **Ambos sistemas son hosts**.

f. Vaya a la página **Política**. Seleccione la política de datos que creó en el paso **Configurar la política de datos**, `l2tpremoteuser`, en la lista desplegable **Política de datos**.

g. Seleccione **El sistema local inicia la conexión** para indicar que sólo el sistema A puede iniciar las conexiones con el sistema B.

h. Vaya a la página **Conexiones**. Seleccione **Generar la siguiente norma de filtro de políticas para este grupo**. Pulse **Editar** para definir los parámetros del filtro de políticas.

i. En la página **Filtro de políticas - Direcciones locales**, seleccione el **Identificador de clave** para el tipo de identificador.

j. Para el identificador, seleccione el identificador de clave `thisisthekeyid`, que ha definido en la política IKE.

k. Vaya a la página **Filtro de políticas - Direcciones remotas**. Seleccione **Dirección IP versión 4** en la lista desplegable **Tipo de identificador** .

l. Especifique `205.13.237.6` en el campo **Identificador**.

m. Vaya a la página **Filtro de políticas - Servicios**. Especifique `1701` en los campos **Puerto local** y **Puerto remoto**. El puerto 1701 es el puerto conocido públicamente de L2TP.

n. Seleccione **UDP** en la lista desplegable **Protocolo**.

o. Pulse **Aceptar** para volver a la página **Conexiones**.

p. Vaya a la página **Interfaces**. Seleccione todas las líneas o perfiles PPP a las que se aplicará este grupo. Aún no ha creado el perfil PPP para este grupo. Después, necesitará editar las propiedades de este grupo de forma que el grupo se aplique al perfil PPP que creará en el próximo paso.

q. Pulse **Aceptar** para crear el grupo de claves dinámicas, 12ptocorp.

4. **Configurar la conexión de claves dinámicas**

a. En el panel **Conexiones**, pulse con el botón derecho del ratón en **Por grupo** y seleccione **Abrir**. De esta forma se visualizará una lista de todos los grupos de claves dinámicas que ha configurado en el sistema A.

b. Pulse con el botón derecho del ratón **l2tptocorp** y seleccione **Nueva conexión de clave dinámica**.

c. En la página **General**, especifique una descripción opcional para la conexión.

d. Para el servidor de claves remotas, seleccione **Dirección IP versión 4** para el tipo de identificador.

e. Seleccione `205.13.237.6` en la lista desplegable **Dirección IP**.

f. Deseleccione **Iniciar bajo petición**.

g. Vaya a la página **Direcciones locales**. Seleccione **Identificador de clave** para el tipo de identificador y, a continuación, seleccione `thisisthekeyid` en la lista desplegable **Identificador**.

h. Vaya a la página **Direcciones remotas**. Seleccione **Dirección IP versión 4** para el tipo de identificador.

i. Especifique `205.13.237.6` en el campo **Identificador**.

j. Vaya a la página **Servicios**. Especifique `1701` en los campos **Puerto local** y **Puerto remoto**. El puerto 1701 es el puerto conocido públicamente de L2TP.

k. Seleccione **UDP** en la lista desplegable **Protocolo**.

l. Pulse **Aceptar** para crear la conexión de claves dinámicas.

**Tareas relacionadas**:

"Configuración de VPN en el sistema B" en la página 33
Para configurar una conexión VPN en el sistema B, siga los mismos pasos que para configurar una conexión VPN en el sistema A y cambie las direcciones IP y los identificadores según corresponda.

## Configuración de un perfil de conexión PPP y una línea virtual en el sistema A

Ahora que se ha configurado una conexión VPN en el sistema A, debe crear el perfil PPP del sistema A. El perfil PPP no tiene ninguna línea física asociada; en su lugar, utiliza una línea virtual. Esto se debe a que el tráfico PPP atraviesa el túnel L2TP, mientras la VPN protege el túnel L2TP.

Siga estos pasos para crear un perfil de conexión PPP para el sistema A:

1. En IBM Navigator for i, expanda **Red** > **Servicios de acceso remoto**.
2. Pulse con el botón derecho del ratón **Perfiles de conexión de originador** y pulse **Acciones** > **Nuevo perfil**.
3. En la página **Configuración**, seleccione **PPP** para el tipo de protocolo.
4. Para la modalidad, seleccione **L2TP (línea virtual)**.
5. Seleccione **Iniciador bajo petición (túnel voluntario)** en la lista desplegable **Modalidad operativa**.
6. Pulse **Aceptar** para ir a las páginas de propiedades de los perfiles PPP.
7. En la página **General**, especifique un nombre que identifique el tipo y el destino de la conexión. En ese caso, especifique `toCORP`. El nombre que especifique debe ser de 10 caracteres como máximo.
8. Opcional: especifique una descripción para el perfil.
9. Vaya a la página **Conexión**.
10. En el campo **Nombre de línea virtual**, seleccione **tocorp** en la lista desplegable. Recuerde que esta línea no tiene ninguna interfaz física asociada. La línea virtual describe varias características de este perfil PPP; por ejemplo, tamaño máximo de trama, información de autenticación, el nombre de host local, etc. Se abrirá el recuadro de diálogo **Propiedades de línea L2TP**.
11. En la página **General**, especifique una descripción para la línea virtual.
12. Vaya a la página **Autenticación**.
13. En el campo **Nombre de host local**, especifique el nombre del host del servidor de claves local, `SystemA`.
14. Pulse **Aceptar** para guardar la nueva descripción de línea virtual y volver a la página **Conexión**.
15. Especifique la dirección del punto final del túnel remoto, `205.13.237.6`, en el campo **Dirección del punto final del túnel remoto**.
16. Seleccione **Requiere protección IPSec** y seleccione el grupo de claves dinámicas que ha creado en el paso anterior "Configuración de VPN en el sistema A" en la página 29, `l2tptocorp`, en la lista desplegable **Nombre de grupo de conexión**.
17. Vaya a la página **Valores de IPv4 de TCP/IP**.
18. En la sección **Dirección IP local**, seleccione **Asignada por sistema remoto**.
19. En la sección **Dirección IP remota**, seleccione **Utilizar dirección IP fija**. Especifique `10.6.11.1`, que es la dirección IP del sistema remoto en su subred.
20. En la sección de direccionamiento, seleccione **Definir las rutas estáticas adicionales** y pulse **Rutas**. Si el perfil PPP no proporciona información de direccionamiento que ofrezca el perfil PPP, el sistema A sólo podrá alcanzar el punto final del túnel pero ningún otro sistema de la subred 10.6.0.0.
21. Pulse **Añadir** para añadir una entrada de direccionamiento estático.
22. Especifique la subred `10.6.0.0` y la máscara de subred, `255.255.0.0`, para direccionar todo el tráfico 10.6.*.* a través del túnel L2TP.
23. Pulse **Aceptar** para añadir la ruta estática.
24. Vaya a la página **Autenticación** para establecer el nombre y la contraseña de usuario para este perfil PPP.

25. En la sección de identificación del sistema local, seleccione **Permitir que el sistema remoto verifique la identidad de este sistema**.
26. En **Protocolo de autenticación a utilizar**, seleccione **Se requiere contraseña cifrada (CHAP-MD5)**. En la sección de identificación del sistema local, seleccione **Permitir que el sistema remoto verifique la identidad de este sistema**.
27. Especifique el nombre de usuario, `SystemA` y una contraseña.
28. Pulse **Aceptar** para guardar el perfil PPP.
29. Vuelva a escribir la contraseña para confirmarla.

## Aplicación del grupo de claves dinámicas `l2tptocorp` al perfil PPP `toCorp`

Tras haber configurado su perfil de conexión PPP, necesitará volver al grupo de claves dinámicas, `l2tptocorp`, que ha creado y asociarlo con el perfil PPP.

Para asociar el grupo de claves dinámicas con el perfil PPP, siga estos pasos:

1. En IBM Navigator for i, expanda **Red** > **Políticas IP** > **Red privada virtual**.
2. Pulse **Conexiones seguras** para abrir el panel **Conexiones** y pulse con el botón derecho del ratón en **Por grupo** y, a continuación, seleccione **Abrir**.
3. Pulse con el botón derecho del ratón el grupo de claves dinámicas, `l2tptocorp` y seleccione **Propiedades**.
4. Vaya a la página **Interfaces** y seleccione **Aplicar este grupo** para el perfil PPP que creó en "Configuración de un perfil de conexión PPP y una línea virtual en el sistema A" en la página 32, `toCorp`.
5. Pulse **Aceptar** para aplicar `l2tptocorp` al perfil PPP, `toCorp`.

## Configuración de VPN en el sistema B

Para configurar una conexión VPN en el sistema B, siga los mismos pasos que para configurar una conexión VPN en el sistema A y cambie las direcciones IP y los identificadores según corresponda.

Considere estos otros aspectos antes de empezar:

- La identificación del servidor de claves remoto mediante el identificador de clave que especificó para el servidor de claves local en el sistema A. Por ejemplo, `thisisthekeyid`.
- Utilice *exactamente* la misma clave precompartida.
- Asegúrese de que sus transformaciones coinciden con las que ha configurado en el sistema A o las conexiones fallarán.
- No especifique **Protege un túnel L2TP iniciado localmente** en la página **General** del grupo de claves dinámicas.
- El sistema remoto inicia la conexión.
- Especifique que la conexión deberá iniciarse bajo petición.

**Tareas relacionadas**:

"Configuración de VPN en el sistema A" en la página 29
Complete estos pasos para configurar una conexión VPN en el sistema A.

## Configuración de un perfil de conexión PPP y una línea virtual en el sistema B

Ahora que se ha configurado una conexión VPN en el sistema B, debe crear el perfil PPP del sistema B. El perfil PPP no tiene ninguna línea física asociada; en su lugar, utiliza una línea virtual. Esto se debe a que el tráfico PPP atraviesa el túnel L2TP, mientras la VPN protege el túnel L2TP.

Siga estos pasos para crear un perfil de conexión PPP para el sistema B:

1. En IBM Navigator for i, expanda **Red** > **Servicios de acceso remoto**.
2. Pulse **Perfiles de conexión de receptor** para abrir el panel **Perfiles de conexión de receptor** y pulse **Acciones** > **Nuevo perfil**.

3. En la página **Configuración**, seleccione **PPP** para el tipo de protocolo.
4. Para la modalidad, seleccione **L2TP (línea virtual)**.
5. Seleccione **Terminador (servidor de red)** en la lista desplegable **Modalidad operativa**.
6. Pulse **Aceptar** en las páginas de propiedades de los perfiles PPP.
7. En la página **General**, especifique un nombre que identifique el tipo y el destino de la conexión. En ese caso, especifique `tobranch`. El nombre que especifique debe ser de 10 caracteres como máximo.
8. Opcional: especifique una descripción para el perfil.
9. Vaya a la página **Conexión**.
10. Seleccione la dirección IP del punto final del túnel local, 205.13.237.6.
11. En el campo **Nombre de línea virtual**, seleccione **tobranch** en la lista desplegable. Recuerde que esta línea no tiene ninguna interfaz física asociada. La línea virtual describe varias características de este perfil PPP; por ejemplo, tamaño máximo de trama, información de autenticación, el nombre de host local, etc. Pulse **Abrir** junto al campo **Nombre de línea virtual** para abrir el panel **Propiedades de línea L2TP**.
12. En la página **General**, especifique una descripción para la línea virtual.
13. Vaya a la página **Autenticación**.
14. En el campo **Nombre de host local**, especifique el nombre del host del servidor de claves local, `SystemB`.
15. Pulse **Aceptar** para guardar la nueva descripción de línea virtual y volver a la página **Conexión**.
16. Vaya a la página **Valores TCP/IP**.
17. En la sección **Dirección IP local**, seleccione la dirección IP fija del sistema local, 10.6.11.1.
18. En la sección **Dirección IP remota**, seleccione **Agrupación de direcciones** como método para asignar direcciones. Especifique una dirección de inicio y, a continuación, especifique el número de direcciones que pueden asignarse al sistema remoto.
19. Seleccione **Permitir que el sistema remoto acceda a otras redes (reenvío IP)**.
20. Vaya a la página **Autenticación** para establecer el nombre y la contraseña de usuario para este perfil PPP.
21. En la sección de identificación del sistema local, seleccione **Permitir que el sistema remoto verifique la identidad de este sistema**. De esta forma, se abrirá el recuadro de diálogo **Identificación del sistema local**.
22. En **Protocolo de autenticación a utilizar**, seleccione **Se requiere contraseña cifrada (CHAP-MD5)**.
23. Especifique el nombre de usuario, `SystemB` y una contraseña.
24. Pulse **Aceptar** para guardar el perfil PPP.

## Activación de las normas de paquetes

El asistente de VPN crea automáticamente las normas de paquetes que la conexión requiere para funcionar adecuadamente. Sin embargo, deberá activarlas en ambos sistemas antes de poder iniciar la conexión VPN.

Para activar las normas de paquetes en el sistema A, siga estos pasos:

1. En IBM Navigator for i, expanda **Red** > **Políticas IP**.
2. Pulse **Reglas de paquete** para abrir el panel **Reglas de paquete** y pulse **Acciones** > **Activar reglas**. Esta acción abrirá el panel **Activar reglas de paquete**.
3. Seleccione si desea activar sólo las normas generadas por VPN, sólo un archivo seleccionado o ambos. Puede elegir la última opción (ambos), por ejemplo, si tiene diversas normas PERMIT y DENY que desea forzar en la interfaz, además de las normas generadas por VPN.
4. Seleccione la interfaz en la que desea que se activen las reglas. En este caso, seleccione **Activar estas reglas en todas las interfaces y todos los identificadores de filtro punto a punto**.

5. Pulse **Aceptar** en el recuadro de diálogo para confirmar que desea verificar y activar las normas en la interfaz o interfaces que ha especificado. Después de pulsar Aceptar, el sistema comprueba si existen errores de sintaxis y semántica en las normas e informa de los resultados en una ventana de mensaje situada en la parte inferior del editor.
6. Repita estos pasos para activar las normas de paquetes en el sistema B.

## Escenario: VPN compatible con el cortafuegos

En este escenario, una gran empresa de seguros desea establecer una VPN entre una pasarela en Chicago y un host en Minneapolis, donde ambas redes están detrás de un cortafuegos.

### Situación

Supongamos que tiene una gran empresa de seguros de viviendas con base en Minneapolis y que acaba de abrir una sucursal en Chicago. La sucursal de Chicago necesita acceder a la base de datos de clientes de la oficina central de Minneapolis. Desea asegurarse de que la información que se transfiere es segura, ya que la base de datos contiene información confidencial sobre los clientes como, por ejemplo, nombres, direcciones y números de teléfono. Decide conectar las dos oficinas a través de Internet utilizando una red privada virtual (VPN). Las dos oficinas están detrás de un cortafuegos y utilizan la conversión de direcciones de red (NAT) para ocultar las direcciones IP privadas no registradas detrás de un conjunto de direcciones IP registradas. No obstante, las conexiones VPN presentan algunas incompatibilidades bien conocidas con NAT. Una conexión VPN descarta los paquetes enviados a través de un dispositivo NAT, ya que NAT cambia la dirección IP en el paquete, lo que invalida el paquete. No obstante, sí que puede utilizar una conexión VPN con NAT si implementa una encapsulación UDP.

En este escenario, la dirección IP privada de la red de Chicago se coloca en una nueva cabecera IP y se convierte cuando pasa a través del cortafuegos C (vea la imagen siguiente). A continuación, cuando el paquete alcanza el cortafuegos D, convertirá la dirección IP de destino en la dirección IP del sistema E, con lo que el paquete se reenviará al sistema E. Por último, cuando el paquete alcanza el sistema E, elimina la cabecera UDP, dejando el paquete IPSec original, que ahora pasará todas las validaciones y permitirá una conexión VPN segura.

### Objetivos

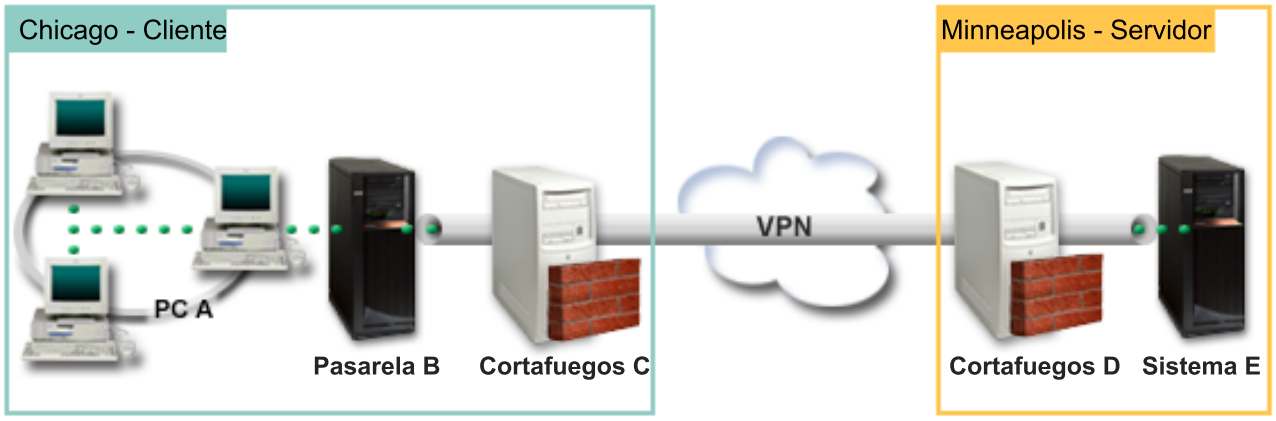
En este escenario, una gran empresa de seguros desea establecer una VPN entre una pasarela en Chicago (Cliente) y un host en Minneapolis (Servidor), donde ambas redes están detrás de un cortafuegos.

Los objetivos de este escenario son los siguientes:

- La pasarela de la sucursal de Chicago siempre inicia la conexión con el host de Minneapolis.
- La VPN debe proteger todo el tráfico de datos entre la pasarela de Chicago y el host de Minneapolis.
- Permitir que todos los usuarios de la pasarela de Chicago accedan a una base de datos IBM i ubicada en la red de Minneapolis a través de una conexión VPN.

## Detalles

La siguiente ilustración muestra las características de la red de este escenario:




**Red de Chicago - Cliente**

- La pasarela B se conecta a Internet con una dirección IP 214.72.189.35 y es el punto final de conexión del túnel de la VPN. La pasarela B realiza negociaciones IKE y aplica la encapsulación UDP a los datagramas IP salientes.
- La pasarela B y el PC A están en la subred 10.8.11.0 con la máscara 255.255.255.0
- El PC A es el origen y el destino de los datos que fluyen a través de la conexión VPN, por lo que es el punto final de datos del túnel de la VPN.
- Sólo la pasarela B puede iniciar la conexión con el sistema E.
- El cortafuegos C tiene una norma NAT Masq con la dirección IP pública 129.42.105.17 que oculta la dirección IP de la pasarela B

**Red de Minneapolis - Servidor**

- El sistema E tiene una dirección IP 56.172.1.1.
- El sistema E es el contestador en este escenario.
- El cortafuegos D tiene una dirección IP 146.210.18.51.
- El cortafuegos D tiene una norma NAT estática que correlaciona la IP pública (146.210.18.15) con la IP privada del sistema E (56.172.1.1). Por lo tanto, desde el punto de vista de los clientes, la dirección IP del sistema E es la dirección IP pública (146.210.18.51) del cortafuegos D.

## Tareas de configuración

**Conceptos relacionados**:

"Gestión de claves" en la página 9
Una VPN dinámica ofrece seguridad adicional para las comunicaciones mediante el protocolo IKE (intercambio de claves de Internet) para la gestión de claves. IKE permite a los servidores VPN de cada extremo de la conexión negociar nuevas claves a intervalos determinados.

"IPSec (compatible con NAT) con UDP" en la página 15
La encapsulación UDP permite que el tráfico IPSec pase a través de un dispositivo NAT convencional. Consulte este tema para obtener más información acerca de sus características y las razones por las que debe utilizarla para las conexiones VPN.

## Cómo completar las hojas de trabajo de planificación

Las siguientes listas de comprobación de planificación ilustran el tipo de información que necesita para empezar a configurar la VPN. Todas las respuestas de la lista de comprobaciones de los prerrequisitos deben ser SÍ antes de poder proseguir con la configuración de la VPN.

**Nota:** Existen hojas de trabajo independientes para la pasarela B y el sistema E.

*Tabla 5. Requisitos del sistema*

| **Lista de comprobación de los prerrequisitos** | **Respuestas** |
|---|---|
| ¿Está instalada la opción Digital Certificate Manager? | Sí |
| ¿Se ha iniciado el servidor HTTP (para dar soporte a IBM Navigator for i)? | Sí |
| ¿Está instalado IBM TCP/IP Connectivity Utilities para i? | Sí |
| ¿Ha establecido en 1 el valor del sistema de retener datos de seguridad del servidor (QRETSVRSEC *SEC)? | Sí |
| ¿Está configurado TCP/IP en el sistema (incluyendo las interfaces IP, rutas IP, el nombre del host local IP y el nombre de dominio local IP)? | Sí |
| ¿Se ha establecido la comunicación normal TCP/IP entre los puntos finales? | Sí |
| ¿Ha aplicado los últimos arreglos temporales de programa (PTF)? | Sí |
| Si el túnel de la VPN atraviesa los cortafuegos o direccionadores que utilizan el filtrado de paquetes IP, ¿soportan las normas de filtro del cortafuegos o direccionador los protocolos AH y ESP? | Sí |
| ¿Están configurados los cortafuegos o los direccionadores para permitir el tráfico a través del puerto 4500 para las negociaciones de claves? Normalmente, las VPN asociadas realizan las negociaciones IKE a través del puerto 500, cuando IKE detecta el envío de paquetes NAT a través del puerto 4500. | Sí |
| ¿Están configurados los cortafuegos para habilitar el reenvío de IP? | Sí |

*Tabla 6. Configuración de la pasarela B*

| **Necesita esta información para configurar la VPN para la pasarela B** | **Respuestas** |
|---|---|
| ¿Qué tipo de conexión está creando? | pasarela-a-otro host |
| ¿Cómo se denominará el grupo de claves dinámicas? | CHIgw2MINhost |
| ¿Qué tipo de seguridad y rendimiento del sistema necesita para proteger las claves? | equilibrado |
| ¿Utiliza certificados para autenticar la conexión? Si no es así, ¿cuál es la clave precompartida? | No : topsecretstuff |
| ¿Cuál es el identificador del servidor de claves local? | Dirección IP: 214.72.189.35 |
| ¿Cuál es el identificador del punto final de datos local? | Subred: 10.8.11.0<br>Máscara: 255.255.255.0 |
| ¿Cuál es el identificador del servidor de claves remoto? | Dirección IP: 146.210.18.51 |
| ¿Cuál es el identificador del punto final de datos remoto? | Dirección IP: 146.210.18.51 |
| ¿Qué puertos y protocolos desea permitir fluir a través de la conexión? | Cualquiera |
| ¿Qué tipo de seguridad y rendimiento del sistema necesita para proteger sus datos? | equilibrado |
| ¿A qué interfaces se aplica la conexión? | TRLINE |

*Tabla 7. Configuración del sistema E*

| Necesita esta información para configurar la VPN para el sistema E | Respuestas |
|---|---|
| ¿Qué tipo de conexión está creando? | host-a-otra pasarela |
| ¿Cómo se denominará el grupo de claves dinámicas? | CHIgw2MINhost |
| ¿Qué tipo de seguridad y rendimiento del sistema necesita para proteger las claves? | máxima |
| ¿Utiliza certificados para autenticar la conexión? Si no es así, ¿cuál es la clave precompartida? | No : topsecretstuff |
| ¿Cuál es el identificador del servidor de claves local? | Dirección IP: 56.172.1.1 |
| ¿Cuál es el identificador del servidor de claves remoto?<br>**Nota:** Si no se conoce la dirección IP del cortafuegos C, puede utilizar *ANYIP como identificador para el servidor de claves remoto. | Dirección IP:<br>129.42.105.17 |
| ¿Cuál es el identificador del punto final de datos remoto? | Subred: 10.8.11.0<br>Máscara: 255.255.255.0 |
| ¿Qué puertos y protocolos desea permitir fluir a través de la conexión? | Cualquiera |
| ¿Qué tipo de seguridad y rendimiento del sistema necesita para proteger sus datos? | máxima |
| ¿A qué interfaces se aplica la conexión? | TRLINE |

## Configuración de VPN en la pasarela B

Complete estos pasos para configurar una conexión VPN en la pasarela B.

Utilice la información de sus hojas de trabajo de planificación para configurar la VPN en la pasarela B de la forma siguiente:

1. En IBM Navigator for i, expanda **Red** > **Políticas IP** > **Red privada virtual**.
2. Pulse **Conexiones seguras** para abrir el panel **Conexiones**.
3. Pulse **Acciones** > **Conexión nueva** para iniciar el asistente de Conexión.
4. Revise la página de **Bienvenida** para obtener información acerca de los objetos que crea el asistente.
5. Pulse **Siguiente** para ir a la página **Nombre de la conexión**.
6. En el campo **Nombre**, especifique `CHIgw2MINhost`.
7. Opcional: Especifique una descripción para este grupo de conexión.
8. Pulse **Siguiente** para ir a la página **Escenario de la conexión**.
9. Seleccione **Conectar su pasarela a otro host**.
10. Pulse **Siguiente** para ir a la página **Política de intercambio de claves de Internet**.
11. Seleccione **Crear una nueva política** y, a continuación, seleccione **Equilibrar seguridad y rendimiento**.

    **Nota:** Si recibe un mensaje de error que empieza por "No se ha podido procesar la solicitud del certificado", puede ignorarlo porque no está utilizando certificados para el intercambio de claves.
12. Opcional: Si tiene certificados instalados, aparecer la página **Certificado para punto final de conexión local**. Seleccione No para indicar que utilizará certificados para autenticar la conexión.
13. Pulse **Siguiente** para ir a la página **Servidor de claves local**.
14. Seleccione **IP versión 4** como campo **Tipo de identificador**.
15. Seleccione `214.72.189.35` en el campo **Dirección IP**.
16. Pulse **Siguiente** para ir a la página **Servidor de claves remoto**.
17. Seleccione **Dirección IP versión 4** en el campo **Tipo de identificador**.
18. Especifique `146.210.18.51` en el campo **Identificador**.

**Nota:** Si la pasarela B inicia una conexión con una NAT estática, debe especificar un intercambio de claves de modalidad principal para poder entrar una única IP para la clave remota. El intercambio de claves de modalidad principal se selecciona de forma predeterminada cuando se crea una conexión con el Asistente de conexión VPN. Si se utiliza la modalidad agresiva en este caso, se debe especificar un tipo no IPV4 de identificador remoto para la clave remota.

19. Especifique `topsecretstuff` en el campo **Clave precompartida**.
20. Pulse **Siguiente** para ir a la página **Punto final de datos local**.
21. Seleccione **Subred IP versión 4** en el campo **Tipo de identificador**.
22. Especifique `10.8.0.0` en el campo **Identificador**.
23. Especifique `255.255.255.0` en el campo **Máscara de subred**.
24. Pulse **Siguiente** para ir a la página **Servicios de datos**.
25. Acepte los valores predeterminados y, a continuación, pulse **Siguiente** para ir a la página Política de datos.
26. Seleccione **Crear una nueva política** y, a continuación, seleccione **Equilibrar seguridad y rendimiento**.
27. Pulse **Siguiente** para ir a la página **Requerir filtro de política**.
28. Seleccione **Esta conexión necesita un filtro de política**.
29. Pulse **Siguiente** para ir a la página **Interfaces aplicables**.
30. Seleccione **TRLINE** en la tabla Línea.
31. Pulse **Siguiente** para ir a la página **Resumen**.
32. Revise los objetos que creará el asistente para asegurar que son correctos.
33. Pulse **Finalizar** para completar la configuración.
34. Cuando aparezca el recuadro de diálogo **Activar filtros de políticas**, seleccione **Si**, activar los filtros de política generados y, a continuación, seleccione **Permitir el resto de tráfico**.
35. Pulse **Aceptar** para completar la configuración.

## Configuración de VPN en el sistema E

Complete estos pasos para configurar una conexión VPN en el sistema E.

Utilice la información de sus hojas de trabajo de planificación para configurar la VPN en el sistema E de la forma siguiente:

1. En IBM Navigator for i, expanda **Red** > **Políticas IP** > **Red privada virtual**.
2. Pulse **Conexiones seguras** para abrir el panel **Conexiones**.
3. Pulse **Acciones** > **Conexión nueva** para iniciar el asistente de Conexión.
4. Revise la página de **Bienvenida** para obtener información acerca de los objetos que crea el asistente.
5. Pulse **Siguiente** para ir a la página **Nombre de la conexión**.
6. En el campo **Nombre**, especifique `CHIgw2MINhost`.
7. Opcional: Especifique una descripción para este grupo de conexión.
8. Pulse **Siguiente** para ir a la página **Escenario de la conexión**.
9. Seleccione **Conectar su host a otra pasarela**.
10. Pulse **Siguiente** para ir a la página **Política de intercambio de claves de Internet**.
11. Seleccione **Crear una nueva política** y, a continuación, seleccione **Equilibrar seguridad y rendimiento**.

    **Nota:** Si recibe un mensaje de error que empieza por "No se ha podido procesar la solicitud del certificado", puede ignorarlo porque no está utilizando certificados para el intercambio de claves.
12. Opcional: Si tiene certificados instalados, aparecer la página **Certificado para punto final de conexión local**. Seleccione No para indicar que utilizará certificados para autenticar la conexión.
13. Pulse **Siguiente** para ir a la página **Servidor de claves local**.

14. Seleccione **Dirección IP versión 4** como campo **Tipo de identificador**.
15. Seleccione `56.172.1.1` en el campo **Dirección IP**.
16. Pulse **Siguiente** para ir a la página **Servidor de claves remoto**.
17. Seleccione **Dirección IP versión 4** en el campo **Tipo de identificador**.
18. Especifique `129.42.105.17` en el campo **Identificador**.

    **Nota:** Si no se conoce la dirección IP del cortafuegos C, puede utilizar *ANYIP como identificador para el servidor de claves remoto.
19. Especifique `topsecretstuff` en el campo **Clave precompartida**.
20. Pulse **Siguiente** para ir a la página **Punto final de datos remoto**.
21. Seleccione **Subred IP versión 4** en el campo **Tipo de identificador**.
22. Especifique `10.8.11.0` en el campo **Identificador**.
23. Especifique `255.255.255.0` en el campo **Máscara de subred**.
24. Pulse **Siguiente** para ir a la página **Servicios de datos**.
25. Acepte los valores predeterminados y, a continuación, pulse **Siguiente** para ir a la página Política de datos.
26. Seleccione **Crear una nueva política** y, a continuación, seleccione **Equilibrar seguridad y rendimiento**.
27. Pulse **Siguiente** para ir a la página **Requerir filtro de política**.
28. Seleccione **Esta conexión necesita un filtro de política**.
29. Pulse **Siguiente** para ir a la página **Interfaces aplicables**.
30. Seleccione **TRLINE** en la tabla Línea.
31. Pulse **Siguiente** para ir a la página **Resumen**.
32. Revise los objetos que creará el asistente para asegurar que son correctos.
33. Pulse **Finalizar** para completar la configuración.
34. Cuando aparezca el recuadro de diálogo **Activar filtros de políticas**, seleccione **Si**, activar los filtros de política generados y, a continuación, seleccione **Permitir el resto de tráfico**.
35. Pulse **Aceptar** para completar la configuración.

## Inicio de una conexión

Una vez configurada la conexión VPN en el sistema E, debe iniciarla.

Siga estos pasos para confirmar que la conexión CHIgw2MINhost en el sistema E está activa:

1. Inicie sesión en IBM Navigator for i para el Sistema E: http://<systemE>:2001.
2. En IBM Navigator for i, expanda **Red** > **Políticas IP** > **Red privada virtual**.
3. Pulse **Conexiones seguras** para abrir el asistente de Conexiones.
4. Pulse **Acciones** > **Todas las conexiones**.
5. Visualice **CHIgw2MINhost** y compruebe que el campo **Estado** sea *Desocupado* o *Por solicitud*.

Siga estos pasos para iniciar la conexión CHIgw2MINhost desde la pasarela B:

1. Inicie sesión en IBM Navigator for i para la Pasarela B: http://<Gateway B>:2001.
2. En IBM Navigator for i, expanda **Red** > **Todas las tareas** > **Políticas IP** > **Red privada virtual**.
3. Si el servidor VPN no está iniciado, pulse **Iniciar servidor VPN**.
4. Expanda **Red** > **Políticas IP** > **Red privada virtual** y pulse **Conexiones seguras**.
5. Pulse con el botón derecho del ratón en **Todas las conexiones** para visualizar una lista de conexiones en el panel derecho.
6. Pulse con el botón derecho del ratón **CHIgw2MINhost** y seleccione **Iniciar**.

7. Desde el menú **Visualizar**, seleccione **Renovar**. Si la conexión se inicia satisfactoriamente, el campo **Estado** debe cambiar de *Iniciando* o *Por solicitud* a *Habilitado*. La conexión tardará un poco en iniciarse, por lo tanto, renueve periódicamente la visualización hasta que el estado cambie a *Habilitado*.

### Prueba de la conexión

Cuando haya terminado la configuración de la pasarela B y el sistema E, y haya iniciado satisfactoriamente los servidores VPN, pruebe la conectividad para asegurarse de que los dos sistemas pueden comunicarse entre sí.

Para probar las conexiones, siga estos pasos:

1. Busque un sistema en la red del PC A y abra una sesión Telnet.
2. Especifique la dirección IP pública del sistema E, que es 146.210.18.51.
3. Especifique la información de inicio de sesión si es necesaria. Si puede visualizar la pantalla de inicio de sesión, la conexión funciona correctamente.

## Escenario: conexión VPN con usuarios remotos

El administrador debe configurar una conexión de red privada virtual (VPN) con los usuarios remotos para habilitar las conexiones remotas.

Las siguientes tareas muestran cómo configura el administrador una conexión VPN con los usuarios remotos.

### Ejecución de las hojas de trabajo de planificación para la conexión VPN de la sucursal al personal de ventas remoto

El administrador de la sucursal de ventas utiliza las hojas de trabajo de planificación VPN para configurar una red privada virtual (VPN) en los sistemas y las estaciones de trabajo remotas.

El asesor de planificación de VPN ya no está soportado mediante el Centro de información. Cada una de las siguientes hojas de trabajo de planificación puede utilizarse como plantilla para ayudar a planificar y configurar una VPN, utilizando el asistente de Nueva conexión VPN en IBM Navigator for i.

*Tabla 8. Hoja de trabajo de planificación para la conexión VPN entre la sucursal y el personal de ventas remoto*

| **Preguntas del asistente VPN** | **Valores recomendados (de resultados anteriores del Asesor de planificación)** |
|---|---|
| ¿Cómo desea denominar a este grupo de conexión? | SalestoRemote |
| ¿Qué tipo de grupo de conexión desea crear? | Seleccione **Conectar su host a otro host** |
| ¿Qué política de intercambio de claves de Internet desea utilizar para proteger la clave? | Seleccione **Crear una nueva política** y, a continuación, seleccione **Máxima seguridad, mínimo rendimiento** |
| ¿Utiliza certificados? | Seleccione **No** |

*Tabla 8. Hoja de trabajo de planificación para la conexión VPN entre la sucursal y el personal de ventas remoto (continuación)*

| **Preguntas del asistente VPN** | **Valores recomendados (de resultados anteriores del Asesor de planificación)** |
|---|---|
| Entre el identificador que representa el servidor de claves local de esta conexión. | Tipo de identificador: **Dirección IP versión 4**, Dirección IP: **192.168.1.2**. Para la dirección IPv6, tipo de identificador: **Dirección IP versión 6**, Dirección IP: **2001:DB8::2**.<br>**Nota:** Las direcciones IP que se utilizan en este escenario se proporcionan sólo a efectos de ejemplo. No reflejan ningún esquema de direcciones IP y no deben utilizarse en ninguna configuración real. Utilice sus propias direcciones IP cuando complete estas tareas. |
| ¿Cuál es el identificador del servidor de claves al que desea conectarse? | Tipo de identificador: **Cualquier dirección IP**, **Clave precompartida**: mycokey.<br>**Nota:** La clave precompartida es una serie de texto de 32 caracteres que IBM i VPN utiliza para autenticar la conexión, así como para establecer las claves que protegen los datos. En general, debe tratar una clave precompartida de la misma forma que una contraseña. |
| ¿Cuáles son los puertos y los protocolos de los datos que protegerá esta conexión? | **Puerto local**: 1701, **Puerto remoto**: Cualquier puerto, **Protocolo**: UDP |
| ¿Qué política de datos desea utilizar para proteger los datos? | Seleccione **Crear una nueva política** y, a continuación, seleccione **Máxima seguridad, mínimo rendimiento** |
| Compruebe las interfaces en el sistema local a las que se aplicará esta conexión. | ETHLINE (sucursal de ventas) |

## Configuración de un perfil de terminador L2TP del sistema A

Si desea configurar las conexiones remotas con las estaciones de trabajo remotas, debe configurar el sistema A para que acepte conexiones de entrada de esos clientes.

Para configurar un perfil de terminador L2TP (Layer Two Tunneling Protocol) para el sistema A, siga estos pasos:

1. En un navegador web, especifique http://systemA:2001, donde systemA es el nombre de host del Sistema A.
2. Inicie una sesión en el sistema con su perfil de usuario y contraseña.
3. Expanda **Red** > **Servicios de acceso remoto**.

4. Pulse **Perfiles de conexión de receptor** con el botón derecho del ratón para establecer el sistema A como un servidor que permita las conexiones entrantes de usuarios remotos, y seleccione **Perfil nuevo**.
5. Seleccione las siguientes opciones en la página Configuración:
   - **Tipo de protocolo:** PPP
   - **Tipo de conexión:** L2TP (línea virtual)

     **Nota:** El campo **Modalidad operativa** debe mostrar automáticamente **Terminador (servidor de red)**.
   - **Tipo de servicio de línea:** Línea individual
6. Pulse **Aceptar**. Aparecerá la página Propiedades de perfil punto a punto nuevo.
7. En la pestaña **General**, complete estos campos:
   - **Nombre**: MYCOL2TP
   - Seleccione **Iniciar perfil con TCP/IP** si desea que el perfil se inicie automáticamente con TCP.
8. En la pestaña **Conexión**, seleccione **192.168.1.2** (**2001:DB8::2** en IPv6) para la **Dirección IP del punto final del túnel local**.

   **Importante:** Las direcciones IP que se utilizan en este escenario se proporcionan sólo a efectos de ejemplo. No reflejan ningún esquema de direcciones IP y no deben utilizarse en ninguna configuración real. Utilice sus propias direcciones IP cuando complete estas tareas.
9. Seleccione **MYCOL2TP** como **Nombre de línea virtual**. Aparecerá la página Propiedades L2TP nuevas.
10. En la página Autenticación, entre `systema` como nombre de host. Pulse **Aceptar**. Volverá a la página Conexión.
11. En la página Conexión, seleccione las siguientes opciones y especifique `25` como **Número máximo de conexiones**.
    a. Pulse la pestaña **Autenticación** y seleccione **Requerir que este sistema verifique la identidad del sistema remoto**.
    b. Seleccione **Autenticar localmente utilizando una lista de validación**.
    c. Entre `QL2TP` en el campo **Nombre de lista de validación** y pulse **Nuevo**.
12. En la página Lista de validación, seleccione **Añadir**.
13. Añada nombres de usuario y contraseñas para cada uno de los empleados remotos. Pulse **Aceptar**.
14. En la página de confirmación de contraseña, vuelva a especificar la contraseña de cada empleado remoto. Pulse **Aceptar**.
15. En la página Valores de IPv4 de TCP/IP, seleccione 10.1.1.1 para **Dirección IP local**.
16. En el campo **Método de asignación de direcciones IP**, seleccione **Agrupación de direcciones**.
17. En el campo **Dirección IP inicial**, entre `10.1.1.100` y `49` como **Número de direcciones**. Para la dirección IPv6, marque **Habilitar campo IPv6** en la pestaña de valores de IPv6 de TCP/IP.
18. Seleccione **Permitir que el sistema remoto acceda a otras redes (reenvío IP)**. Pulse **Aceptar**.

## Inicio del perfil de conexión de receptor

Después de configurar el perfil de conexión de receptor L2TP (Layer Two Tunneling Protocol) para el sistema A, el administrador debe iniciar esta conexión para que escuche las peticiones entrantes de los clientes remotos.

**Nota:** Puede recibir un mensaje de error indicando que el subsistema QUSRWRK no se ha iniciado. Este mensaje aparece cuando intenta iniciar el perfil de conexión de receptor. Para iniciar el subsistema QUSRWRK, siga estos pasos:

1. En una interfaz basada en caracteres, especifique `strsbs`.
2. En la pantalla Iniciar subsistema, especifique `QUSRWRK` en el campo **Descripción del subsistema**.

Para iniciar el perfil de conexión de receptor para clientes remotos, realice estas tareas:

1. Inicie sesión en IBM Navigator for i desde *Sistema A* y expanda **Red** > **Servicios de acceso remoto**.
2. Pulse **Perfiles de conexión de receptor** para abrir el panel **Perfiles de conexión de receptor**.
3. Pulse con el botón derecho del ratón **MYCOL2TP** y seleccione **Iniciar**.
4. El campo **Estado** cambia a **En espera de peticiones de conexión**.

## Configuración de una conexión VPN en el sistema A para clientes remotos

Después de configurar e iniciar el perfil de conexión de receptor L2TP (Layer Two Tunneling Protocol) para el sistema A, el administrador debe configurar una red privada virtual (VPN) para proteger la conexión entre los clientes remotos y la red en la sucursal de ventas.

Para configurar una VPN para clientes remotos, siga estos pasos:

**Importante:** Las direcciones IP que se utilizan en este escenario se proporcionan sólo a efectos de ejemplo. No reflejan ningún esquema de direcciones IP y no deben utilizarse en ninguna configuración real. Utilice sus propias direcciones IP cuando complete estas tareas.

1. En un navegador web, especifique http://systemA:2001, donde systemA es el nombre de host del sistema A.
2. Inicie una sesión en el sistema con su perfil de usuario y contraseña.
3. Expanda **Red** > **Políticas IP** > **Todas las tareas** > **Políticas IP** > **Red privada virtual**.
4. Pulse **Crear conexión** para iniciar el asistente Nueva conexión VPN. Revise la página de bienvenida para obtener información acerca de los objetos que crea el asistente.
5. Pulse **Siguiente** para ir a la página Nombre de la conexión.
6. En el campo **Nombre**, especifique `SalestoRemote`.
7. Opcional: Especifique una descripción para este grupo de conexión. Pulse **Siguiente**.
8. En la página Escenario de conexión, seleccione **Conectar su host a otro host**. Pulse **Siguiente**
9. En la página Política de intercambio de claves Internet, seleccione **Crear una nueva política** y, a continuación, seleccione **Máxima seguridad, mínimo rendimiento**. Pulse **Siguiente**.
10. En la página Certificado de punto final de conexión local, seleccione **No**. Pulse **Siguiente**.
11. En la página Servidor de claves local, seleccione **Dirección IP versión 4** como el tipo de identificador. La dirección IP asociada debe ser 192.168.1.2. Pulse **Siguiente**. Para la dirección IPv6, en la página Servidor de claves local, seleccione **Dirección IP versión 6** como el tipo de identificador. La dirección IP asociada debe ser 2001:DB8::2. Pulse **Siguiente**.
12. En la página Servidor de claves remoto, seleccione **Cualquier dirección IP** en el campo **Tipo de identificador**. En el campo **Clave precompartida**, especifique `mycokey`. Pulse **Siguiente**.
13. En la página Servicios de datos, entre `1701` como puerto local. A continuación, seleccione `1701` como puerto remoto y **UDP** como el protocolo. Pulse **Siguiente**.
14. En la página Política de datos, seleccione **Crear una nueva política** y, a continuación, seleccione **Máxima seguridad, mínimo rendimiento**. Pulse **Siguiente**.
15. En la página Interfaces aplicables, seleccione **ETHLINE**. Pulse **Siguiente**.
16. En la página Resumen, revise los objetos que creará el asistente para asegurar que son correctos.
17. Pulse **Finalizar** para completar la configuración. Cuando se abra la ventana Activar filtros de políticas, seleccione **No, las normas de paquetes se activarán más tarde**. Pulse **Aceptar**.

## Activación de las normas de filtros

El asistente crea automáticamente las normas de paquetes que la conexión requiere para funcionar adecuadamente. Sin embargo, deberá activarlas en ambos sistemas antes de poder iniciar la conexión de la red privada virtual (VPN).

Para activar las normas de filtros en el sistema A, siga estos pasos:

**Importante:** Las direcciones IP que se utilizan en este escenario se proporcionan sólo a efectos de ejemplo. No reflejan ningún esquema de direcciones IP y no deben utilizarse en ninguna configuración real. Utilice sus propias direcciones IP cuando complete estas tareas.

1. En un navegador web, especifique http://systemA:2001, donde systemA es el nombre de host del sistema A.
2. Inicie una sesión en el sistema con su perfil de usuario y contraseña.
3. Expanda **Red** > **Políticas IP**.
4. Pulse **Reglas de paquete** y seleccione **Activar reglas** en las acciones de la tabla Reglas de paquete.
5. En la página Activar normas de paquetes, seleccione **activar sólo las normas generadas por VPN** y seleccione **ETHLINE** como la interfaz en la que desea activar estas normas de filtro. Pulse **Aceptar**.

Antes de que los usuarios remotos puedan configurar las estaciones de trabajo Windows, el administrador les proporciona la siguiente información para que puedan configurar su lado de la conexión. Para cada uno de los usuarios remotos, proporcione la siguiente información:

- Nombre de la clave precompartida: `mycokey`
- Dirección IP del sistema A: 192.168.1.2 (2001:DB8::2 en IPv6)
- Nombre de usuario y contraseña de la conexión

**Nota:** Estos se crean cuando el administrador añade el nombre de usuario y las contraseñas a una lista de validación durante la configuración del perfil de terminador L2TP (Layer Two Tunneling Protocol).

## Configuración de VPN en el cliente Windows

Utilice este procedimiento para configurar VPN en un cliente Windows.

Los usuarios remotos en MyCo, Inc necesitan configurar el cliente Windows remoto siguiendo estos pasos:

1. En el menú de Windows **Inicio**, expanda **Todos los programas** > **Accesorios** > **Comunicaciones** > **Asistente para conexión nueva**.
2. En la página de bienvenida, lea la información general. Pulse **Siguiente**.
3. En la página Tipo de conexión de red, seleccione **Conectarse a la red de mi lugar de trabajo**. Pulse **Siguiente**.
4. En la página Conexión de red, seleccione **Conexión de red privada virtual**. Pulse **Siguiente**.
5. En la página Nombre de conexión, escriba `Conexión con sucursal` en el campo **Nombre de la organización**. Pulse **Siguiente**.
6. En la página Red pública, seleccione **No usar la conexión inicial**. Pulse **Siguiente**.
7. En la página Selección de servidor VPN, entre `192.168.1.2` (`2001:DB8::2` en IPv6) en el campo **Nombre del host o dirección IP**. Pulse **Siguiente**.
8. En la página Disponibilidad de conexión, seleccione **Sólo para mi uso**. Pulse **Siguiente**.
9. En la página Resumen, pulse **Agregar un acceso directo a esta conexión a mi escritorio**. Pulse **Finalizar**.
10. Pulse el icono **Conectar conexión a MyCo** que se ha creado en el escritorio.
11. En la página Conectar conexión a MyCo, escriba el nombre de usuario y la contraseña que le ha proporciona el administrador.
12. Seleccione **Guardar este nombre de usuario y contraseña para los siguientes usuarios** y **Sólo yo**. Pulse **Propiedades**.
13. En la página **Seguridad**, compruebe que las siguientes **Opciones de seguridad** estén seleccionadas:
    - **Típica**
    - **Requerir una contraseña segura**
    - **Requerir cifrado de datos**

    Pulse **Configuración IPSec**.

14. En la página Configuración IPSec, seleccione **Usar clave previamente compartida autenticar** y especifique `mycokey` en el campo **Clave previamente compartida**. Pulse **Aceptar**.
15. En la página Redes, seleccione **Red privada virtual (VPN) con L2TP/IPsec** como **Tipo de red privada virtual**. Pulse **Aceptar**.
16. Inicie una sesión con el nombre de usuario y la contraseña y pulse **Conectar**.

Para iniciar la conexión de red privada virtual (VPN) en el lado del cliente, pulse el icono que aparece en el escritorio después de completar el asistente de conexión.

### Prueba de una conexión VPN entre puntos finales

Tras haber finalizado la configuración de la conexión entre el sistema A y los usuarios remotos, y haber iniciado satisfactoriamente la conexión, pruebe la conectividad para asegurarse de que los hosts remotos pueden comunicarse entre sí.

Para probar la conectividad, siga estos pasos:

1. En un navegador web, especifique http://systemA:2001, donde systemA es el nombre de host del sistema A.
2. Inicie una sesión en el sistema con su perfil de usuario y contraseña.
3. Expanda **Red** > **Todas las tareas** > **Configuración TCP/IP**.
4. Pulse **Trabajar con Ping**.
5. En el panel **Ping**, especifique 10.1.1.101 (2001:DA8::1:101 en IPv6) en el campo **Ping**.

   **Nota:** 10.1.1.101 representa la dirección IP asignada dinámicamente (al cliente de ventas remoto) desde la agrupación de direcciones especificada en el perfil de terminador L2TP (Layer Two Tunneling Protocol) del sistema A.
6. Pulse **Realizar PING ahora** para verificar la conectividad del sistema A con una estación de trabajo remota. Pulse **Aceptar**.

Para probar la conexión desde el cliente remoto, el empleado remoto realiza estos pasos en una estación de trabajo que ejecuta Windows:

1. En el indicador de mandatos, entre `ping 10.1.1.2` (`ping 2001:DA8::2` en IPv6). Esta es la dirección IP de una de las estaciones de trabajo en la red de la oficina central.
2. Repita estos pasos para probar la conectividad desde la oficina central a la sucursal.

## Escenario: utilización de la conversión de direcciones de red para VPN

En este escenario, la empresa desea intercambiar datos sensibles con uno de sus asociados comerciales mediante VPN. Para preservar mejor la privacidad de la estructura de red de la empresa, ésta también utilizará VPN NAT para ocultar la dirección IP privada del sistema que utiliza para alojar las aplicaciones a las que el asociado comercial tiene acceso.

### Situación

Imagine que es el administrador de red de una pequeña empresa de fabricación de Barcelona. Uno de sus asociados comerciales, un proveedor de piezas que se encuentra en Logroño, desea empezar a desarrollar un volumen mayor de su negocio con su empresa a través de Internet. Puesto que es de vital importancia que su empresa disponga de los componentes y cantidades específicos en el preciso momento en que los necesite, el proveedor tendrá que conocer siempre el estado del inventario y las planificaciones de producción de su empresa. Actualmente, usted maneja esta interacción de forma manual, pero considera que resulta lenta, costosa e incluso inexacta a veces y por tanto está deseoso de investigar nuevas opciones.

Dada la confidencialidad y sensibilidad con respecto al tiempo de la información que intercambia, decide crear una VPN entre la red de su proveedor y la red de su empresa. Para preservar mejor la privacidad

de la estructura de red de su empresa, decide que necesitará ocultar la dirección IP privada del sistema que alberga las aplicaciones a las que el proveedor tiene acceso.

Puede utilizar las VPN no sólo para crear las definiciones de conexión de la pasarela VPN de la red de su empresa, sino también para proporcionar la conversión de direcciones que necesita para ocultar las direcciones privadas locales. A diferencia de la conversión de direcciones de red (NAT) convencional, que cambia las direcciones IP de las asociaciones de seguridad (AS) que VPN necesita para funcionar, VPN NAT realiza conversiones de direcciones antes de la validación SA, asignando una dirección a la conexión cuando ésta se inicia.

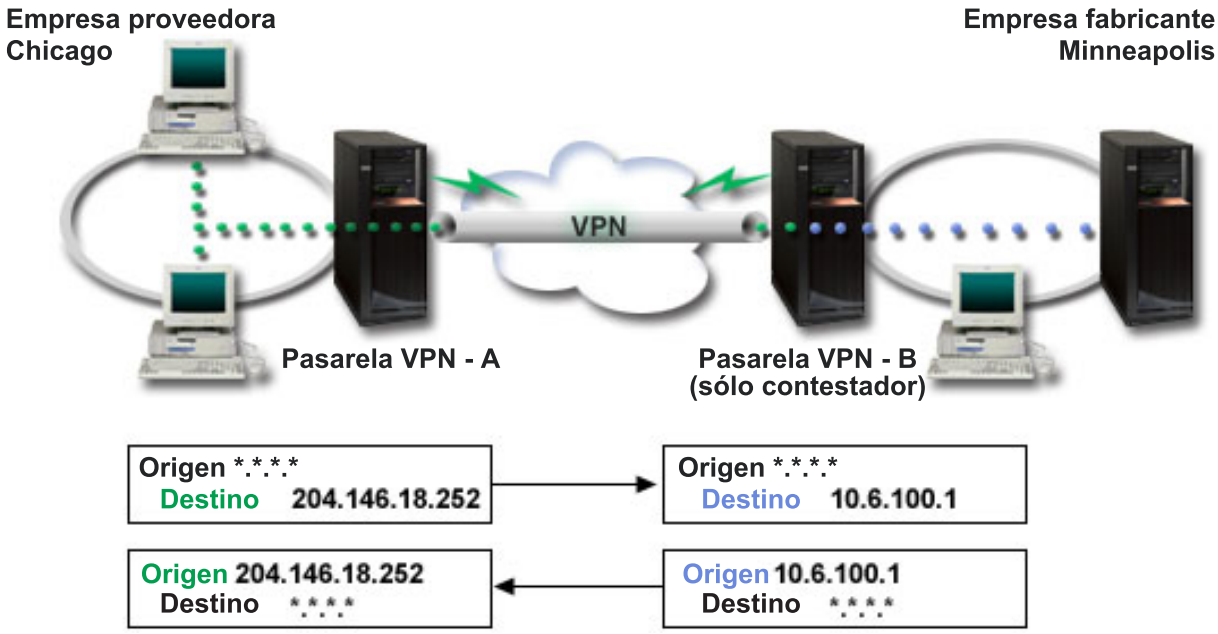
## Objetivos

Los objetivos de este escenario son:

- permitir a los clientes de la red del proveedor el acceso a un sólo host de la red del fabricante a través de una conexión VPN de pasarela a pasarela.
- ocultar la dirección IP privada del host de la red del fabricante, convirtiéndola en una dirección IP pública mediante la conversión de direcciones de red para VPN (NAT VPN).

## Detalles

El siguiente diagrama muestra las características de la red del proveedor y de la red del fabricante:




- La pasarela-A VPN está configurada para iniciar siempre las conexiones en la pasarela-B VPN.
- La pasarela-A VPN define el punto final destino de la conexión como 204.146.18.252 (la dirección pública asignada al sistema C).
- El sistema C tiene una dirección IP privada en la red del fabricante de 10.6.100.1.
- Se ha definido la dirección pública 204.146.18.252 en la agrupación de servicios locales de la pasarela-B VPN para la dirección privada del sistema C, 10.6.100.1.
- La pasarela-B VPN convierte la dirección pública del sistema C a su dirección privada, 10.6.100.1, para los datagramas de entrada. La pasarela-B VPN convierte los datagramas de salida que se devuelven, de 10.6.100.1 de nuevo a la dirección pública del sistema C, 204.146.18.252. En lo que concierne a los clientes de la red del proveedor, la dirección IP del sistema C es 204.146.18.252. Nunca tendrán conocimiento de que se ha producido una conversión de direcciones.

### Tareas de configuración

Debe completar cada una de las siguientes tareas para configurar la conexión descrita en este escenario:

1. Configurar una VPN básica de pasarela a pasarela entre la **pasarela-A VPN** y la **pasarela-B VPN**.
2. Definir una agrupación de servicios local en la **pasarela-B VPN** para ocultar la dirección privada de **Sistema C** detrás del identificador público, 204.146.18.252.
3. Configurar la **pasarela-B VPN** para que convierta las direcciones locales utilizando direcciones de la agrupación de servicios local.

**Conceptos relacionados**:

"Conversión de direcciones de red para VPN" en la página 13
VPN proporciona una forma de realizar la conversión de direcciones de red, denominada NAT VPN. NAT VPN se diferencia de la NAT tradicional en que aquélla convierte las direcciones antes de aplicarlas a los protocolos IKE e IPSec. Consulte este tema para obtener más información.

---

## Planificación de VPN

El primer paso para utilizar VPN satisfactoriamente es la planificación. Este tema proporciona información acerca de la migración desde releases anteriores, requisitos de configuración y una hoja de trabajo de planificación personalizada para sus especificaciones.

La planificación es una parte esencial de su solución VPN total. Deberá tomar muchas decisiones complejas para asegurar que la conexión funcione correctamente. Utilice estos recursos para recopilar toda la información que necesite para asegurar que la VPN sea satisfactoria:

- Requisitos de configuración de VPN
- Determinar qué tipo de VPN se va a crear
- Completar las hojas de trabajo de planificación VPN

Después de haber realizado un plan para la VPN, puede empezar a configurarla.

**Tareas relacionadas**:

"Configuración de VPN" en la página 52
La interfaz de VPN le ofrece varias formas distintas de configurar las conexiones VPN. Puede configurar una conexión manual o dinámica.

## Requisitos de configuración de VPN

Para que una conexión VPN funcione correctamente en los sistemas y con los clientes de red, debe cumplir unos requisitos mínimos

A continuación se ofrece una lista de los requisitos mínimos para configurar una conexión VPN:

**Requisitos del sistema**

- Digital Certificate Manager
- IBM Navigator for i
- Establezca en 1 el valor del sistema de retener los datos de seguridad del servidor (QRETSVRSEC *SEC)
- TCP/IP, incluyendo las interfaces IP, las rutas, el nombre del host local y el nombre de dominio local deben estar configurados
- Las características de IBM i 7.1 IKEv2 y Algoritmos criptográficos mejorados sólo están disponibles en IBM Navigator for i

**Tareas relacionadas**:

"Iniciación a la resolución de problemas de VPN" en la página 68
Complete esta tarea para conocer los distintos métodos posibles para determinar los problemas de VPN que pueden surgir en el sistema.

## Cómo determinar qué tipo de VPN se va a crear

Determinar cómo se va a utilizar la VPN es uno de los primeros pasos que hay que seguir para realizar una planificación satisfactoria. Para hacer esto, es necesario comprender el rol que desempeñan los servidores de claves local y remoto en la conexión.

Por ejemplo, ¿son los puntos finales de *conexión* distintos de los puntos finales de *datos*? ¿Son iguales o una combinación de ambos? Los puntos finales de conexión autentican y cifran (o descifran) el tráfico de datos de la conexión y, de forma opcional, ofrecen la gestión de claves con el protocolo IKE (intercambio de claves de Internet). No obstante, los puntos finales de datos definen el tráfico IP que fluye por la VPN en la conexión entre dos sistemas; por ejemplo, todo el tráfico TCP/IP entre 123.4.5.6 y 123.7.8.9. Normalmente, cuando los puntos finales de conexión y de datos difieren, el servidor VPN es una pasarela. Cuando son iguales, el servidor VPN es un host.

Los varios tipos de implementaciones VPN que se adaptan a las necesidades de la mayor parte de empresas son los siguientes:

**De pasarela a pasarela**
: Los puntos finales de conexión de ambos sistemas son distintos de los puntos finales de datos. El protocolo IPSec (IP Security) protege el tráfico que circula entre las pasarelas. Sin embargo, IPSec no protege el tráfico de datos en cada extremo de las pasarelas, dentro de las redes internas. Esta configuración es habitual para conexiones entre sucursales ya que el tráfico que se direcciona más allá de las pasarelas de sucursal, a las redes internas, habitualmente se considera de confianza.

**De pasarela a host**
: IPSec protege el tráfico de datos mientras circula entre la pasarela y un host en una red remota. VPN no protege el tráfico de datos en la red local porque se considera de confianza.

**De host a host**
: VPN protege el tráfico de datos mientras circula entre un host en la red local y una pasarela remota. VPN no protege el tráfico de datos en la red remota.

**De host a host**
: Los puntos finales de la conexión corresponden a los puntos finales de datos tanto en el sistema local como en el remoto. VPN protege el tráfico de datos entre un host de la red local y un host de la red remota. Este tipo de VPN proporciona protección IPSec de extremo a extremo.

## Cómo completar las hojas de trabajo de planificación de VPN

Utilice las hojas de trabajo de planificación para recopilar información detallada sobre sus proyectos de utilización de la VPN. Necesitará completar estas hojas de trabajo para planificar su estrategia VPN de forma adecuada. También puede utilizar esta información para configurar la VPN.

Si lo prefiere, puede imprimir y completar las hojas de trabajo de planificación para recopilar información detallada sobre sus proyectos de utilización de la VPN.

Seleccione la hoja de trabajo del tipo de conexión que desea crear.

- Hoja de trabajo de planificación para conexiones dinámicas
- Hoja de trabajo de planificación para conexiones manuales

Si va a crear varias conexiones con propiedades parecidas, quizás desee configurar los valores predeterminados de VPN. Deberá proporcionar los valores predeterminados en las hojas de propiedades VPN. Esto significa que no necesita configurar las mismas propiedades cada vez. Para establecer los valores predeterminados, seleccione **Editar** del menú principal VPN y, a continuación, seleccione **Valores predeterminados**.

### Hoja de trabajo de planificación para conexiones dinámicas

Complete esta hoja de trabajo para configurar una conexión dinámica.

Antes de crear las conexiones VPN dinámicas, complete esta hoja de trabajo. La hoja de trabajo presupone que utilizará el asistente Nueva conexión. El asistente permite configurar la VPN en base a sus requisitos de seguridad básicos. En algunos casos, puede necesitar refinar las propiedades que el asistente configura para una conexión. Por ejemplo, si decide que necesita registrar por diario o si desea que el servidor VPN se inicie cada vez que se inicie TCP/IP. Si es así, pulse con el botón derecho del ratón el grupo de claves dinámicas o la conexión que el asistente ha creado y seleccione **Propiedades**.

Responda a cada pregunta antes de proceder con la configuración de la VPN.

*Tabla 9. Requisitos del sistema*

| **Lista de comprobación de los prerrequisitos** | **Respuestas** |
|---|---|
| ¿Está instalada la opción Digital Certificate Manager? | Sí |
| ¿Se ha iniciado el servidor HTTP (para dar soporte a IBM Navigator for i)? | Sí |
| ¿Está instalado IBM TCP/IP Connectivity Utilities para i? | Sí |
| ¿Ha establecido en 1 el valor del sistema de retener datos de seguridad del servidor (QRETSVRSEC *SEC)? | Sí |
| ¿Está configurado TCP/IP en el sistema (incluyendo las interfaces IP, rutas IP, el nombre del host local IP y el nombre de dominio local IP)? | Sí |
| ¿Se ha establecido la comunicación normal TCP/IP entre los puntos finales? | Sí |
| ¿Ha aplicado los últimos arreglos temporales de programa (PTF)? | Sí |
| Si el túnel de la VPN atraviesa los cortafuegos o direccionadores que utilizan el filtrado de paquetes IP, ¿soportan las normas de filtro del cortafuegos o direccionador los protocolos AH y ESP? | Sí |
| ¿Están configurados los cortafuegos o los direccionadores para permitir los protocolos IKE (UDP puerto 500), AH y ESP? | Sí |
| ¿Están configurados los cortafuegos para habilitar el reenvío de IP? | Sí |

*Tabla 10. Configuración de VPN*

| **Necesita esta información para configurar una conexión VPN dinámica** | **Respuestas** |
|---|---|
| ¿Qué tipo de conexión está creando?<br>• De pasarela a pasarela<br>• De host a host<br>• De pasarela a host<br>• De host a host | |
| ¿Cómo se denominará el grupo de claves dinámicas? | |
| ¿Qué tipo de seguridad y rendimiento del sistema necesita para proteger las claves?<br>• Máxima seguridad, mínimo rendimiento<br>• Equilibrar seguridad y rendimiento<br>• Mínima seguridad y máximo rendimiento | |
| ¿Utiliza certificados para autenticar la conexión? Si no es así, ¿cuál es la clave precompartida? | |
| ¿Cuál es el identificador del servidor de claves local? | |
| ¿Cuál es el identificador del servidor de claves local? | |
| ¿Cuál es el identificador del servidor de claves remoto? | |
| ¿Cuál es el identificador del punto final de datos remoto? | |

*Tabla 10. Configuración de VPN (continuación)*

| | |
|---|---|
| ¿Qué tipo de seguridad y rendimiento del sistema necesita para proteger sus datos?<br>• Máxima seguridad, mínimo rendimiento<br>• Equilibrar seguridad y rendimiento<br>• Mínima seguridad y máximo rendimiento | |

## Hoja de trabajo de planificación para conexiones manuales

Complete esta hoja de trabajo para configurar una conexión manual.

Complete esta hoja de trabajo que le ayudará a crear sus conexiones de red privada virtual (VPN) que no utilicen IKE para la gestión de claves. Responda a cada una de las siguientes preguntas antes de proseguir con la configuración de su VPN:

*Tabla 11. Requisitos del sistema*

| **Lista de comprobación de los prerrequisitos** | **Respuestas** |
|---|---|
| ¿Está instalado Digital Certificate Manager? | |
| ¿Se ha iniciado el servidor HTTP (para dar soporte a IBM Navigator for i)? | |
| ¿Está instalado IBM TCP/IP Connectivity Utilities para i? | |
| ¿Ha establecido en 1 el valor del sistema de retener datos de seguridad del servidor (QRETSVRSEC *SEC)? | |
| ¿Está configurado TCP/IP en el sistema (incluyendo las interfaces IP, rutas IP, el nombre del host local IP y el nombre de dominio local IP)? | |
| ¿Se ha establecido la comunicación normal TCP/IP entre los puntos finales? | |
| ¿Ha aplicado los últimos arreglos temporales de programa (PTF)? | |
| Si el túnel de la VPN atraviesa los cortafuegos o direccionadores que utilizan el filtrado de paquetes IP, ¿soportan las normas de filtro del cortafuegos o direccionador los protocolos AH y ESP? | |
| ¿Están configurados los cortafuegos o los direccionadores para permitir los protocolos AH y ESP? | |
| ¿Están configurados los cortafuegos para habilitar el reenvío de IP? | |

*Tabla 12. Configuración de VPN*

| **Necesita esta información para configurar una VPN manual** | **Respuestas** |
|---|---|
| ¿Qué tipo de conexión está creando?<br>• De host a host<br>• De host a host<br>• De pasarela a host<br>• De pasarela a pasarela | |
| ¿Cómo se denominará la conexión? | |
| ¿Cuál es el identificador del punto final de conexión local? | |
| ¿Cuál es el identificador del punto final de conexión remoto? | |
| ¿Cuál es el identificador del punto final de datos local? | |
| ¿Cuál es el identificador del punto final de datos remoto? | |
| ¿Qué tipo de tráfico permitirá para esta conexión (puerto local, puerto remoto y protocolo)? | |
| ¿Necesita conversión de direcciones para esta conexión? Consulte Conversión de direcciones de red para VPN para obtener más información. | |
| ¿Utilizará la modalidad de túnel o de transporte? | |

*Tabla 12. Configuración de VPN (continuación)*

| | |
|---|---|
| ¿Qué protocolo IPSec utilizará la conexión (AH, ESP o AH con ESP)? Consulte IPSec (IP Security) para obtener más información. | |
| ¿Qué algoritmo de autenticación utilizará la conexión (HMAC-MD5 o HMAC-SHA)? | |
| ¿Qué algoritmo de cifrado utilizará la conexión (DES-CBC o 3DES-CBC)?<br>**Nota:** Deberá especificar el algoritmo de cifrado sólo si ha seleccionado ESP como protocolo IPSec. | |
| ¿Cuál es la clave AH entrante? Si utiliza MD5, la clave será una serie de caracteres hexadecimales de 16 bytes. Si utiliza SHA, la clave será una serie de caracteres hexadecimales de 20 bytes.<br><br>La clave entrante debe coincidir exactamente con la clave saliente del servidor remoto. | |
| ¿Cuál es la clave AH saliente? Si utiliza MD5, la clave será una serie de caracteres hexadecimales de 16 bytes. Si utiliza SHA, la clave será una serie de caracteres hexadecimales de 20 bytes.<br><br>La clave saliente debe coincidir exactamente con la clave entrante del servidor remoto. | |
| ¿Cuál es la clave ESP entrante? Si utiliza DES, la clave será una serie de caracteres hexadecimales de 8 bytes. Si utiliza 3DES, la clave será una serie de caracteres hexadecimales de 24 bytes.<br><br>La clave entrante debe coincidir exactamente con la clave saliente del servidor remoto. | |
| ¿Cuál es la clave ESP saliente? Si utiliza DES, la clave será una serie de caracteres hexadecimales de 8 bytes. Si utiliza 3DES, la clave será una serie de caracteres hexadecimales de 24 bytes.<br><br>La clave saliente debe coincidir exactamente con la clave entrante del servidor remoto. | |
| ¿Cuál es el SPI (Índice de política de seguridad) entrante? El SPI entrante es una serie de caracteres hexadecimales de 4 bytes, donde el primer byte está establecido en 00.<br><br>El SPI entrante debe coincidir exactamente con el SPI saliente del servidor remoto. | |
| ¿Cuál es el SPI saliente? El SPI saliente es una serie de caracteres hexadecimales de 4 bytes.<br><br>El SPI saliente debe coincidir exactamente con el SPI entrante del servidor remoto. | |

**Conceptos relacionados**:

"Conversión de direcciones de red para VPN" en la página 13
VPN proporciona una forma de realizar la conversión de direcciones de red, denominada NAT VPN. NAT VPN se diferencia de la NAT tradicional en que aquélla convierte las direcciones antes de aplicarlas a los protocolos IKE e IPSec. Consulte este tema para obtener más información.

## Configuración de VPN

La interfaz de VPN le ofrece varias formas distintas de configurar las conexiones VPN. Puede configurar una conexión manual o dinámica.

Una conexión dinámica genera y negocia dinámicamente las claves que protegen la conexión, mientras está activa, mediante el protocolo IKE. Las conexiones dinámicas proporcionan un nivel suplementario de seguridad para los datos que fluyen a través de ellas porque las claves cambian automáticamente, a intervalos regulares. En consecuencia, es más difícil que un asaltante capture una clave, tenga tiempo de descifrarla y la utilice para desviar o capturar el tráfico protegido por esta.

Por otro lado, una conexión manual no proporciona soporte para negociaciones IKE ni, por tanto, gestión de claves automática. Además, ambos extremos de la conexión requieren la configuración de varios atributos que deben coincidir exactamente. Las conexiones manuales utilizan claves estáticas que no se

renuevan ni cambian mientras la conexión está activa. Debe detener una conexión manual para cambiar la clave asociada. Si considera que supone un riesgo para la seguridad, puede crear una conexión dinámica en su lugar.

**Conceptos relacionados**:

"Planificación de VPN" en la página 48
El primer paso para utilizar VPN satisfactoriamente es la planificación. Este tema proporciona información acerca de la migración desde releases anteriores, requisitos de configuración y una hoja de trabajo de planificación personalizada para sus especificaciones.

## Configuración de las conexiones VPN con el asistente Nueva conexión

El asistente Nueva conexión permite crear una red privada virtual (VPN) entre cualquier combinación de hosts y pasarelas.

Por ejemplo, de host a host, de pasarela a host, de host a pasarela o de pasarela a pasarela.

El asistente crea automáticamente cada uno de los objetos de configuración que VPN necesita para funcionar correctamente, incluyendo las normas de paquetes. Sin embargo, si necesita añadir más funciones a la VPN, como por ejemplo, registrar por diario o convertir direcciones de red para VPN (VPN NAT), deberá refinar más la VPN mediante las hojas de propiedades del grupo de claves dinámicas o de la conexión adecuados. Para ello, primero debe detener la conexión si está activa. A continuación, pulse con el botón derecho del ratón el grupo de claves dinámicas o la conexión y seleccione **Propiedades**.

Para crear una VPN con el asistente Conexión, siga estos pasos:

1. En IBM Navigator for i, expanda **Red** > **Todas las tareas** > **Políticas IP** > **Red privada virtual**.
2. Pulse **Crear conexión** para iniciar el asistente.
3. Siga los pasos del asistente para crear una conexión VPN básica. Pulse el botón **Ayuda** si la necesita.

## Configuración de políticas de seguridad de VPN

Después de determinar cómo va a utilizar la VPN, debe definir sus políticas de seguridad VPN.

**Nota:** Después de configurar las políticas de seguridad VPN, debe configurar las conexiones seguras.

**Tareas relacionadas**:

"Configuración de una conexión VPN segura" en la página 55
Tras haber definido las políticas de seguridad para la conexión, deberá configurar la conexión segura.

### Configuración de una política de intercambio de claves de Internet

La política de intercambio de claves de Internet (IKE) define qué nivel de autenticación y de protección de cifrado utilizará IKE durante las negociaciones de fase 1.

La fase 1 de IKE establece las claves que protegen los mensajes que fluyen en las negociaciones subsiguientes de la fase 2. No es necesario definir una política IKE cuando crea una conexión manual. Además, si crea la VPN con el asistente Nueva conexión, éste puede crear la política IKE.

| VPN utiliza la modalidad de firma RSA, ECDSA, o claves precompartidas para autenticar las negociaciones de fase 1. Si tiene previsto utilizar certificados digitales para autenticar los servidores de claves, en primer lugar deberá configurarlos mediante Digital Certificate Manager. La política IKE también identifica qué servidor de claves remoto utilizará esta política.

Para definir una política IKE o realizar cambios en una existente, siga estos pasos:

| 1. En IBM Navigator for i, expanda **Red** > **Políticas IP** > **Red privada virtual**, pulse **Políticas de**
| **seguridad IP**.

2. Para crear una política nueva, pulse con el botón derecho del ratón **Políticas IKE (intercambio de claves de Internet)** y seleccione **Política IKE (intercambio de claves de Internet) nueva**. Para realizar cambios en una política existente, pulse con el botón derecho del ratón en **Políticas de intercambio de claves de internet** y seleccione **Abrir**. Pulse con el botón derecho del ratón en la política que desee cambiar y seleccione **Propiedades**.
3. Cumplimente todas las hojas de propiedades. Pulse **Ayuda** si tiene preguntas acerca de cómo cumplimentar una página o alguno de los campos.
4. Pulse **Aceptar** para guardar los cambios.

Es recomendable utilizar la negociación de modalidad principal siempre que se utilice una clave precompartida para la autenticación. Ofrece un intercambio más seguro. Si debe utilizar claves precompartidas y la negociación de modalidad agresiva, seleccione contraseñas oscuras de improbable descubrimiento en los ataques que exploran el diccionario. También es recomendable cambiar periódicamente las contraseñas. Para forzar que un intercambio de clave utilice la negociación de modalidad principal, realice las siguientes tareas:

1. En IBM Navigator for i, expanda **Red** > **Políticas IP** > **Red privada virtual**, pulse **Políticas de seguridad IP**.
2. Pulse con el botón derecho del ratón en **Políticas de intercambio de claves de internet** y seleccione **Abrir**.
3. Pulse con el botón derecho del ratón una política de intercambio de clave y seleccione **Propiedades**.
4. En la página Transformaciones, pulse **Política de respuesta**. Aparecerá el panel de Política de intercambio de clave Internet de respuesta.
5. En el campo Protección de identidad, deseleccione la **Negociación de modalidad agresiva IKE (sin protección de identidad)**.
6. Pulse **Aceptar** para regresar al diálogo de propiedades.
7. Pulse **Aceptar** otra vez para guardar los cambios.

**Nota:** Al establecer el campo de protección de identidad, el cambio es efectivo para todos los intercambios con los servidores de claves remotos, ya que solamente hay una política IKE de respuesta para todo el sistema. La negociación de modalidad principal asegura que el sistema inicial solamente puede solicitar un intercambio de política de clave de modalidad principal.

**Conceptos relacionados**:

"Gestión de claves" en la página 9
Una VPN dinámica ofrece seguridad adicional para las comunicaciones mediante el protocolo IKE (intercambio de claves de Internet) para la gestión de claves. IKE permite a los servidores VPN de cada extremo de la conexión negociar nuevas claves a intervalos determinados.

**Tareas relacionadas**:

Digital Certificate Manager

## Configuración de una política de datos

Una política de datos define el nivel de autenticación o cifrado con que se protegen los datos que fluyen a través de la VPN.

Los sistemas que establecen la comunicación se ponen de acuerdo sobre estos atributos durante las negociaciones de la fase 2 del protocolo IKE (intercambio de claves de Internet). No es necesario definir una política de datos cuando se crea una conexión manual. Además, si crea la VPN con el asistente Conexión, éste puede crear una política de datos.

Para definir una política de datos o realizar cambios en una existente, siga estos pasos:

1. En IBM Navigator for i, expanda **Red** > **Políticas IP** > **Red privada virtual** y, a continuación, pulse **Políticas de seguridad IP**.

2. Para crear una política de datos nueva, pulse con el botón derecho del ratón **Políticas de datos** y seleccione **Política de datos nueva**. Para realizar cambios en una política de datos existente, pulse con el botón derecho del ratón en **Políticas de datos** y seleccione **Abrir**. Pulse con el botón derecho del ratón en la política de datos que desee cambiar y seleccione **Propiedades**.
3. Cumplimente todas las hojas de propiedades. Pulse **Ayuda** si tiene preguntas acerca de cómo cumplimentar una página o alguno de los campos.
4. Pulse **Aceptar** para guardar los cambios.

**Conceptos relacionados**:

"Gestión de claves" en la página 9
Una VPN dinámica ofrece seguridad adicional para las comunicaciones mediante el protocolo IKE (intercambio de claves de Internet) para la gestión de claves. IKE permite a los servidores VPN de cada extremo de la conexión negociar nuevas claves a intervalos determinados.

## Configuración de una conexión VPN segura

Tras haber definido las políticas de seguridad para la conexión, deberá configurar la conexión segura.

Para las conexiones dinámicas, el objeto de conexión segura incluye un grupo de claves dinámicas y una conexión de claves dinámicas.

El **grupo de claves dinámicas** define las características comunes de una o varias conexiones VPN. La configuración de un grupo de claves dinámicas permite utilizar las mismas políticas, pero puntos finales de datos distintos, para cada conexión del grupo. Los grupos de claves dinámicas también permiten negociar con iniciadores remotos satisfactoriamente cuando los puntos finales de datos propuestos por el sistema remoto no se conocen específicamente de antemano. Lo lleva a cabo asociando la información de políticas del grupo de claves dinámicas con una norma de filtro de políticas que tenga un tipo de acción IPSec. Si los puntos finales de datos específicos que ofrece el iniciador remoto caen dentro del rango especificado en la norma de filtro IPSec, pueden estar sujetos a la política definida en el grupo de claves dinámicas.

La **conexión de claves dinámicas** define las características de las conexiones de datos individuales entre los pares de puntos finales. La conexión de claves dinámicas existe dentro del grupo de claves dinámicas. Después de configurar un grupo de claves dinámicas para describir qué conexiones de políticas del grupo se utilizan, necesita crear conexiones de claves dinámicas individuales para las conexiones que inicie localmente.

Para configurar el objeto de conexión segura, complete las tareas Parte 1 y Parte 2:

**Conceptos relacionados**:

"Configuración de políticas de seguridad de VPN" en la página 53
Después de determinar cómo va a utilizar la VPN, debe definir sus políticas de seguridad VPN.

"Configuración de normas de paquetes VPN" en la página 57
Si está creando una conexión por primera vez, permita que VPN genere automáticamente las normas de paquetes VPN. Puede llevarlo a cabo utilizando el asistente Nueva conexión o las páginas de propiedades de VPN para configurar la conexión.

**Tareas relacionadas**:

"Activación de las normas de paquetes VPN" en la página 61
Para poder iniciar conexiones VPN, primero debe activar las normas de paquetes VPN.

### Parte 1: Configurar un grupo de claves dinámicas

1. En IBM Navigator for i, expanda **Red** > **Políticas IP** > **Red privada virtual** y luego pulse **Conexiones seguras**.
2. Pulse con el botón derecho del ratón **Por grupo** y seleccione **Nuevo grupo de claves dinámicas**.
3. Pulse **Ayuda** si tiene preguntas acerca de cómo cumplimentar una página o alguno de los campos.

4. Pulse **Aceptar** para guardar los cambios.

### Parte 2: configurar una conexión de claves dinámicas

1. En IBM Navigator for i, expanda **Red** > **Políticas IP** > **Red privada virtual** y luego pulse **Conexiones seguras**.
2. Pulse con el botón derecho del ratón **Por grupo** y seleccione **Abrir**.
3. Pulse con el botón derecho del ratón en el grupo de claves dinámicas que ha creado en la parte uno y seleccione **Conexión de clave dinámica nueva**.
4. Pulse **Ayuda** si tiene preguntas acerca de cómo cumplimentar una página o alguno de los campos.
5. Pulse **Aceptar** para guardar los cambios.

Tras completar estos pasos, necesitará activar las normas de paquetes que la conexión requiere para funcionar correctamente.

**Nota:** En la mayoría de los casos, permita que la interfaz VPN genere las normas de paquetes VPN automáticamente seleccionando la opción **Generar el siguiente filtro de políticas para este grupo** en la página**Grupo de claves dinámicas - Conexiones**. Sin embargo, si selecciona la opción **La norma de filtro de políticas se definirá en las Normas de paquetes**, deberá configurar normas de paquetes VPN mediante el editor de normas de paquetes y, a continuación, activarlas.

## Configuración de una conexión manual

Una conexión manual es una conexión en la que deben configurarse todas las propiedades de VPN sin utilizar asistentes.

Además, ambos extremos de la conexión requieren la configuración de varios elementos que deben coincidir *exactamente*. Por ejemplo, las claves de entrada, deben coincidir con las claves de salida del sistema remoto, de otro modo fallará la conexión.

Las conexiones manuales utilizan claves estáticas que no se renuevan ni cambian mientras la conexión está activa. Debe detener una conexión manual para cambiar la clave asociada. Si considera que supone un riesgo para la seguridad y ambos extremos de la conexión soportan el protocolo IKE (intercambio de claves de Internet), considere la posibilidad de configurar una conexión dinámica como alternativa.

Para definir las propiedades para la conexión manual, siga estos pasos:

1. En IBM Navigator for i, expanda **Red** > **Políticas IP** > **Red privada virtual** y pulse **Conexiones seguras**.
2. Pulse con el botón derecho del ratón **Todas las conexiones** y seleccione **Nueva conexión manual**.
3. Cumplimente todas las hojas de propiedades. Pulse **Ayuda** si tiene preguntas acerca de cómo cumplimentar una página o alguno de los campos.
4. Pulse **Aceptar** para guardar los cambios.

**Nota:** En la mayoría de los casos, permita que la interfaz VPN genere las normas de paquetes VPN automáticamente seleccionando la opción **Generar un filtro de políticas que coincida con los puntos finales de datos** en la página **Conexión manual - Conexión**. Sin embargo, si selecciona la opción **La norma de filtro de políticas se definirá en las Normas de paquetes**, deberá configurar una norma de filtro de políticas manualmente y, a continuación, activarlas.

**Tareas relacionadas**:

"Configuración de una norma de filtro de políticas" en la página 59
Sólo debe realizar esta tarea si ha especificado que no desea que VPN genere las normas de filtro de políticas automáticamente.

## Configuración de una conexión dinámica

Una conexión dinámica genera y negocia dinámicamente las claves que protegen la conexión, mientras está activa, mediante el protocolo IKE.

Complete el asistente Nueva conexión de clave dinámica para configurar una conexión dinámica siguiendo estos pasos:

1. En IBM Navigator for i, expanda **Red** > **Políticas IP** > **Red privada virtual** y luego pulse **Conexiones seguras**.
2. Pulse con el botón derecho del ratón **Por grupo** y seleccione **Abrir**.
3. Pulse con el botón derecho del ratón en el grupo de claves dinámicas específico y seleccione **Nueva conexión de clave dinámica**.
4. Cumplimente todas las hojas de propiedades. Pulse **Ayuda** si tiene preguntas acerca de cómo cumplimentar una página o alguno de los campos.
5. Pulse **Aceptar** para guardar los cambios.

## Configuración de normas de paquetes VPN

Si está creando una conexión por primera vez, permita que VPN genere automáticamente las normas de paquetes VPN. Puede llevarlo a cabo utilizando el asistente Nueva conexión o las páginas de propiedades de VPN para configurar la conexión.

Si decide crear normas de paquetes mediante el editor de normas de paquetes de IBM Navigator for i, cree también cualquier otra norma de esta forma. A la inversa, si desea que VPN genere las normas de filtrado de políticas, deberá crear todas las normas de filtrado de políticas adicionales de esta forma.

En general, las VPN requieren dos tipos de normas de filtro: normas de filtro anteriores a IPSec y normas de filtro de políticas. Consulte los temas que se indican más abajo para aprender a configurar estas normas mediante el editor de normas de paquetes de IBM Navigator for i. Si desea obtener información acerca de otras opciones de VPN y de filtrado, consulte la sección VPN y filtrado IP del tema relativo a los conceptos de VPN.

- Configurar la norma de filtro anterior a IPSec

  Las normas anteriores a IPSec son todas las normas del sistema que preceden a las normas con un tipo de acción IPSec. Este tema sólo trata las normas anteriores a IPSec que VPN necesita para funcionar correctamente. En este caso, las normas anteriores a IPSec son un par de normas que permiten el proceso IKE en la conexión. IKE permite generar y negociar claves dinámicas para la conexión. Puede necesitar añadir otras normas anteriores a IPSec en función de su entorno de red particular y de su política de seguridad.

  **Nota:** Sólo es necesario configurar este tipo de norma anterior a IPSec si ya tiene otras normas que permiten IKE para sistemas específicos. Si en el sistema no existen normas de filtro específicamente escritas para permitir el tráfico IKE, el tráfico IKE se permite implícitamente.
- Configurar una norma de filtro de políticas

  La norma de filtro de políticas define el tráfico que puede utilizar la VPN y qué política de protección de datos debe aplicarse a este tráfico.

### Aspectos a considerar antes de empezar

Al añadir normas de filtro a una interfaz, el sistema añade automáticamente una norma DENY predeterminada para esa interfaz. Esto significa que se deniega cualquier tráfico no permitido explícitamente. No es posible ver ni cambiar esta norma. Como resultado, el tráfico que anteriormente funcionaba falla misteriosamente al activar las normas de filtrado de VPN. Si desea permitir en la interfaz un tráfico que no sea VPN, debe añadir explícitamente normas PERMIT para hacerlo.

Tras configurar las normas de filtro apropiadas, debe definir la interfaz a la que se aplicarán y, a continuación, activarlas.

Es esencial que configure las normas de filtro de forma apropiada. Si no es así, las normas de filtrado pueden bloquear todo el tráfico IP entrante y saliente del sistema. Esto incluye la conexión a IBM Navigator for i, que se utiliza para configurar las normas de filtro.

Si las normas de filtro no permiten el tráfico de IBM i, IBM Navigator for i no podrá comunicarse con el sistema. Si se encuentra en esta situación, necesitará conectarse al sistema mediante una interfaz que aún tenga conectividad, como por ejemplo, la consola de operaciones. Utilice el mandato RMVTCPTBL para eliminar todos los filtros del sistema. Este mandato también finaliza los servidores *VPN y, a continuación, los reinicia. Después, configure los filtros y reactívelos.

**Conceptos relacionados**:

"VPN y filtrado IP" en la página 16
El filtrado IP y VPN están estrechamente relacionados. De hecho, la mayoría de conexiones VPN requieren normas de filtro para funcionar correctamente. Este tema proporciona información acerca de los filtros necesarios para VPN, y también acerca de otros conceptos de filtrado relacionados con VPN.

**Tareas relacionadas**:

"Configuración de una conexión VPN segura" en la página 55
Tras haber definido las políticas de seguridad para la conexión, deberá configurar la conexión segura.

"Configurar la norma de filtro anterior a IPSec"
Sólo debe realizar esta tarea si ha especificado que no desea que VPN genere las normas de filtro de políticas automáticamente.

"Configuración de una norma de filtro de políticas" en la página 59
Sólo debe realizar esta tarea si ha especificado que no desea que VPN genere las normas de filtro de políticas automáticamente.

"Definición de una interfaz para las normas de filtrado VPN" en la página 61
Después de configurar las normas de paquetes de VPN y cualquier otra norma que necesite para habilitar la conexión VPN, debe definir la interfaz a la que aplicarlas.

"Activación de las normas de paquetes VPN" en la página 61
Para poder iniciar conexiones VPN, primero debe activar las normas de paquetes VPN.

## Configurar la norma de filtro anterior a IPSec

Sólo debe realizar esta tarea si ha especificado que no desea que VPN genere las normas de filtro de políticas automáticamente.

Un par de servidores de intercambio de claves de Internet (IKE) negocian y renuevan las claves dinámicamente. IKE utiliza el puerto conocido públicamente 500. Para que IKE funcione correctamente, debe permitir el tráfico IP de los datagramas UDP a través del puerto 500. Para ello, tendrá que crear un par de normas de filtro; una para el tráfico entrante y otra para el tráfico saliente, de forma que la conexión pueda negociar claves dinámicamente para proteger la conexión:

1. En IBM Navigator for i, expanda **Red** > **Políticas IP** y pulse **Reglas de paquete**.
2. En el panel **Reglas de paquete**, seleccione **Acciones** > **Editor de reglas**. De esta forma se visualizará el editor Normas de paquete, que le permitirá crear o editar normas NAT y de filtro para el sistema.
3. En el panel de Bienvenida, seleccione **Crear un archivo de reglas de paquete nuevo** y pulse **Aceptar**.
4. Si aparece el panel **Iniciación**, lea la guía del usuario sobre el panel **Iniciación** y pulse **Aceptar**.
5. En el editor Reglas de paquete, seleccione **Insertar** > **Filtro**.
6. En la página **General**, especifique un nombre de conjunto para las normas de filtro VPN. Es recomendable crear al menos tres conjuntos distintos: uno para las normas de filtro anteriores a IPSec, uno para las normas de filtro de políticas y otra para las normas de filtro DENY y PERMIT misceláneas. El nombre del conjunto que contiene las normas de filtro anteriores a IPSec deben llevar el prefijo *preipsec*. Por ejemplo, preipsecfilters.

7. En el campo **Acción**, seleccione **PERMIT** en la lista desplegable.
8. En el campo **Acción**, seleccione **OUTBOUND** en la lista desplegable.
9. En el campo **Nombre de dirección de origen**, seleccione **=** en la lista desplegable y, a continuación, especifique la dirección IP del servidor de claves local en el segundo campo. Ha especificado la dirección IP del servidor de claves local en la política IKE.
10. En el campo **Nombre de dirección de destino**, seleccione **=** en la lista desplegable y, a continuación, especifique la dirección IP del servidor de claves remoto en el segundo campo. Ha especificado la dirección IP del servidor de claves remoto en la política IKE.
11. En la página **Servicios**, seleccione **Servicio**. De esta forma se habilitan los campos **Protocolo**, **Puerto origen** y **Puerto destino**.
12. En el campo **Protocolo**, seleccione **UDP** en la lista desplegable.
13. Para **Puerto origen**, seleccione **=** en el primer campo y, a continuación especifique `500` en el segundo campo.
14. Repita el paso anterior para **Puerto destino**.
15. Pulse **Aceptar**.
16. Repita estos pasos para configurar el filtro INBOUND. Utilice el mismo nombre de conjunto e invierta las direcciones de la forma necesaria.

**Nota:** Hay una opción menos segura pero más sencilla para permitir el tráfico IKE a través de la conexión, que consiste en configurar sólo el filtro anterior a IPSec y utilizar valores de comodín (*) en los campos**Dirección**, **Nombre de dirección de origen** y **Nombre de dirección de destino**.

El siguiente paso es configurar una norma de filtro de políticas para definir qué tráfico IP debe proteger la conexión VPN.

**Conceptos relacionados**:

"Configuración de normas de paquetes VPN" en la página 57
Si está creando una conexión por primera vez, permita que VPN genere automáticamente las normas de paquetes VPN. Puede llevarlo a cabo utilizando el asistente Nueva conexión o las páginas de propiedades de VPN para configurar la conexión.

**Tareas relacionadas**:

"Configuración de una norma de filtro de políticas"
Sólo debe realizar esta tarea si ha especificado que no desea que VPN genere las normas de filtro de políticas automáticamente.

## Configuración de una norma de filtro de políticas

Sólo debe realizar esta tarea si ha especificado que no desea que VPN genere las normas de filtro de políticas automáticamente.

La norma de filtro de políticas (una norma en la que acción=IPSEC) define qué direcciones, protocolos y puertos pueden utilizar la VPN. También identifica la política que se aplicará al tráfico en la conexión VPN. Para configurar una norma de filtro de políticas, siga estos pasos:

**Nota:** Si acaba de configurar la norma anterior a IPSec (sólo para conexiones dinámicas), el editor de normas de paquetes aún estará abierto; vaya al paso 4.

1. En IBM Navigator for i, expanda **Red** > **Políticas IP** y pulse **Reglas de paquete**.
2. Pulse **Acciones** > **Editor de reglas**. De esta forma se visualizará el editor Reglas de paquete, que le permitirá crear o editar reglas NAT y de filtro para el sistema.
3. En el panel de Bienvenida, seleccione **Crear un archivo de reglas de paquete nuevo** y pulse **Aceptar**.
4. En el editor Reglas de paquete, seleccione **Insertar** > **Filtro**.

5. En la página **General**, especifique un nombre de conjunto para las reglas de filtro VPN. Es recomendable crear al menos tres conjuntos distintos: uno para las normas de filtro anteriores a IPSec, uno para las normas de filtro de políticas y otra para las normas de filtro DENY y PERMIT misceláneas. Por ejemplo, `policyfilters`
6. En el campo **Acción**, seleccione **IPSEC** en la lista desplegable. El campo **Dirección** toma OUTBOUND de forma predeterminada y no puede cambiarlo. El campo **Acción** se especifica como OUTBOUND, ya que es el único sentido en que IPSec se aplicará a los paquetes que no están ya en el protocolo ESP.
7. Para **Nombre de la dirección de origen**, seleccione **=** en el primer campo y, a continuación, especifique la dirección IP del punto final de datos local en el segundo campo. También puede especificar un rango de direcciones IP o una dirección IP más una máscara de subred tras haberlos definido mediante la función **Definir direcciones**.
8. Para **Nombre de dirección de destino**, seleccione **=** en el primer campo y, a continuación, especifique la dirección IP del punto final de datos remoto en el segundo campo. También puede especificar un rango de direcciones IP o una dirección IP más una máscara de subred tras haberlos definido mediante la función **Definir direcciones**.
9. En el campo **Registro por diario**, especifique el nivel de registro por diario que necesita.
10. En el campo **Grupo de conexión**, seleccione la definición de conexión a la que se aplican estas reglas de filtro.
11. (opcional) Especifique una descripción.
12. En la página **Servicios**, seleccione **Servicio**. De esta forma se habilitan los campos **Protocolo**, **Puerto origen** y **Puerto destino**.
13. En los campos **Protocolo**, **Puerto de origen** y **Puerto de destino**, seleccione el valor apropiado para el tráfico. O puede seleccionar el asterisco (*) en la lista desplegable. De esta forma, cualquier protocolo puede utilizar la VPN a través de cualquier puerto.
14. Pulse **Aceptar**.

El siguiente paso consiste en definir la interfaz a la que se aplican estas normas de filtro.

**Nota:** Al añadir normas de filtro para una interfaz, el sistema añade automáticamente una norma DENY predeterminada para la interfaz. Esto significa que se deniega cualquier tráfico no permitido explícitamente. No es posible ver ni cambiar esta norma. Como consecuencia, verá que algunas conexiones que anteriormente funcionaban, fallan misteriosamente tras activar sus normas de paquetes VPN. Si desea permitir en la interfaz un tráfico que no sea VPN, debe añadir explícitamente normas PERMIT para hacerlo.

**Conceptos relacionados**:

"Configuración de normas de paquetes VPN" en la página 57
Si está creando una conexión por primera vez, permita que VPN genere automáticamente las normas de paquetes VPN. Puede llevarlo a cabo utilizando el asistente Nueva conexión o las páginas de propiedades de VPN para configurar la conexión.

**Tareas relacionadas**:

"Configuración de una conexión manual" en la página 56
Una conexión manual es una conexión en la que deben configurarse todas las propiedades de VPN sin utilizar asistentes.

"Configurar la norma de filtro anterior a IPSec" en la página 58
Sólo debe realizar esta tarea si ha especificado que no desea que VPN genere las normas de filtro de políticas automáticamente.

"Definición de una interfaz para las normas de filtrado VPN" en la página 61
Después de configurar las normas de paquetes de VPN y cualquier otra norma que necesite para habilitar la conexión VPN, debe definir la interfaz a la que aplicarlas.

## Definición de una interfaz para las normas de filtrado VPN

Después de configurar las normas de paquetes de VPN y cualquier otra norma que necesite para habilitar la conexión VPN, debe definir la interfaz a la que aplicarlas.

Para definir una interfaz a la que pueda aplicar las normas de filtro VPN, siga estos pasos:

**Nota:** Si acaba de configurar las normas de paquetes VPN, la interfaz de normas de paquetes aún estará abierta; vaya al cuarto paso.

1. En IBM Navigator for i, expanda **Red** > **Políticas IP** y luego pulse **Reglas de paquete**.
2. Pulse **Acciones** > **Editor de reglas**. De esta forma se visualizará el editor Reglas de paquete, que le permitirá crear o editar normas NAT y de filtro para el sistema.
3. En el panel de Bienvenida, seleccione **Crear un archivo de reglas de paquete nuevo** y pulse **Aceptar**.
4. En el editor Reglas de paquete, seleccione **Insertar** > **Interfaz de filtro**.
5. En la página **General**, seleccione **Nombre de línea** y, a continuación, seleccione la descripción de línea a la que se aplicarán las normas de paquetes VPN en la lista desplegable.
6. (opcional) Especifique una descripción.
7. En la página **Conjuntos de filtros**, pulse **Añadir** para añadir el nombre de cada conjunto a los filtros que acaba de configurar.
8. Pulse **Aceptar**.
9. Guarde el archivo de normas. El archivo se guarda en el sistema de archivos integrado del sistema con la extensión i3p.

   **Nota:** No guarde el archivo en el siguiente directorio:

   `/QIBM/UserData/OS400/TCPIP/RULEGEN`

   Este directorio es de uso exclusivo del sistema. Si alguna vez necesita utilizar el mandato RMVTCPTBL *ALL para desactivar las normas de paquetes, el mandato suprimirá todos los archivos que se encuentren dentro de este directorio.

Después de definir una interfaz para las normas de filtro, debe activarlas para poder iniciar la VPN.

**Conceptos relacionados**:

"Configuración de normas de paquetes VPN" en la página 57
Si está creando una conexión por primera vez, permita que VPN genere automáticamente las normas de paquetes VPN. Puede llevarlo a cabo utilizando el asistente Nueva conexión o las páginas de propiedades de VPN para configurar la conexión.

**Tareas relacionadas**:

"Configuración de una norma de filtro de políticas" en la página 59
Sólo debe realizar esta tarea si ha especificado que no desea que VPN genere las normas de filtro de políticas automáticamente.

"Activación de las normas de paquetes VPN"
Para poder iniciar conexiones VPN, primero debe activar las normas de paquetes VPN.

## Activación de las normas de paquetes VPN

Para poder iniciar conexiones VPN, primero debe activar las normas de paquetes VPN.

No puede activar (ni desactivar) las normas de filtrado mientras se estén ejecutando conexiones VPN en el sistema. Por tanto, antes de activar las normas de filtrado VPN, asegúrese de que no hay ninguna conexión activa asociada con éstas.

Si ha creado las conexiones VPN con el asistente Nueva conexión, puede elegir que las normas asociadas se activen automáticamente. Tenga en cuenta que, si existen otras normas de paquetes activas en cualquiera de las interfaces que especifique, las normas de filtrado de políticas VPN las sustituirán.

Si elige activar las normas generadas por VPN mediante el editor de normas de paquetes, siga estos pasos:

1. En IBM Navigator for i, expanda la **Red** > **Políticas IP** y luego pulse **Reglas de paquete**.
2. Pulse **Acciones** > **Activar reglas**. De esta forma, se abrirá el panel **Activar reglas de paquete**.
3. Seleccione si desea activar sólo las normas generadas por VPN, sólo un archivo seleccionado o ambos. Puede elegir la última opción (ambos), por ejemplo, si tiene diversas normas PERMIT y DENY que desea forzar en la interfaz, además de las normas generadas por VPN.
4. Seleccione la interfaz en la que desea activar las normas. Puede elegir activarlas en una interfaz específica, en un identificador punto a punto o en todas las interfaces y en todos los identificadores punto a punto.
5. Pulse **Aceptar** en el recuadro de diálogo para confirmar que desea verificar y activar las normas en la interfaz o interfaces que ha especificado. Después de pulsar Aceptar, el sistema comprueba si existen errores de sintaxis y semántica en las normas e informa de los resultados en una ventana de mensaje situada en la parte inferior del editor.

Después de haber activado las normas de filtrado, podrá iniciar la conexión VPN.

**Conceptos relacionados**:

"Configuración de normas de paquetes VPN" en la página 57
Si está creando una conexión por primera vez, permita que VPN genere automáticamente las normas de paquetes VPN. Puede llevarlo a cabo utilizando el asistente Nueva conexión o las páginas de propiedades de VPN para configurar la conexión.

**Tareas relacionadas**:

"Configuración de una conexión VPN segura" en la página 55
Tras haber definido las políticas de seguridad para la conexión, deberá configurar la conexión segura.

"Definición de una interfaz para las normas de filtrado VPN" en la página 61
Después de configurar las normas de paquetes de VPN y cualquier otra norma que necesite para habilitar la conexión VPN, debe definir la interfaz a la que aplicarlas.

"Inicio de una conexión VPN" en la página 64
Complete esta tarea para iniciar las conexiones que se inician localmente.

## Configuración de la confidencialidad de flujo de tráfico

Si la política de datos se configura para la modalidad de túnel, puede utilizar la confidencialidad de flujo de tráfico (TFC) para ocultar la longitud real de los paquetes de datos transferidos a través de una conexión VPN.

TFC añade un relleno adicional a los paquetes enviados y envía paquetes ficticios con distintas longitudes a intervalos aleatorios para ocultar la longitud real de los paquetes. Utilice TFC para obtener una seguridad adicional contra los atacantes que puedan averiguar el tipo de datos que se está enviando a partir de la longitud del paquete. Cuando se habilita TFC, se obtiene una mayor seguridad, aunque se reduce el rendimiento del sistema. Por lo tanto, debe probar el rendimiento de los sistemas antes y después de habilitar TFC en una conexión VPN. IKE no negocia la TFC, y un usuario sólo debe habilitar TFC cuando ambos sistemas le den soporte.

Para habilitar TFC en una conexión VPN, siga estos pasos:

1. En IBM Navigator for i, expanda **Red** > **Políticas IP** > **Red privada virtual**.
2. Pulse **Conexiones seguras**, pulse con el botón derecho del ratón **Todas las conexiones** y seleccione **Abrir**.
3. Pulse con el botón derecho del ratón la conexión en la que desee habilitar TFC y seleccione **Propiedades**.
4. En la pestaña **General**, seleccione **Utilizar Confidencialidad de flujo de tráfico (TFC) cuando esté en la modalidad de túnel**.

## Configuración del número de secuencia ampliado

Puede utilizar el número de secuencia ampliado (ESN) para aumentar la velocidad de transferencia de datos de una conexión VPN.

ESN permite transmitir grandes volúmenes de datos a una gran velocidad sin necesidad de volver a aplicar las claves. La conexión VPN utiliza números de secuencia de 64 bits, en lugar de números de 32 bits a través de IPSec. La utilización de números de secuencia de 64 bits permite disponer de más tiempo antes de volver a aplicar las claves, lo que evita que se agoten los números de secuencia y minimiza el uso de recursos del sistema.

Para habilitar ESN en una conexión VPN, siga estos pasos:

1. En IBM Navigator for i, expanda **Red** > **Todas las tareas** > **Políticas IP** > **Red privada virtual**.
2. Pulse **Propiedades**.
3. En la pestaña **General**, seleccione **Utilizar Número de secuencia ampliado (ESN)**.

## Configuración de llenar desde paquete

Puede generarse automáticamente una conexión de host a host a un único sistema de destino basándose en la información del paquete.

Llenar desde paquete permite que se negocien conexiones VPN individuales utilizando puntos finales basándose en la información encontrada en un paquete de salida. Los puntos finales deben estar dentro del rango predefinido de puntos finales permitidos para el túnel de la VPN.

Para configurar una conexión para habilitar llenar desde paquete, siga estos pasos:

1. En IBM Navigator for i, expanda **Red** > **Políticas IP** > **Red privada virtual** y pulse **Conexiones seguras**.
2. Pulse con el botón derecho del ratón **Todas las conexiones** y seleccione **Abrir**.
3. Pulse con el botón derecho del ratón en la conexión que será el *sistema local* y seleccione **Propiedades**.
4. En la pestaña **General**, seleccione **Iniciar por solicitud**. Pulse **Aceptar**.
5. Vuelva a pulsar con el botón derecho del ratón en la conexión y seleccione **Propiedades de grupo**.
6. En la pestaña **General**, seleccione **El sistema local es un host y el sistema remoto es una pasarela**.
7. En la pestaña **Conexiones**, **Personalizar coincidencia con filtro de política**. Pulse **Personalizar**.
8. Seleccione **Valor único** para la **Dirección remota**. Pulse **Aceptar**.

## Configuración de VPN NPF para VIPA

Puede permitir que se apliquen conexiones VPN Sin filtro de política (NPF) automáticamente como las interfaces preferidas para direcciones IP virtuales (VIPA).

Antes de IBM i 7.2, la conexión NPF sólo se cargaría para la descripción de línea actualmente indicada como elección local para el salto siguiente dada una ruta al destino deseado. Esto causa problemas si se han configurado las direcciones IP virtuales, lo que podría permitir varias vías de acceso a un destino concreto.

Si se carga una conexión NPF y la dirección IP local está destinada a ser una dirección VIPA, la conexión se cargará para cualquier descripción de línea adicional que se incluya en la lista de interfaces locales preferidas de la dirección IP.

Si la VPN configurada para NPF no funciona con una dirección VIPA concreta, lleve a cabo una de las siguientes opciones:

NOTA: el siguiente ejemplo es específicamente para configuraciones VPN de conectividad IBM Universal Care. En este ejemplo, la dirección IP de la pasarela IBM es 129.42.160.16.

1. Defina una ruta de host para las dos pasarelas de IBM que enlazan la ruta a una interfaz local determinada ADDTCPRTE RTEDEST('129.42.160.16') SUBNETMASK(*HOST) NEXTHOP('192.168.20.86') BINDIFC('192.168.20.103')
2. Inhabilitar todas excepto una interfaz local que utiliza la VIPA.
3. Modificar el grupo de conexión VPN para predefinir las reglas de filtro para la conexión VPN (para eCare los nombres de grupo son QIBM01VPN1 y QIBM01VPN2). Para ello, realice lo siguiente.
   a. En IBM Navigator for i, expanda **Red** > **Políticas IP**. Pulse **Conexiones seguras**.
   b. Pulse con el botón derecho del ratón **Todas las conexiones** y seleccione **Abrir**.
   c. Pulse con el botón derecho del ratón en el perfil con la dirección IP modificada, seleccione **Propiedades de grupo**.
   d. En la pestaña Conexiones, verifique que se ha seleccionado **Generar el filtro de política siguiente para este grupo**. Pulse **Editar**.
   e. En la pestaña Direcciones locales, seleccione **Cualquier dirección IP versión 4** para el **Tipo de identificador**.
   f. En la pestaña Direcciones remotas, especifique el punto final de la VPN para el **Identificador**.
   g. En la pestaña Servicios, especifique 1701 para el **Puerto local** y el **Puerto remoto**. Seleccione UDP para el **Protocolo**. Pulse **Aceptar**.
   h. En la pestaña Interfaces, seleccione las interfaces que se comunicarán con la dirección de la pasarela de IBM. Pulse **Aceptar.**
   i. Active la regla expandiendo **Red** > **Políticas IP**
   j. Pulse **Reglas de paquete** para abrir el panel **Reglas de paquete** y pulse **Acciones** > **Activar reglas**. De esta forma, se abrirá el panel **Activar reglas de paquete**.
   k. Seleccione **Activar sólo las reglas generadas por la VPN**. Seleccione también **Activar estas reglas en todas las interfaces y todos los identificadores de filtro punto a punto**. Pulse **Aceptar**.

## Diferencias de configuración de IKEv2

Comparación entre la configuración de IKEv1 e IKEv2.

Los objetos existentes se han utilizado todo los posible para permitir los intercambios de IKEv1 o IKEv2. Este diseño se ha utilizado para minimizar el impacto sobre la interfaz GUI actual y los objetos de configuración de VPN cuando IKE versión 2 está habilitado.

- Para habilitar IKEv2, se suministra un valor de Versión IKE en la definición de conexión dinámica.
- Pueden utilizarse políticas de intercambio de claves tanto para IKEv1 como para IKEv2.
- No hay más diferencias en los demás atributos, como por ejemplo los identificadores de política de intercambio de claves (todos siguen estando soportados) y las transformaciones.
- Los valores de modalidad principal/modalidad agresiva se ignoran si se utiliza la política de intercambio de claves para IKEv2.
- Son necesarios IBM i 7.1 y IBM Navigator for i para configurar una conexión IKEv2.

**Conceptos relacionados**:

"IKE versión 2" en la página 11
IKE versión 2 es una mejora del protocolo de intercambio de claves de Internet.

## Inicio de una conexión VPN

Complete esta tarea para iniciar las conexiones que se inician localmente.

Estas instrucciones presuponen que ha configurado correctamente la conexión VPN. Siga estos pasos para iniciar la conexión VPN:

1. En IBM Navigator for i, expanda **Red** > **Todas las tareas** > **Políticas IP** > **Red privada virtual**.

2. Si el servidor VPN no está iniciado, pulse **Iniciar servidor VPN**. De esta forma, se iniciará el servidor VPN.
3. Asegúrese de que las normas de paquetes están activadas.
4. Expanda **Red** > **Políticas IP** > **Red privada virtual**.
5. Pulse **Conexiones seguras**.
6. Pulse con el botón derecho del ratón **Todas las conexiones** y seleccione **Abrir** para visualizar una lista de conexiones.
7. Pulse con el botón derecho del ratón la conexión que desee iniciar y seleccione **Iniciar**. Para iniciar varias varias conexiones, seleccione cada conexión que desee iniciar, pulse el botón derecho del ratón y seleccione **Iniciar**.

El mandato STRVPNCNN le permite iniciar una conexión VPN desde la línea de mandatos o mediante programación.

**Tareas relacionadas**:

"Activación de las normas de paquetes VPN" en la página 61
Para poder iniciar conexiones VPN, primero debe activar las normas de paquetes VPN.

"Iniciación a la resolución de problemas de VPN" en la página 68
Complete esta tarea para conocer los distintos métodos posibles para determinar los problemas de VPN que pueden surgir en el sistema.

## Gestión de VPN

Puede utilizar la interfaz VPN de IBM Navigator for i para manejar todas las tareas de gestión de VPN como, por ejemplo, detener una conexión y visualizar atributos de conexión.

Utilice la interfaz VPN de IBM Navigator for i para manejar todas las tareas de gestión, que son:

## Establecimiento de los atributos predeterminados de las conexiones

Los valores predeterminados se rellenan los paneles que utilizará para crear nuevas políticas y conexiones. Puede establecer los valores predeterminados para los niveles de seguridad, la gestión de sesiones con clave, el tiempo de vida de la clave y los tiempos de vida de las conexiones.

Los valores de seguridad predeterminados figuran en varios campos cuando se crean objetos VPN nuevos.

Para establecer los valores de seguridad predeterminados para las conexiones VPN, siga estos pasos:

1. En IBM Navigator for i, expanda **Red** > **Todas las tareas** > **Políticas IP** > **Red privada virtual**.
2. Pulse **Valores predeterminados**.
3. Pulse **Ayuda** si tiene preguntas acerca de cómo cumplimentar una página o alguno de los campos.
4. Pulse **Aceptar** una vez haya cumplimentado todas las hojas de propiedades.

## Restablecimiento de conexiones en estado de error

El restablecimiento de las conexiones con errores las devuelve al estado de desocupado.

Para renovar una conexión cuyo estado sea de error, siga estos pasos:

1. En IBM Navigator for i, expanda **Red** > **Políticas IP** > **Red privada virtual** y luego pulse **Conexiones seguras**.
2. Pulse con el botón derecho del ratón **Todas las conexiones** y seleccione **Abrir** para visualizar una lista de conexiones en el panel derecho.

3. Pulse con el botón derecho del ratón la conexión que desea restablecer y seleccione **Restablecer**. De esta manera el estado de la conexión se restablece desocupado. Para restablecer varias conexiones que se encuentran en estado de error, seleccione cada conexión que desee restablecer, pulse el botón derecho del ratón y seleccione **Restablecer**.

## Visualización de la información de errores

Complete esta tarea que le ayudará a determinar por qué la conexión da error.

Para visualizar la información sobre las conexiones con errores, siga estos pasos:

1. En IBM Navigator for i, expanda **Red** > **Políticas IP** > **Red privada virtual** y pulse **Conexiones seguras**.
2. Pulse con el botón derecho del ratón**Todas las conexiones** para visualizar una lista de conexiones en el panel derecho.
3. Pulse con el botón derecho del ratón la conexión activa o por solicitud que desea ver y seleccione **Información de error**.

**Tareas relacionadas**:

"Iniciación a la resolución de problemas de VPN" en la página 68
Complete esta tarea para conocer los distintos métodos posibles para determinar los problemas de VPN que pueden surgir en el sistema.

## Visualización de los atributos de las conexiones activas

Complete esta tarea para comprobar el estado y otros atributos de las conexiones activas.

Para visualizar los atributos actuales de una conexión activa o bajo petición, siga estos pasos:

1. En IBM Navigator for i, expanda **Red** > **Políticas IP** > **Red privada virtual** y pulse **Conexiones seguras**.
2. Pulse con el botón derecho del ratón**Todas las conexiones** y seleccione **Abrir** para visualizar una lista de conexiones en el panel derecho.
3. Pulse con el botón derecho del ratón la conexión activa o por solicitud que desea ver y seleccione **Propiedades**.
4. Vaya a la página **Atributos actuales** para ver los atributos de la conexión.

También puede visualizar los atributos de todas las conexiones en la ventana de IBM Navigator for i. De forma predeterminada, los únicos atributos que se visualizarán son Estado, Descripción y Tipo de conexión. Puede modificar qué datos se visualizarán siguiendo estos pasos:

1. En IBM Navigator for i, expanda **Red** > **Políticas IP** > **Red privada virtual** y pulse **Conexiones seguras**.
2. Pulse con el botón derecho del ratón **Todas las conexiones** y seleccione **Abrir** para visualizar una lista de conexiones en el panel derecho.
3. Desde el menú **Objetos**, seleccione **Columnas**. De esta forma, se abrirá un recuadro de diálogo que le permite seleccionar qué atributos desea visualizar en el panel de IBM Navigator for i.

Debe ser consciente de que, al cambiar las columnas a visualizar, los cambios no serán específicos para un usuario o sistema determinado, sino que afectarán a todo el sistema.

**Conceptos relacionados**:

"Mensajes de error habituales del gestor de conexiones VPN" en la página 80
El gestor de conexiones VPN anota dos mensajes en las anotaciones de trabajo QTOVMAN cuando se produce un error con una conexión VPN.

## Visualización de las anotaciones de trabajo del servidor VPN

Siga estas instrucciones para visualizar las anotaciones de trabajo para el gestor de claves VPN y el gestor de conexiones VPN.

Para ver las anotaciones de trabajo del gestor de claves de la VPN o del gestor de conexiones de la VPN, siga estos pasos:

1. En IBM Navigator for i, expanda **Red** > **Todas las tareas** > **Políticas IP** > **Red privada virtual**.
2. Pulse **Visualizar trabajos de servidor** para ver los registros de trabajo.

## Visualización de los atributos de las asociaciones de seguridad

Complete esta tarea para visualizar los atributos de las SA (asociaciones de seguridad) que están asociadas con una conexión habilitada.

Para ver los atributos de las asociaciones de seguridad (SA) asociadas a una conexión habilitada. Para ello, siga estos pasos:

1. En IBM Navigator for i, expanda **Red** > **Políticas IP** > **Red privada virtual** y pulse **Conexiones seguras**.
2. Pulse con el botón derecho del ratón **Todas las conexiones** y seleccione **Abrir** para visualizar una lista de conexiones en el panel derecho.
3. Pulse con el botón derecho del ratón la conexión activa adecuada y seleccione **Asociaciones de seguridad**. El panel resultante permite ver las propiedades para cada una de las SA asociadas a una conexión específica.

## Detención de una conexión VPN

Complete esta tarea para detener las conexiones activas.

Para detener una conexión activa o bajo petición, siga estos pasos:

1. En IBM Navigator for i, expanda **Red** > **Políticas IP** > **Red privada virtual** y pulse **Conexiones seguras**.
2. Pulse con el botón derecho del ratón **Todas las conexiones** para visualizar una lista de conexiones en el panel derecho.
3. Pulse con el botón derecho del ratón la conexión que desee detener y pulse **Detener**. Para detener varias conexiones, seleccione cada conexión que desee detener, pulse el botón derecho del ratón y seleccione **Detener**.

El mandato ENDVPNCNN le permite finalizar una conexión VPN desde la línea de mandatos o mediante programación.

## Supresión de objetos de configuración de VPN

Antes de suprimir un objeto de configuración de VPN debe conocer el efecto de la conexión sobre otras conexiones VPN y grupos de conexiones.

Si está seguro de que necesita suprimir una conexión VPN de la base de datos de políticas VPN, siga estos pasos:

1. En IBM Navigator for i, expanda **Red** > **Políticas IP** > **Red privada virtual** y luego pulse **Conexiones seguras**.
2. Pulse con el botón derecho del ratón **Todas las conexiones** para visualizar una lista de conexiones en el panel derecho.
3. Pulse con el botón derecho del ratón la conexión que desea suprimir y pulse **Suprimir**.

## Resolución de problemas de VPN

Utilice los siguientes métodos de resolución de problemas para resolver algunos de los problemas básicos que puede experimentar cuando se configura una conexión VPN.

VPN es una tecnología compleja y muy cambiante que exige como mínimo un conocimiento básico de las tecnologías IPSec estándares. También deberá estar familiarizado con las normas de paquetes IP, porque VPN requiere varias normas de filtrado para poder funcionar adecuadamente. Debido a su complejidad, de vez en cuando podrá encontrarse con problemas con las conexiones VPN. La solución de problemas de VPN no es siempre una tarea fácil. Deberá comprender los entornos de su sistema y su red, así como los componentes que utiliza para gestionarlos. Los siguientes temas le ofrecen algunas indicaciones sobre cómo solucionar los distintos problemas que podría encontrar al utilizar VPN:

## Iniciación a la resolución de problemas de VPN

Complete esta tarea para conocer los distintos métodos posibles para determinar los problemas de VPN que pueden surgir en el sistema.

Hay varias formas de empezar a analizar los problemas de VPN:

1. Asegúrese siempre de haber aplicado los últimos arreglos temporales de programa (PTF).
2. Asegúrese de que cumple los requisitos mínimos de configuración de VPN.
3. Revise cualquier mensaje de error que se encuentre en la ventana de Información de error o en las anotaciones de trabajo del servidor VPN para los sistemas local y remoto. De hecho, para solucionar los problemas de conexión VPN, normalmente es necesario comprobar ambos extremos de la conexión. Además, necesita tener en cuenta que debe comprobar cuatro direcciones: los puntos finales de las conexiones local y remota, que son las direcciones donde IPSec se aplica a los paquetes IP y los puntos finales de datos remoto y local, que son las direcciones de origen y destino de los paquetes IP.
4. Si los mensajes de error que encuentra no le ofrecen suficiente información para resolver el problema, compruebe el diario del filtro IP.
5. El rastreo de la comunicación en el sistema le ofrece otra forma de encontrar información general sobre si el sistema local recibe o envía peticiones de conexión.
6. El mandato Rastrear Aplicación TCP (TRCTCPAPP) ofrece, no obstante, otra forma de identificar los problemas. Habitualmente, el Servicio de IBM utiliza el mandato TRCTCPAPP para obtener una salida de rastreo que permita analizar los problemas de conexión.

**Conceptos relacionados**:

"Requisitos de configuración de VPN" en la página 48
Para que una conexión VPN funcione correctamente en los sistemas y con los clientes de red, debe cumplir unos requisitos mínimos

"Resolución de problemas de VPN con de las anotaciones de trabajo VPN" en la página 79
Si encuentra problemas con las conexiones VPN, se recomienda siempre que analice las anotaciones de trabajo. De hecho, hay varias anotaciones de trabajo que contienen mensajes de error y otra información relacionada con un entorno VPN.

"Resolución de problemas de VPN con el rastreo de comunicaciones" en la página 86
IBM i ofrece la posibilidad de rastrear los datos de una línea de comunicaciones, como por ejemplo la interfaz LAN (red de área local) o WAN (red de área amplia). Puede que el usuario medio no entienda todo el contenido de los datos de rastreo. Sin embargo, puede utilizar las entradas de rastreo para determinar si se ha producido un intercambio de datos entre los sistemas local y remoto.

**Tareas relacionadas**:

"Visualización de la información de errores" en la página 66
Complete esta tarea que le ayudará a determinar por qué la conexión da error.

"Resolución de problemas de VPN con el diario QIPFILTER" en la página 74
Consulte esta información para aprender a utilizar las normas de filtro VPN.

“Inicio de una conexión VPN” en la página 64
Complete esta tarea para iniciar las conexiones que se inician localmente.

### Otros aspectos a comprobar

Si se produce un error tras haber configurado una conexión y no está seguro de en qué parte de la red se ha producido el error, intente reducir la complejidad de su entorno. Por ejemplo, en lugar de investigar todas las partes de una conexión VPN a la vez, empiece por la propia conexión IP. La siguiente lista ofrece algunas pautas sobre cómo iniciar el análisis de los problemas de VPN, de la conexión IP más simple a la conexión VPN más compleja:

1. Empiece con una configuración IP entre el host local y el remoto. Elimine todos los filtros IP de la interfaz que los sistemas local y remoto utilizan para comunicarse. ¿Puede realizar un PING desde el host local al host remoto?

   **Nota:** Recuerde solicitar en el mandato PING; especifique la dirección del sistema remoto y utilice PF10 para introducir más parámetros y, a continuación, especifique la dirección de IP local. Esto es especialmente importante si tiene interfaces lógicas o físicas múltiples. Le asegura que se coloquen las direcciones correctas en los paquetes PING correctos.

   Si la respuesta es **sí**, prosiga al paso 2. Si la respuesta es **no**, compruebe la configuración IP, el estado de la interfaz y las entradas de direccionamiento. Si la configuración es correcta, utilice un rastreo de comunicaciones para comprobar, por ejemplo, que una petición PING sale del sistema. Si envía una petición PING pero no recibe ninguna respuesta, es muy probable que el problema radique en la red o en el sistema remoto.

   **Nota:** Puede haber direccionadores intermedios o cortafuegos que realicen el filtrado de paquetes IP y puede que estén filtrando los paquetes PING. El PING está habitualmente basado en el protocolo ICMP. Si el PING es satisfactorio, sabrá dónde tiene conectividad. Si el PING no es satisfactorio, sólo sabrá que el PING fue anómalo. Puede intentar comprobar otros protocolos IP entre los dos sistemas, como Telnet o FTP, para verificar la conectividad.
2. Compruebe las normas de filtro para VPN y asegúrese de que están activadas. ¿Se ha iniciado el filtrado satisfactoriamente? Si la respuesta es **sí**, continúe en el paso 3. Si la respuesta es **no**, compruebe si hay mensajes de error en el panel Reglas de paquete en IBM Navigator for i. Asegúrese de que las normas de filtro no especifican NAT (Conversiones de direcciones de red) para ningún tráfico VPN.
3. Inicie la conexión VPN. ¿Se ha iniciado la conexión satisfactoriamente? Si la respuesta es **sí**, continúe con el paso 4. Si la respuesta es **no**, compruebe si hay errores en las anotaciones de trabajo QTOVMAN, QTOKVPNIKE y QTOKVPNIK2. Cuando utilice la VPN, su proveedor de servicios de Internet (ISP) y cada pasarela de seguridad de su red deben soportar los protocolos de cabecera de autenticación (AH) y de carga útil de seguridad encapsulada (ESP). La decisión de utilizar AH o ESP dependerá de las proposiciones que defina para la conexión VPN.
4. ¿Puede activar una sesión de usuario a través de la conexión VPN? Si la respuesta es **sí**, la conexión VPN funcionará tal como es necesario. Si la respuesta es **no**, compruebe las normas de paquetes y los grupos de claves dinámicas y las conexiones VPN para las definiciones de filtro que no permiten el tráfico de usuario que desea.

## Errores de configuración de VPN habituales y cómo solucionarlos

Utilice esta información para revisar los mensajes de error de VPN habituales y conocer las posibles soluciones.

**Nota:** Al configurar VPN, en realidad está creando varios objetos distintos de configuración, que VPN necesita para habilitar una conexión. En términos de la GUI de VPN, estos objetos son: las políticas de seguridad IP y las conexiones seguras. Por lo tanto, cuando esta información se refiere a un objeto, se refiere a una o varias de estas partes de la VPN.

## Mensaje de error de VPN: TCP5B28

Al intentar activar las normas de filtro en una interfaz, recibe este mensaje: TCP5B28 Violación de orden CONNECTION_DEFINITION

**Síntoma:**

Al intentar activar las normas de filtro en una interfaz determinada, ha recibido el siguiente mensaje de error:

```
TCP5B28: Violación de orden de CONECTION_DEFINITION
```

**Posible resolución:**

Las normas de filtro que ha intentado activar contenían definiciones de conexión que tenían un orden distinto que en el juego de normas activadas previamente. La forma más fácil de resolver este error es activar el archivo de normas en **todas las interfaces** en lugar de hacerlo en una interfaz determinada.

## Mensaje de error de VPN: Elemento no encontrado

Al pulsar con el botón derecho del ratón un objeto VPN y seleccionar **Propiedades** o **Eliminar**, obtiene el mensaje **Elemento no encontrado**.

**Síntoma:**

Al pulsar con el botón derecho del ratón un objeto de la ventana de Red privada virtual y seleccionar **Propiedades** o **Eliminar**, aparece el siguiente mensaje:


**Posible resolución:**

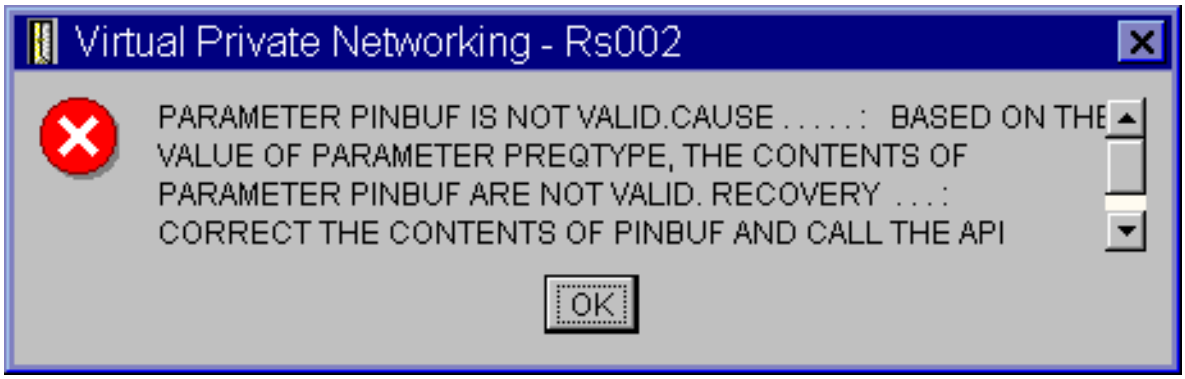
- Puede haber eliminado o renombrado el objeto y no haber renovado aún la ventana. En consecuencia, el objeto aún aparece en la ventana Red privada virtual. Para verificar que se trata de esto, en el menú **Visualizar**, seleccione **Renovar**. Si el objeto aún aparece en la ventana Red privada virtual, pase al siguiente elemento de la lista.
- Al configurar las propiedades del objeto, se puede haber producido un error entre el servidor VPN y el sistema. Muchos de los objetos que aparecen en la ventana VPN están relacionados con más de un objeto de la base de datos de políticas VPN. Esto significa que los errores de comunicación pueden hacer que algunos de los objetos de la base de datos sigan estando relacionados con un objeto en la VPN. Siempre que se cree o actualice un objeto, se produce un error en el momento en que realmente se produce la pérdida de sincronización. La única forma de solucionar el problema es seleccionar **Aceptar** en la ventana del error. De esta forma lanzará la hoja de propiedades del objeto que tiene el error. El único campo de la hoja de propiedades que contiene un valor es el de nombre. El resto están en blanco (o contienen valores predeterminados). Especifique los atributos correctos del objeto y seleccione **Aceptar** para guardar los cambios.
- Se produce un error similar al intentar eliminar el objeto. Para solucionar este problema, complete la hoja de propiedades vacía que aparece al pulsar **Aceptar** en el mensaje de error. De esta forma se actualizan todos los enlaces con la base de datos de políticas VPN que se habían perdido. Ahora puede eliminar el objeto.

## Mensaje de error de VPN: EL PARÁMETRO PINBUF NO ES VÁLIDO

Al intentar iniciar una conexión, obtiene el mensaje **EL PARÁMETRO PINBUF NO ES VÁLIDO...**

**Síntoma:**

Al intentar iniciar una conexión, aparece un mensaje parecido al siguiente:




**Posible resolución:**

Esto se produce cuando su sistema está configurado para utilizar determinados entornos locales en los que las letras minúsculas no se correlacionan correctamente. Para reparar este error, puede asegurarse de que todos los objetos utilicen sólo letras mayúsculas o modificar el entorno local del sistema.

## Mensaje de error de VPN: Elemento no encontrado, Servidor de claves remoto...

Al seleccionar las **Propiedades** de una conexión de claves dinámicas, obtiene un mensaje que le informa de que el servidor no encontró el servidor de claves remoto que ha especificado.

**Síntoma:**

Al seleccionar **Propiedades** de una conexión de claves dinámicas, aparece un mensaje como el siguiente:


**Posible resolución:**

Esto se produce al crear una conexión con un identificador de servidor de claves remoto determinado y, a continuación, el servidor de claves remoto se elimina de su grupo de claves dinámicas. Para solucionar este error, pulse **Aceptar** en el mensaje de error. De esta forma, se abrirá la hoja de propiedades de la conexión de claves dinámicas que da error. A partir de aquí, puede volver a añadir el servidor de claves remoto al grupo de claves dinámicas o seleccionar otro identificador de servidor de claves remoto. Pulse **Aceptar** en la hoja de propiedades para guardar los cambios.

## Mensaje de error de VPN: No ha sido posible actualizar el objeto

Al seleccionar **Aceptar** en la hoja de propiedades de un grupo de claves dinámicas o una conexión manual, obtiene un mensaje que le informa de que el sistema no puede actualizar el objeto.

**Síntoma:**

Al seleccionar **Aceptar** en la hoja de propiedades de un grupo de claves dinámicas o conexión manual, aparece el siguiente mensaje:


**Posible resolución:**

Este error se produce si una conexión activa está utilizando un objeto que está intentando modificar. No puede realizar cambios a un objeto de una conexión activa. Para realizar cambios a un objeto, identifique la conexión activa apropiada y, a continuación, pulse el botón derecho del ratón y seleccione **Detener** en el menú de contexto que aparecerá.

## Mensaje de error de VPN: no ha sido posible cifrar la clave...

Obtiene un mensaje que le informa de que el sistema no puede cifrar sus claves porque el valor QRETSVRSEC debe establecerse en 1.

**Síntoma:**

Aparece el siguiente mensaje de error:


**Posible resolución:**

QRETSVRSEC es un valor del sistema que indica si el sistema puede almacenar claves cifradas. Si este valor se establece en 0, las claves precompartidas y las claves de los algoritmos de una conexión manual no pueden almacenarse en la base de datos de políticas VPN. Para solventar este problema, utilice una sesión de emulación 5250 para su sistema. Escriba `wrksysval` en la línea de mandatos y pulse **Intro**. Busque QRETSVRSEC en la lista y escriba 2 (cambiar) al lado. En el siguiente panel, escriba 1 y pulse **Intro**.

**Conceptos relacionados**:

"Error de VPN: Todas las claves están en blanco" en la página 73
Al visualizar las propiedades de una conexión manual, todas las claves precompartidas y las claves de los algoritmos de la conexión están en blanco.

## Mensaje de error de VPN: CPF9821

Al intentar expandir o abrir el contenedor de políticas IP en IBM Navigator for i, aparece el mensaje CPF9821- No autorizado para el programa QTFRPRS en la biblioteca QSYS.

**Síntoma:**

Al intentar expandir el contenedor de políticas IP en IBM Navigator for i, aparece el mensaje `CPF9821- No autorizado para el programa QTFRPRS en la biblioteca QSYS`.

**Posible resolución:**

Puede que no disponga de la autorización necesaria para recuperar el estado actual de las

Normas de paquetes o del gestor de conexiones VPN. Asegúrese de que tiene acceso a las funciones de Normas de paquetes en IBM Navigator for i.

## Error de VPN: Todas las claves están en blanco

Al visualizar las propiedades de una conexión manual, todas las claves precompartidas y las claves de los algoritmos de la conexión están en blanco.

**Síntoma:**

Todas las claves precompartidas y las claves de algoritmo de las conexiones manuales están en blanco.

**Posible resolución:**

Esto se produce si el valor del sistema QRETSVRSEC se ha establecido nuevamente en 0. Al establecer este valor en 0 se borran todas las claves de la base de datos de políticas VPN. Para solucionar este problema, deberá establecer el valor del sistema en 1 y, a continuación, volver a especificar todas las claves. Consulte Mensaje de error: No es posible cifrar las claves, para obtener más información sobre este tema.

**Conceptos relacionados**:

"Mensaje de error de VPN: no ha sido posible cifrar la clave..." en la página 72
Obtiene un mensaje que le informa de que el sistema no puede cifrar sus claves porque el valor QRETSVRSEC debe establecerse en 1.

## Error VPN: La conexión ha habilitado el estado después de que lo haya detenido

| Después de detener una conexión, el panel de IBM Navigator for i indica que la conexión todavía está habilitada.

**Síntoma:**

| Después de detener una conexión, el panel de IBM Navigator for i indica que la conexión todavía está habilitada.

**Posible resolución:**

| Esto suele suceder porque aún no ha renovado el panel de lista de conexión en IBM Navigator
| for i. Por lo tanto, la lista de conexiones contiene información anticuada. Para solucionarlo, pulse
| el botón **Renovar** en el menú de lista.

## Error VPN: Se ha producido una anomalía al desactivar las normas de filtro activas

Al intentar desactivar el actual conjunto de normas de filtro, aparece el mensaje `Se ha producido una anomalía al intentar desactivar las normas activas` en la ventana de resultados.

**Síntoma:**

Al intentar desactivar el actual conjunto de normas de filtro, aparece el mensaje `Se ha producido una anomalía al intentar desactivar las normas activas` en la ventana de resultados.

**Posible resolución:**

Habitualmente, este mensaje de error significa que existe al menos una conexión VPN activa. Deberá detener cada una de las conexiones que se encuentren en estado `habilitado`. Para ello, pulse cada una de las conexiones activas con el botón derecho del ratón y seleccione **Detener**. Ahora puede desactivar las normas de filtro.

## Error de VPN: El grupo de conexión de claves de una conexión cambia

Al crear una conexión de claves dinámicas, se especifica un grupo de claves dinámicas y un identificador para el servidor de claves remoto. Más adelante, al ver las propiedades del objeto de conexión relacionado, la página General de la hoja de propiedades visualiza el mismo identificador del servidor de claves remoto, pero un grupo de claves dinámicas distinto.

**Síntoma:**

Al crear una conexión de claves dinámicas, se especifica un grupo de claves dinámicas y un identificador para el servidor de claves remoto. Más adelante, al seleccionar **Propiedades** en el

objeto de conexión relacionado, la página **General** de esta hoja de propiedades visualiza el mismo identificador del servidor de claves remoto, pero un grupo de claves dinámicas distinto.

**Posible resolución:**

El identificador es la única información almacenada en la base de datos de políticas VPN que hace referencia al servidor de claves remoto de la conexión de claves dinámicas. Cuando VPN busca una política para un servidor de claves remoto, comprueba el primer grupo de claves dinámicas que contiene ese identificador de servidor de claves remoto. Por tanto, al visualizar las propiedades de una de estas conexiones, utiliza el mismo grupo de claves dinámicas que ha encontrado VPN. Si no desea asociar el grupo de claves dinámicas con este servidor de claves remoto, puede hacer algo de lo siguiente:

1. Elimine el servidor de claves remoto del grupo de claves dinámicas.
2. Expanda **Por grupos** en el panel izquierdo de la interfaz VPN y seleccione y arrastre el grupo de claves dinámicas deseado a la parte superior de la tabla en el panel derecho. Con esto, se asegura de que VPN comprobará en el servidor de claves remoto este grupo de claves dinámicas en primer lugar.

## Resolución de problemas de VPN con el diario QIPFILTER

Consulte esta información para aprender a utilizar las normas de filtro VPN.

El diario QIPFILTER está ubicado en la biblioteca QUSRSYS y contiene información sobre los conjuntos de normas de filtro, así como información acerca de si un datagrama IP ha sido autorizado o denegado. Las anotaciones se basan en la opción de registro por diario que especifique en sus normas de filtro.

**Tareas relacionadas**:

"Iniciación a la resolución de problemas de VPN" en la página 68
Complete esta tarea para conocer los distintos métodos posibles para determinar los problemas de VPN que pueden surgir en el sistema.

### Habilitación del diario QIPFILTER

Utilice el editor de normas de paquetes de IBM Navigator for i para activar el diario QIPFILTER.

Debe habilitar la función de anotaciones para cada norma de filtro individualmente. No hay ninguna función que permita efectuar las anotaciones de todos los datagramas IP que entran o salen del sistema.

**Nota:** Para habilitar el diario QIPFILTER, los filtros deberán estar desactivados.

Los siguientes pasos describen cómo habilitar el registro por diario de una norma de filtro determinada:

1. En IBM Navigator for i, expanda **Red** > **Políticas IP** y pulse **Reglas de paquete**.
2. Pulse **Acciones** > **Editor de reglas**.
3. Abra un archivo de reglas de filtro existente en el **Editor de reglas**.
4. Seleccione la regla de filtro que desee registrar por diario y luego seleccione **Acciones** > **Propiedades**.
5. En la página **General**, seleccione **FULL** en el campo **Registro por diario**, como en el recuadro de diálogo que se muestra arriba. De esta forma, se habilitará para esta norma de filtro determinada.
6. Pulse **Aceptar**.
7. Guarde y active el archivo de normas de filtro modificado.

Si un datagrama IP coincide con las definiciones de la norma de filtro, se creará una entrada en el diario QIPFILTER.

### Utilización del diario QIPFILTER

IBM i crea automáticamente el diario la primera vez que se activa el filtrado de paquetes IP.

Para visualizar los detalles específicos de la entrada en el diario, puede visualizar las entradas del diario en pantalla o puede utilizar el archivo de salida. Si copia las entradas del diario en el archivo de salida,

puede visualizar fácilmente las entradas mediante los programas de utilidades de consulta, como por ejemplo, Query/400 o SQL. También puede escribir sus propios programas HLL para procesar las entradas del archivo de salida.

El siguiente es un ejemplo del mandato Visualizar Diario (DSPJRN):

```
DSPJRN JRN(QIPFILTER) JRNCDE((M)) ENTTYP((TF)) OUTPUT(*OUTFILE)
       OUTFILFMT(*TYPE4) OUTFILE(mylib/myfile) ENTDTALEN(*VARLEN *CALC)
```

Siga estos pasos para copiar las entradas del diario QIPFILTER en el archivo de salida:

1. Haga una copia en una biblioteca de usuario del archivo de salida QSYS/QATOFIPF suministrado por el sistema mediante el mandato Crear Objeto Duplicado (CRTDUPOBJ). El siguiente es un ejemplo del mandato CRTDUPOBJ:

   ```
   CRTDUPOBJ OBJ(QATOFIPF) FROMLIB(QSYS) OBJTYPE(*FILE) TOLIB(mylib)
             NEWOBJ(myfile)
   ```

2. Utilice el mandato Visualizar Diario (DSPJRN) para copiar las entradas desde el diario QUSRSYS/QIPFILTER al archivo de salida que ha creado en el paso anterior.

Si copia el diario DSPJRN en un archivo de salida que no existe, el sistema creará el archivo, pero este archivo no contendrá las descripciones de campo adecuadas.

**Nota:** El diario QIPFILTER sólo contiene entradas de autorización o denegación para las normas de filtro cuya opción de registro por diario se haya establecido en FULL. Por ejemplo, si configura únicamente las normas de filtro PERMIT, los datagramas IP que no se autoricen explícitamente se denegarán. No se añadirá ninguna entrada en el diario para los datagramas denegados. Para analizar el problema, puede añadir una norma de filtro que deniegue explícitamente cualquier otro tráfico y que realice un registro por diario FULL. Entonces, obtendrá entradas DENY en el diario para todos los datagramas IP que se denieguen. Por razones de rendimiento, no se recomienda habilitar el registro por diario para todas las normas de filtro. Una vez que los conjuntos de filtros se hayan comprobado, reduzca el registro por diario a un subconjunto útil de entradas.

**Conceptos relacionados**:

"Campos de diario QIPFILTER"
Revise la siguiente tabla donde se describen los campos del archivo de salida QIPFILTER

## Campos de diario QIPFILTER

Revise la siguiente tabla donde se describen los campos del archivo de salida QIPFILTER

| Nombre del campo | Longitud del campo | Numérico | Descripción | Comentarios |
|---|---|---|---|---|
| TFENTL | 5 | S | Longitud de la entrada | |
| TFSEQN | 10 | S | Número de secuencia | |
| TFCODE | 1 | N | Código del diario | Siempre M |
| TFENTT | 2 | N | Tipo de entrada | Siempre TF |
| TFTIME | 26 | N | Indicación de la hora SAA | |
| TFJOB | 10 | N | Nombre del trabajo | |
| TFUSER | 10 | N | Perfil del usuario | |
| TFNBR | 6 | S | Número de trabajo | |
| TFPGM | 10 | N | Nombre del programa | |
| TFRES1 | 51 | N | Reservado | |
| TFUSPF | 10 | N | Usuario | |

| Nombre del campo | Longitud del campo | Numérico | Descripción | Comentarios |
|---|---|---|---|---|
| TFSYMN | 8 | N | Nombre del sistema | |
| TFRES2 | 20 | N | Reservado | |
| TFRESA | 50 | N | Reservado | |
| TFLINE | 10 | N | Descripción de línea | *ALL si TFREVT es U* , espacio en blanco si TFREVT es L*, nombre de línea si TFREVT es L |
| TFREVT | 2 | N | Evento de norma | L* o L si se cargan las normas. U* si no se cargan las normas, A para acción de filtro |
| TFPDIR | 1 | N | Dirección de paquete IP | O es saliente, I es entrante |
| TFRNUM | 5 | N | Número de norma | Se aplica al número de norma en el archivo de normas activas |
| TFACT | 6 | N | Acción de filtro realizada | PERMIT, DENY o IPSEC |
| TFPROT | 4 | N | Protocolo de transporte | 1 es ICMP<br>6 es TCP<br>17 es UDP<br>50 es ESP<br>51 es AH |
| TFSRCA | 15 | N | Dirección IP de origen | |
| TFSRCP | 5 | N | Puerto origen | Datos innecesarios si TFPROT= 1 (ICMP) |
| TFDSTA | 15 | N | Dirección IP de destino | |
| TFDSTP | 5 | N | Puerto destino | Datos innecesarios si TFPROT= 1 (ICMP) |
| TFTEXT | 76 | N | Texto adicional | Contiene descripción si TFREVT= L* o U* |

**Tareas relacionadas**:

"Utilización del diario QIPFILTER" en la página 74
IBM i crea automáticamente el diario la primera vez que se activa el filtrado de paquetes IP.

## Resolución de problemas de VPN con el diario QVPN

Se proporciona información sobre las conexiones y el tráfico IP.

VPN utiliza un diario independiente para anotar la información acerca del tráfico IP y las conexiones, denominado diario QVPN. El diario QVPN se almacena en la biblioteca QUSRSYS. El código del diario es M y el tipo de diario es TS. Raramente utilizará las entradas del diario día por día. Sin embargo, pueden serle útiles para solucionar problemas y verificar que su sistema, claves y conexiones funcionan

de la forma que ha especificado. Por ejemplo, las entradas de diario ayudan a comprender lo que ocurre con los paquetes de datos. También informan acerca del estado actual de la VPN.

## Habilitación del diario QVPN

Utilice la opción de red privada virtual de IBM Navigator for i para activar el diario VPN.

No hay ninguna función que permita efectuar las anotaciones de todas las conexiones VPN. Por lo tanto, debe habilitar la función de anotaciones para cada grupo de claves dinámicas o conexión manual de forma individual.

Los siguientes pasos describen cómo habilitar la función de registro por diario para un grupo de claves dinámicas o conexión manual determinados:

1. En IBM Navigator for i, expanda **Red** > **Políticas IP** > **Red privada virtual** y pulse **Conexiones seguras**.
2. Para los grupos de claves dinámicas, pulse con el botón derecho del ratón **Por grupo** y seleccione **Abrir** para ver los grupos. Pulse con el botón derecho del ratón el grupo de claves dinámicas cuyo registro por diario desee habilitar y seleccione **Propiedades.**
3. Para las conexiones manuales, pulse con el botón derecho del ratón en **Conexiones manuales** y seleccione **Abrir** para mostrar **Todas las conexiones**. Pulse con el botón derecho del ratón la conexión manual para la que desee habilitar el registro por diario.
4. En la página **General**, seleccione el nivel de registro por diario que necesita. Puede seleccionar entre cuatro opciones. Éstas son las siguientes:

   **Ninguno**
   No se producirá ningún registro por diario para este grupo de conexiones.

   **Todos** Se producirá registro por diario para todas las actividades de conexión, como por ejemplo inicio y detención de una conexión o renovaciones de claves, así como información de tráfico IP.

   **Actividad de conexión**
   Se producirá el registro por diario para actividades de conexión, como por ejemplo, inicio o detención de una conexión.

   **Tráfico IP**
   El registro por diario se produce para todo el tráfico VPN que está asociado con esta conexión. Se realiza una entrada en las anotaciones cada vez que se invoca una norma de filtro. El sistema registra la información de tráfico IP en el diario QIPFILTER, ubicado en la biblioteca QUSRSYS.
5. Pulse **Aceptar**.
6. Inicie la conexión para activar el registro por diario.

**Nota:** Antes de detener el registro por diario, asegúrese de que la conexión esté inactiva. Para modificar el estado del registro por diario de un grupo de conexiones, asegúrese de que no hay ninguna conexión activa asociada con este grupo determinado.

## Utilización del diario QVPN

Para visualizar los detalles específicos de la entrada en el diario VPN, puede visualizar las entradas del diario en pantalla o puede utilizar un archivo de salida.

Si copia las entradas del diario en el archivo de salida, puede visualizar fácilmente las entradas mediante los programas de utilidades de consulta, como por ejemplo, Query/400 o SQL. También puede escribir sus propios programas HLL para procesar las entradas del archivo de salida. El siguiente es un ejemplo del mandato Visualizar Diario (DSPJRN):

```
DSPJRN JRN(QVPN) JRNCDE((M)) ENTTYP((TS)) OUTPUT(*OUTFILE) OUTFILFMT(*TYPE4)
       OUTFILE(mylib/myfile) ENTDTALEN(*VARLEN *CALC)
```

Siga estos pasos para copiar las entradas del diario VPN en el archivo de salida:

.

1. Haga una copia del archivo de salida QSYS/QATOVSOF suministrado por el sistema en una biblioteca de usuario. Puede llevarlo a cabo mediante el mandato Crear Objeto Duplicado (CRTDUPOBJ). El siguiente es un ejemplo del mandato CRTDUPOBJ:

   ```
   CRTDUPOBJ OBJ(QATOVSOF) FROMLIB(QSYS) OBJTYPE(*FILE) TOLIB(mylib)
             NEWOBJ(myfile)
   ```

2. Utilice el mandato Visualizar Diario (DSPJRN) para copiar las entradas desde el diario QUSRSYS/QVPN al archivo de salida que ha creado en el paso anterior. Si intenta copiar el diario DSPJRN en un archivo de salida que no existe, el sistema creará el archivo, pero este archivo no contendrá las descripciones de campo adecuadas.

**Conceptos relacionados**:

"Campos de diario QVPN"
Revise la siguiente tabla donde se describen los campos del archivo de salida QVPN.

## Campos de diario QVPN

Revise la siguiente tabla donde se describen los campos del archivo de salida QVPN.

| Nombre del campo | Longitud del campo | Numérico | Descripción | Comentarios |
|---|---|---|---|---|
| TSENTL | 5 | S | Longitud de la entrada | |
| TSSEQN | 10 | S | Número de secuencia | |
| TSCODE | 1 | N | Código del diario | Siempre M |
| TSENTT | 2 | N | Tipo de entrada | Siempre TS |
| TSTIME | 26 | N | Indicación de la hora de entrada SAA | |
| TSJOB | 10 | N | Nombre del trabajo | |
| TSUSER | 10 | N | Usuario del trabajo | |
| TSNBR | 6 | S | Número de trabajo | |
| TSPGM | 10 | N | Nombre del programa | |
| TSRES1 | 51 | N | No utilizado | |
| TSUSPF | 10 | N | Nombre del perfil de usuario | |
| TSSYNM | 8 | N | Nombre del sistema | |
| TSRES2 | 20 | N | No utilizado | |
| TSRESA | 50 | N | No utilizado | |
| TSESDL | 4 | S | Longitud de los datos específicos | |
| TSCMPN | 10 | N | Componente VPN | |
| TSCONM | 40 | N | Nombre de conexión | |
| TSCOTY | 10 | N | Tipo de conexión | |
| TSCOS | 10 | N | Estado de la conexión | |
| TSCOSD | 8 | N | Fecha de inicio | |
| TSCOST | 6 | N | Hora de inicio | |
| TSCOED | 8 | N | Fecha de finalización | |
| TSCOET | 6 | N | Hora de finalización | |

| Nombre del campo | Longitud del campo | Numérico | Descripción | Comentarios |
|---|---|---|---|---|
| TSTRPR | 10 | N | Protocolo de transporte | |
| TSLCAD | 43 | N | Dirección del cliente local | |
| TSLCPR | 11 | N | Puertos locales | |
| TSRCAD | 43 | N | Dirección del cliente remoto | |
| TSCPR | 11 | N | Puertos remotos | |
| TSLEP | 43 | N | Punto final local | |
| TSREP | 43 | N | Punto final remoto | |
| TSCORF | 6 | N | Número de renovaciones | |
| TSRFDA | 8 | N | Fecha de la nueva renovación | |
| TSRFTI | 6 | N | Fecha de la nueva renovación | |
| TSRFLS | 8 | N | Renovar tiempo de vida | |
| TSSAPH | 1 | N | Fase SA | |
| TSAUTH | 10 | N | Tipo de autenticación | |
| TSENCR | 10 | N | Tipo de cifrado | |
| TSDHGR | 2 | N | Grupo Diffie-Hellman | |
| TSERRC | 8 | N | Código de error | |

**Tareas relacionadas**:

"Utilización del diario QVPN" en la página 77
Para visualizar los detalles específicos de la entrada en el diario VPN, puede visualizar las entradas del diario en pantalla o puede utilizar un archivo de salida.

## Resolución de problemas de VPN con de las anotaciones de trabajo VPN

Si encuentra problemas con las conexiones VPN, se recomienda siempre que analice las anotaciones de trabajo. De hecho, hay varias anotaciones de trabajo que contienen mensajes de error y otra información relacionada con un entorno VPN.

Es importante que analice las anotaciones de trabajo en ambos lados de la conexión si éstos son modelos IBM i. Si una conexión dinámica sufre una anomalía al iniciarse, le será útil comprender lo que sucede en el sistema remoto.

Los trabajos de VPN, QTOVMAN, QTOKVPNIKE y QTOKVPNIK2, se ejecutan en el subsistema QSYSWRK. Puede visualizar sus anotaciones de trabajo respectivas desde IBM Navigator for i.

Esta sección introduce los trabajos más importantes de un entorno VPN. La siguiente lista muestra los nombres de los trabajos con una breve explicación de para qué se utiliza cada uno:

**QTCPIP**

Este trabajo es el trabajo base que inicia todas las interfaces TCP/IP. Si tiene problemas fundamentales con TCP/IP en general, analice las anotaciones de trabajo de QTCPIP.

**QTOKVPNIKE**
El trabajo QTOKVPNIKE es el trabajo del gestor de claves VPN. El gestor de claves VPN está a la escucha en el puerto 500 UDP para llevar a cabo el proceso del protocolo IKE (intercambio de claves de Internet).

**QTOKVPNIK2**
El trabajo QTOKVPNIK2 es el trabajo del gestor de claves VPN para IKEv2. El gestor de claves VPN está a la escucha en el puerto 500 UDP para llevar a cabo el proceso del protocolo IKEv2 (intercambio de claves de Internet versión 2).

**QTOVMAN**
Este trabajo es el gestor de conexiones de las conexiones VPN. Las anotaciones de trabajo relacionadas contienen mensajes de cada intento de conexión que da error.

**QTPPANSxxx**
Este trabajo se utiliza para conexiones de marcación PPP. Responde a intentos de conexión en los que *ANS está definido en un perfil PPP.

**QTPPPCTL**
Este es un trabajo PPP para conexiones de acceso por marcación.

**QTPPPL2TP**
Este es el trabajo del gestor de L2TP (Layer Two Tunneling Protocol). Si tiene problemas con la configuración de un túnel L2TP, compruebe los mensajes de estas anotaciones de trabajo.

**Conceptos relacionados**:

"IKE versión 2" en la página 11
IKE versión 2 es una mejora del protocolo de intercambio de claves de Internet.

**Tareas relacionadas**:

"Iniciación a la resolución de problemas de VPN" en la página 68
Complete esta tarea para conocer los distintos métodos posibles para determinar los problemas de VPN que pueden surgir en el sistema.

## Mensajes de error habituales del gestor de conexiones VPN

El gestor de conexiones VPN anota dos mensajes en las anotaciones de trabajo QTOVMAN cuando se produce un error con una conexión VPN.

El primer mensaje ofrece detalles con relación al error. Puede visualizar la información sobre estos errores en IBM Navigator for i pulsando sobre la conexión errónea con el botón derecho del ratón y seleccionando **Información de error**.

El segundo mensaje describe la acción que estaba intentando realizar en la conexión cuando se produjo el error. Por ejemplo, iniciarla o detenerla. Los mensajes TCP8601, TCP8602, y TCP860A, que se describen a continuación, son ejemplos habituales de estos segundos mensajes.

**Mensajes de error del gestor de conexiones VPN**

| Mensaje | Causa | Recuperación |
| --- | --- | --- |
| TCP8601 No se ha podido iniciar la conexión VPN [*nombre de la conexión*] | No se ha podido iniciar esta conexión VPN debido a uno de los siguientes códigos de razón: *0* - Hay un mensaje anterior en las anotaciones de trabajo con el mismo nombre de conexión VPN que tiene información más detallada. *1* - Configuración de la política VPN. *2* - Anomalía de la red de comunicaciones. *3* - El gestor de claves VPN ha sufrido una anomalía al negociar una nueva asociación de seguridad. *4* - El punto final remoto de esta conexión no está configurado correctamente. *5* - El gestor de claves VPN no pudo responder al gestor de conexiones VPN. *6* - Anomalía al cargar la conexión VPN del componente de seguridad IP. *7* - Anomalía del componente PPP. | 1. Compruebe si hay más mensajes en las anotaciones de trabajo.<br>2. Corrija los errores y vuelva a intentar la petición.<br>3. Utilice IBM Navigator for i para visualizar el estado de la conexión. Las conexiones que no se han podido iniciar estarán en estado de error. |
| TCP8602 Se ha producido un error al detener la conexión VPN [*nombre de la conexión*] | Se ha solicitado detener la conexión VPN especificada; sin embargo, no se ha podido detener o se ha detenido con error debido al código de razón: *0* - Hay un mensaje anterior en las anotaciones de trabajo con el mismo nombre de conexión VPN que tiene información más detallada. *1* - La conexión VPN no existe. *2* - Anomalía interna de comunicaciones con el gestor de claves VPN. *3* - Anomalía interna de comunicaciones con el componente IPSec. *4* - Anomalía de comunicaciones con el punto final remoto de conexión VPN. | 1. Compruebe si hay más mensajes en las anotaciones de trabajo.<br>2. Corrija los errores y vuelva a intentar la petición.<br>3. Utilice IBM Navigator for i para visualizar el estado de la conexión. Las conexiones que no se han podido iniciar estarán en estado de error. |

**Mensajes de error del gestor de conexiones VPN**

| Mensaje | Causa | Recuperación |
| --- | --- | --- |
| TCP8604 Se ha producido una anomalía al iniciar la conexión VPN [*nombre de la conexión*] | Se ha producido una anomalía al iniciar esta conexión VPN debido a uno de los siguientes códigos de razón: *1* - No se ha podido convertir el nombre del host remoto en una dirección IP. *2* - No se ha podido convertir el nombre del host local en una dirección IP. *3* - No se ha cargado una norma de filtro de políticas VPN asociada con esta conexión VPN. *4* - Hay un valor de clave especificado por el usuario que no es válido para el algoritmo asociado. *5* - El valor de iniciación de la conexión VPN no permite realizar la acción especificada. *6* - Hay un rol del sistema de la conexión VPN que es incoherente con la información del grupo de conexión. *7* - Reservado. *8* - Los puntos finales de datos (direcciones y servicios remotos y locales) de esta conexión VPN son incoherentes con la información del grupo de conexión. *9* - Tipo de identificador no válido. | 1. Compruebe si hay más mensajes en las anotaciones de trabajo.<br>2. Corrija los errores y vuelva a intentar la petición.<br>3. Utilice IBM Navigator for i para comprobar o corregir la configuración de la política VPN. Asegúrese de que el grupo de claves dinámicas asociado con la conexión tiene unos valores de configuración aceptables. |
| TCP8605 El gestor de conexiones VPN no ha podido comunicarse con el gestor de claves VPN | El gestor de conexiones VPN necesita los servicios del gestor de claves VPN para poder establecer asociaciones de seguridad para las conexiones VPN dinámicas. El gestor de conexiones VPN no ha podido comunicarse con el gestor de claves VPN. | 1. Compruebe si hay más mensajes en las anotaciones de trabajo.<br>2. Verifique que la interfaz *LOOPBACK esté activa mediante el mandato NETSTAT OPTION(*IFC).<br>3. Finalice el servidor VPN mediante el mandato ENDTCPSVR SERVER(*VPN). A continuación, reinicie el servidor VPN mediante el mandato STRTCPSRV SERVER(*VPN).<br>**Nota:** Esto hace que finalicen todas las conexiones VPN actuales. |

**Mensajes de error del gestor de conexiones VPN**

| Mensaje | Causa | Recuperación |
| --- | --- | --- |
| TCP8606 El gestor de claves VPN no ha podido establecer la asociación de seguridad solicitada para la conexión, [*nombre de la conexión*] | El gestor de claves VPN no ha podido establecer la asociación de seguridad solicitada debido a uno de los siguientes códigos de razón: *24* - Se ha producido una anomalía al autenticar la conexión de la clave del gestor de claves VPN. *8300* - Se ha producido una anomalía durante las negociaciones de conexión de la clave del gestor de claves VPN. *8306* - No se ha encontrado ninguna clave precompartida local. *8307* - No se ha encontrado ninguna política de fase 1 IKE remota. *8308* - No se ha encontrado ninguna clave precompartida remota. *8327* - Se ha agotado el tiempo de espera para las negociaciones de conexión de la clave del gestor de claves VPN. *8400* - Se ha producido una anomalía durante las negociaciones de conexión VPN del gestor de claves VPN. *8407* - No se ha encontrado ninguna política de fase 2 IKE remota. *8408* - Se ha agotado el tiempo de espera para las negociaciones de conexión VPN del gestor de claves VPN. *8500 o 8509* - Se ha producido un error de red del gestor de claves VPN. | 1. Compruebe si hay más mensajes en las anotaciones de trabajo.<br>2. Corrija los errores y vuelva a intentar la petición.<br>3. Utilice IBM Navigator for i para comprobar o corregir la configuración de la política VPN. Asegúrese de que el grupo de claves dinámicas asociado con la conexión tiene unos valores de configuración aceptables. |
| TCP8608 La conexión VPN [*nombre de la conexión*] no ha podido obtener una dirección NAT | Este grupo de claves dinámicas o conexión de datos especifica que la conversión de direcciones de red (NAT) debe hacerse en una o varias direcciones y que ha fallado probablemente debido a uno de los siguientes códigos de razón: *1* - La dirección a la que se aplica NAT no es una dirección IP individual. *2* - Se han utilizado todas las direcciones disponibles. | 1. Compruebe si hay más mensajes en las anotaciones de trabajo.<br>2. Corrija los errores y vuelva a intentar la petición.<br>3. Utilice IBM Navigator for i para comprobar o corregir la política VPN. Asegúrese de que el grupo de claves dinámicas asociado con la conexión tiene unos valores aceptables para las direcciones configuradas. |
| TCP8620 El punto final de conexión local no está disponible | No ha sido posible habilitar esta conexión VPN porque el punto final de datos local no estaba disponible. | 1. Compruebe si en las anotaciones de trabajo hay más mensajes pertinentes a esta conexión.<br>2. Asegúrese de que el punto final de conexión local está definido e iniciado mediante el mandato NETSTAT OPTION(*IFC).<br>3. Corrija los errores y vuelva a intentar la petición. |

**Mensajes de error del gestor de conexiones VPN**

| Mensaje | Causa | Recuperación |
| --- | --- | --- |
| TCP8621 Punto final de datos local a hacer disponible | No ha sido posible habilitar esta conexión VPN porque el punto final de datos local no estaba disponible. | 1. Compruebe si en las anotaciones de trabajo hay más mensajes pertinentes a esta conexión.<br>2. Asegúrese de que el punto final de conexión local está definido e iniciado mediante el mandato NETSTAT OPTION(*IFC).<br>3. Corrija los errores y vuelva a intentar la petición. |
| TCP8622 No se permite encapsular el transporte con una pasarela | No ha sido posible habilitar esta conexión VPN porque la política negociada especificaba modalidad de encapsulado del transporte y esta pasarela está definida como pasarela de seguridad. | 1. Compruebe si en las anotaciones de trabajo hay más mensajes pertinentes a esta conexión.<br>2. Utilice IBM Navigator for i para modificar la política VPN asociada con esta conexión VPN.<br>3. Corrija los errores y vuelva a intentar la petición. |
| TCP8623 La conexión VPN se solapa con otra conexión existente | No ha sido posible habilitar esta conexión VPN porque ya se había habilitado otra conexión VPN existente. Esta conexión tiene un punto final de datos local de [*valor del punto final de datos local*] y un punto final de datos remoto de [*valor del punto final de datos remoto*]. | 1. Compruebe si en las anotaciones de trabajo hay más mensajes pertinentes a esta conexión.<br>2. Utilice IBM Navigator for i para visualizar todas las conexiones habilitadas que tienen puntos finales de datos locales y puntos finales de datos remotos que se solapan con la conexión. Cambie la política de la conexión existente si ambas conexiones son necesarias.<br>3. Corrija los errores y vuelva a intentar la petición. |

**Mensajes de error del gestor de conexiones VPN**

| Mensaje | Causa | Recuperación |
| --- | --- | --- |
| TCP8624 La conexión VPN no está en el ámbito de la norma de filtro de políticas asociada | No ha sido posible habilitar esta conexión VPN porque los puntos finales de datos no se encuentran dentro de la norma de filtro de políticas definida. | 1. Compruebe si en las anotaciones de trabajo hay más mensajes pertinentes a esta conexión.<br>2. Utilice IBM Navigator for i para visualizar las restricciones del punto final de datos para esta conexión o grupo de claves dinámicas. Si está seleccionado **Subconjunto de filtros de políticas** o **Personalizar para que coincida con filtro de políticas**, compruebe los puntos finales de datos de la conexión. Éstos deben ajustarse a la norma de filtro activa que tiene una acción IPSEC y un nombre de conexión VPN asociados con esta conexión. Cambie la política o la norma de filtros de la conexión existente para habilitar esta conexión.<br>3. Corrija los errores y vuelva a intentar la petición. |
| TCP8625 La conexión VPN ha sufrido una anomalía al comprobar un algoritmo ESP | No ha sido posible habilitar esta conexión VPN porque la clave secreta asociada con la conexión era insuficiente. | 1. Compruebe si en las anotaciones de trabajo hay más mensajes pertinentes a esta conexión.<br>2. Utilice IBM Navigator for i para visualizar la política asociada con esta conexión y especifique una clave secreta distinta.<br>3. Corrija los errores y vuelva a intentar la petición. |
| TCP8626 El punto final de conexión VPN no es el mismo que el punto final de datos | No ha sido posible habilitar esta conexión VPN porque la política especifica que es un host y el punto final de conexión VPN no es el mismo que el punto final de datos. | 1. Compruebe si en las anotaciones de trabajo hay más mensajes pertinentes a esta conexión.<br>2. Utilice IBM Navigator for i para visualizar las restricciones del punto final de datos para esta conexión o grupo de claves dinámicas. Si está seleccionado **Subconjunto de filtros de políticas** o **Personalizar para que coincida con filtro de políticas**, compruebe los puntos finales de datos de la conexión. Éstos deben ajustarse a la norma de filtro activa que tiene una acción IPSEC y un nombre de conexión VPN asociados con esta conexión. Cambie la política o la norma de filtros de la conexión existente para habilitar esta conexión.<br>3. Corrija los errores y vuelva a intentar la petición. |

**Mensajes de error del gestor de conexiones VPN**

| Mensaje | Causa | Recuperación |
| --- | --- | --- |
| TCP8628 Norma de filtro de políticas no cargada | La norma de filtro de políticas de esta conexión no está activa. | 1. Compruebe si en las anotaciones de trabajo hay más mensajes pertinentes a esta conexión.<br>2. Utilice IBM Navigator for i para visualizar los filtros de políticas activos. Compruebe la norma de filtro de políticas de esta conexión.<br>3. Corrija los errores y vuelva a intentar la petición. |
| TCP8629 Paquete IP descartado para la conexión VPN | Esta conexión VPN tiene la NAT VPN configurada y el conjunto de direcciones NAT requeridas ha excedido las direcciones NAT disponibles. | 1. Compruebe si en las anotaciones de trabajo hay más mensajes pertinentes a esta conexión.<br>2. Utilice IBM Navigator for i para incrementar el número de direcciones NAT asignadas a esta conexión VPN.<br>3. Corrija los errores y vuelva a intentar la petición. |
| TCP862A Se ha producido una anomalía al iniciar la conexión PPP | Esta conexión VPN estaba asociada con un perfil PPP. Al iniciarla, se intentó iniciar el perfil PPP, pero se produjo una anomalía. | 1. Compruebe si en las anotaciones de trabajo hay más mensajes pertinentes a esta conexión.<br>2. Compruebe las anotaciones de trabajo asociadas con la conexión PPP.<br>3. Corrija los errores y vuelva a intentar la petición. |

**Tareas relacionadas**:

"Visualización de los atributos de las conexiones activas" en la página 66
Complete esta tarea para comprobar el estado y otros atributos de las conexiones activas.

# Resolución de problemas de VPN con el rastreo de comunicaciones

IBM i ofrece la posibilidad de rastrear los datos de una línea de comunicaciones, como por ejemplo la interfaz LAN (red de área local) o WAN (red de área amplia). Puede que el usuario medio no entienda todo el contenido de los datos de rastreo. Sin embargo, puede utilizar las entradas de rastreo para determinar si se ha producido un intercambio de datos entre los sistemas local y remoto.

## Inicio del rastreo de las comunicaciones

Utilice el mandato Iniciar rastreo de comunicaciones (STRCMNTRC) para iniciar el rastreo de las comunicaciones en su sistema. El siguiente es un ejemplo del mandato STRCMNTRC:

```
STRCMNTRC CFGOBJ(TRNLINE) CFGTYPE(*LIN) MAXSTG(2048) TEXT('Problemas de VPN')
```

Los parámetros del mandato se explican en la siguiente lista:

**CFGOBJ (Objeto de configuración)**
El nombre del objeto de configuración a rastrear. El objeto puede ser una descripción de línea, una descripción de interfaz de red o una descripción de servidor de red.

**CFGTYPE(Tipo de configuración)**
Si se está rastreando una línea (*LIN), una interfaz de red (*NWI) o un servidor de red (*NWS).

**MAXSTG (Tamaño del almacenamiento intermedio)**
El tamaño del almacenamiento intermedio del rastreo. El valor predeterminado se establece en 128 KB. El rango va de 128 KB a 64 MB. El tamaño máximo real del almacenamiento intermedio en todo el sistema está definido en las SST (Herramientas de servicio del sistema). Por lo tanto, puede recibir un mensaje de error al utilizar en el mandato STRCMNTRC un tamaño de almacenamiento intermedio superior al definido en SST. Recuerde que la suma de los tamaños de almacenamiento intermedio especificados en todos los rastreos de comunicaciones iniciados no debe exceder el tamaño máximo de almacenamiento intermedio definido en las SST.

**DTADIR (Dirección de datos)**
La dirección del tráfico de datos a rastrear. La dirección puede ser tráfico sólo saliente (*SND), tráfico sólo entrante (*RCV) o ambas direcciones (*BOTH).

**TRCFULL (Rastreo completo)**
Qué sucede cuando el almacenamiento intermedio del rastreo está lleno. Este parámetro tiene dos valores posibles. El valor predeterminado es *WRAP, que significa que cuando el almacenamiento intermedio del rastreo está lleno, el rastreo vuelve al inicio. Los registros de rastreo más antiguos se sobreescriben con otros nuevos a medida que se recopilan.

El segundo valor *STOPTRC permite detener el rastreo cuando el almacenamiento del rastreo especificado en el parámetro MAXSTG está lleno de registros de rastreo. Como norma general, defina siempre el tamaño del almacenamiento intermedio para que sea lo suficientemente grande como para almacenar todos los registros de rastreo. Si el rastreo se reinicia, puede perder información de rastreo importante. Si encuentra un problema altamente intermitente, defina el almacenamiento intermedio de rastreo de forma que sea lo suficientemente grande como para que un reinicio del almacenamiento intermedio no comporte una pérdida de información importante.

**USRDTA (Número de bytes de usuario a rastrear)**
Define el número de datos a rastrear en la parte de datos de usuario de las tramas de datos. De forma predeterminada, para las interfaces LAN sólo se capturan los primeros 100 bytes de los datos de usuario. Para las demás interfaces se capturan todos los datos de usuario. Asegúrese de especificar *MAX si sospecha que puede haber problemas en los datos de usuario de una trama.

**TEXTO (Descripción de rastreo)**
Ofrece una descripción significativa del rastreo.

## Detención del rastreo de comunicaciones

Si no especifica lo contrario, el rastreo normalmente se detendrá tan pronto como se produzca la condición para la cual está realizando el rastreo. Utilice el mandato Finalizar Rastreo de Comunicaciones (ENDCMNTRC) para detener el rastreo. El siguiente es un ejemplo del mandato ENDCMNTRC:

```
ENDCMNTRC CFGOBJ(TRNLINE) CFGTYPE(*LIN)
```

El mandato tiene dos parámetros:

**CFGOBJ (Objeto de configuración)**
El nombre del objeto de configuración para el cual se está ejecutando el rastreo. El objeto puede ser una descripción de línea, una descripción de interfaz de red o una descripción de servidor de red.

**CFGTYPE(Tipo de configuración)**
Si se está rastreando una línea (*LIN), una interfaz de red (*NWI) o un servidor de red (*NWS).

### Impresión de los datos de rastreo

Tras haber detenido el rastreo de comunicaciones, necesitará imprimir los datos de rastreo. Utilice el mandato Imprimir Rastreo de Comunicaciones (PRTCMNTRC) para llevar a cabo la tarea. Puesto que todo el tráfico de línea se captura durante el periodo de rastreo, dispone de múltiples opciones de filtro para generar la salida. Intente mantener el archivo en spool lo más pequeño posible. De esta forma, el análisis se llevará a cabo más rápida y eficientemente. En el caso de que se produzca un problema VPN, filtre sólo en el tráfico IP y, si es posible, en una dirección IP determinada. También tiene la posibilidad de filtrar en un número de puerto IP específico. El siguiente es un ejemplo del mandato PRTCMNTRC:

```
PRTCMNTRC CFGOBJ(TRNLINE) CFGTYPE(*LIN) FMTTCP(*YES) TCPIPADR('10.50.21.1)
        SLTPORT(500) FMTBCD(*NO)
```

En este ejemplo, el rastreo está formateado para el tráfico IP y contiene sólo datos para la dirección IP, donde la dirección de origen o destino es 10.50.21.1 y el número de puerto IP de origen o destino es 500.

A continuación, se explican los parámetros de mandato más importantes para el análisis de problemas de VPN:

**CFGOBJ (Objeto de configuración)**
El nombre del objeto de configuración para el cual se está ejecutando el rastreo. El objeto puede ser una descripción de línea, una descripción de interfaz de red o una descripción de servidor de red.

**CFGTYPE(Tipo de configuración)**
Si se está rastreando una línea (*LIN), una interfaz de red (*NWI) o un servidor de red (*NWS).

**FMTTCP (Formatear datos TCP/IP)**
Si el rastreo se formatea para datos TCP/IP y UDP/IP. Especifique *YES para formatear el rastreo para datos IP.

**TCPIPADR (Formatear datos TCP/IP por dirección)**
Este parámetro consta de dos elementos. Si especifica las direcciones IP en ambos elementos, sólo se imprimirá el tráfico IP entre estas direcciones.

**SLTPORT (número de puerto IP)**
El número de puerto IP a filtrar.

**FMTBCD (Formatear datos de difusión general)**
Si todas las tramas de difusión general se van a imprimir. El valor predeterminado es sí. Si, por ejemplo, no desea realizar peticiones ARP (Protocolo de resolución de direcciones), especifique *NO; en caso contrario, puede obtener una ingente cantidad de mensajes de difusión general.

**Tareas relacionadas**:

"Iniciación a la resolución de problemas de VPN" en la página 68
Complete esta tarea para conocer los distintos métodos posibles para determinar los problemas de VPN que pueden surgir en el sistema.

## Información relacionada para VPN

Las publicaciones IBM Redbooks y los sitios Web contienen información relacionada con la colección de temas de las redes privadas virtuales. Puede ver o imprimir los archivos PDF que desee.

### IBM Redbooks

- IBM System i Security Guide for IBM i5/OS Versión 5 Release 4
- AS/400 Internet Security: Implementing AS/400 Virtual Private Networks
- AS/400 Internet Security Scenarios: A Practical Approach

- OS/400 V5R2 Virtual Private Networks: Remote Access to the IBM eServer iSeries Server with Windows 2000 VPN Clients 

### Sitios Web

- TCP/IP on IBM i: RFC Documents 

# Avisos

Esta información se ha escrito para productos y servicios ofrecidos en Estados Unidos de América.

Es posible que IBM no ofrezca en otros países los productos, servicios o características que se describen en este documento. Consulte con el representante local de IBM para obtener información acerca de los productos y servicios que actualmente están disponibles en su zona. Las referencias a programas, productos o servicios de IBM no pretenden establecer ni implicar que sólo puedan utilizarse dichos productos, programas o servicios de IBM. En su lugar, se puede utilizar cualquier producto, programa o servicio funcionalmente equivalente que no infrinja ninguno de los derechos intelectuales de IBM. No obstante, es responsabilidad del usuario evaluar y verificar el funcionamiento de cualquier producto, programa o servicio que no sea de IBM.

IBM puede tener patentes o solicitudes de patentes pendientes que cubran la materia descrita en este documento. La posesión de este documento no le otorga ninguna licencia sobre dichas patentes. Puede enviar consultas sobre licencias, por escrito, a:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
EE.UU.

Para consultas sobre licencias relacionadas con información de doble byte (DBCS), póngase en contacto con el Departamento de propiedad intelectual de IBM de su país o envíe consultas, por escrito, a:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
1623-14, Shimotsuruma, Yamato-shi
Kanagawa 242-8502 Japón

El párrafo siguiente no se aplica al Reino Unido ni a ningún otro país donde estas disposiciones sean incompatibles con la legislación local: INTERNATIONAL BUSINESS MACHINES CORPORATION PROPORCIONA ESTA PUBLICACIÓN "TAL CUAL" SIN GARANTÍAS DE NINGÚN TIPO, NI EXPLÍCITAS NI IMPLÍCITAS, INCLUYENDO PERO NO LIMITÁNDOSE A ELLAS, LAS GARANTÍAS IMPLÍCITAS DE NO VULNERACIÓN, COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO. Algunas legislaciones no contemplan la declaración de limitación de garantías, ni implícitas ni explícitas, en determinadas transacciones, por lo que cabe la posibilidad de que esta declaración no sea aplicable en su caso.

Esta información puede contener imprecisiones técnicas o errores tipográficos. La información incluida en este documento está sujeta a cambios periódicos, que se incorporarán en nuevas ediciones de la publicación. IBM puede realizar en cualquier momento mejoras o cambios en los productos o programas descritos en esta publicación sin previo aviso.

Las referencias hechas en esta publicación a sitios Web que no son de IBM se proporcionan únicamente por cortesía y de ningún modo deben interpretarse como promoción de dichos sitios Web. Los materiales de dichos sitios Web no forman parte de los materiales de este producto IBM y su utilización es responsabilidad del usuario.

IBM puede utilizar o distribuir cualquier información que se le proporcione en la forma que considere adecuada, sin incurrir por ello en ninguna obligación para con el remitente.

Los licenciatarios de este programa que deseen obtener información sobre él para poder: (i) intercambiar información entre programas creados de forma independiente y otros programas (incluidos este) y (ii) y utilizar, de forma mutua, la información que se ha intercambiado, deben ponerse en contacto con:

IBM Corporation
Software Interoperability Coordinator, Department YBWA
3605 Highway 52 N
Rochester, MN 55901
EE.UU.

Esta información puede estar disponible, sujeta a los términos y condiciones pertinentes, e incluir en algunos casos el pago de una cantidad.

El programa bajo licencia descrito en este documento y todo el material con licencia disponible se proporcionan bajo los términos de IBM Customer Agreement, IBM International Program License Agreement o cualquier otro acuerdo equivalente entre IBM y el cliente.

La información concerniente a productos que no son de IBM se ha obtenido de los suministradores de dichos productos, de sus anuncios publicados o de otras fuentes de información pública disponibles. IBM no ha probado esos productos y no puede confirmar la exactitud del rendimiento, de la compatibilidad ni de ninguna otra declaración relacionada con productos que no sean de IBM. Las consultas acerca de las prestaciones de los productos que no son de IBM deben dirigirse a los suministradores de tales productos.

Todas las declaraciones relativas a la dirección o intención futura de IBM están sujetas a cambios o anulación sin previo aviso y representan únicamente metas y objetivos.

Esta documentación se suministra solo a efectos de planificación. La información que aquí se incluye está sujeta a cambios antes de que los productos descritos estén disponibles.

Esta información contiene ejemplos de datos e informes utilizados en operaciones comerciales diarias. Para ilustrarlas de la forma más completa posible, los ejemplos incluyen nombres de personas, empresas, marcas y productos. Todos estos nombres son ficticios y cualquier parecido con los nombres y direcciones utilizados por una empresa real es pura coincidencia.

LICENCIA DE COPYRIGHT:

Esta información contiene programas de aplicación de ejemplo en lenguaje fuente, que muestran técnicas de programación en diversas plataformas operativas. Puede copiar, modificar y distribuir estos programas de muestra de cualquier modo sin pagar a IBM con el fin de desarrollar, utilizar, comercializar o distribuir programas de aplicación que se ajusten a la interfaz de programación de aplicaciones para la plataforma operativa para la que se ha escrito el código de muestra. Estos ejemplos no se han comprobado de forma exhaustiva en todas las condiciones. Por lo tanto, IBM no puede garantizar ni dar por supuesta la fiabilidad, la capacidad de servicio ni la funcionalidad de estos programas. Los programas de ejemplo se ofrecen "TAL CUAL", sin garantía de ningún tipo. IBM no se hará responsable de los daños derivados de la utilización que haga el usuario de los programas de ejemplo.

Cada copia o parte de estos programas de ejemplo, así como todo trabajo derivado, debe incluir un aviso de copyright como el siguiente:

© (nombre de su empresa) (año). Partes de este código derivan de programas de ejemplo de IBM Corp. Sample Programs.

© Copyright IBM Corp. _escriba el año o años_.

## Información de la interfaz de programación

Esta publicación sobre redes privadas virtuales documenta las interfaces de programación que permiten al cliente grabar programas para obtener los servicios de IBM i.

## Marcas registradas

IBM, el logotipo de IBM e ibm.com son marcas registradas o marcas comerciales registradas de International Business Machines Corp., registradas en muchas jurisdicciones de todo el mundo. Otros nombres de servicios y productos podrían ser marcas registradas de IBM u otras compañías. Hay disponible una lista actual de marcas registradas de IBM en la web “Información de marca registrada y copyright” en www.ibm.com/legal/copytrade.shtml.

Adobe, el logotipo de Adobe, PostScript y el logotipo de PostScript son marcas registradas de Adobe Systems Incorporated en los Estados Unidos y/o en otros países.

Microsoft, Windows, Windows NT y el logotipo de Windows con marcas registradas de Microsoft Corporation en Estados Unidos y/o en otros países.

Otros nombres de servicios y productos podrían ser marcas registradas de IBM u otras compañías.

## Términos y condiciones

Los permisos para utilizar estas publicaciones están sujetos a los siguientes términos y condiciones.

**Uso personal:** puede reproducir estas publicaciones para uso personal (no comercial) siempre y cuando incluya una copia de todos los avisos de derechos de autor. No puede distribuir ni visualizar estas publicaciones ni ninguna de sus partes, como tampoco elaborar trabajos que se deriven de ellas, sin el consentimiento explícito de IBM.

**Uso comercial:** puede reproducir, distribuir y visualizar estas publicaciones únicamente dentro de su empresa, siempre y cuando incluya una copia de todos los avisos de derechos de autor. No puede elaborar trabajos que se deriven de estas publicaciones, ni tampoco reproducir, distribuir ni visualizar estas publicaciones ni ninguna de sus partes fuera de su empresa, sin el consentimiento explícito de IBM.

Aparte de la autorización que se concede explícitamente en este permiso, no se otorga ningún otro permiso, licencia ni derecho, ya sea explícito o implícito, sobre las publicaciones, la información, los datos, el software o cualquier otra propiedad intelectual contenida en ellas.

IBM se reserva el derecho de retirar los permisos aquí concedidos siempre que, según el parecer del fabricante, se utilicen las publicaciones en detrimento de sus intereses o cuando, también según el parecer del fabricante, no se sigan debidamente las instrucciones anteriores.

No puede bajar, exportar ni reexportar esta información si no lo hace en plena conformidad con la legislación y normativa vigente, incluidas todas las leyes y normas de exportación de Estados Unidos.

IBM NO PROPORCIONA NINGUNA GARANTÍA SOBRE EL CONTENIDO DE ESTAS PUBLICACIONES. LAS PUBLICACIONES SE PROPORCIONAN "TAL CUAL", SIN GARANTÍA DE NINGUNA CLASE, YA SEA EXPLÍCITA O IMPLÍCITA, INCLUIDAS, PERO SIN LIMITARSE A ELLAS, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN, NO VULNERACIÓN E IDONEIDAD PARA UN FIN DETERMINADO.

Número de Programa: 5770-SS1

Impreso en España