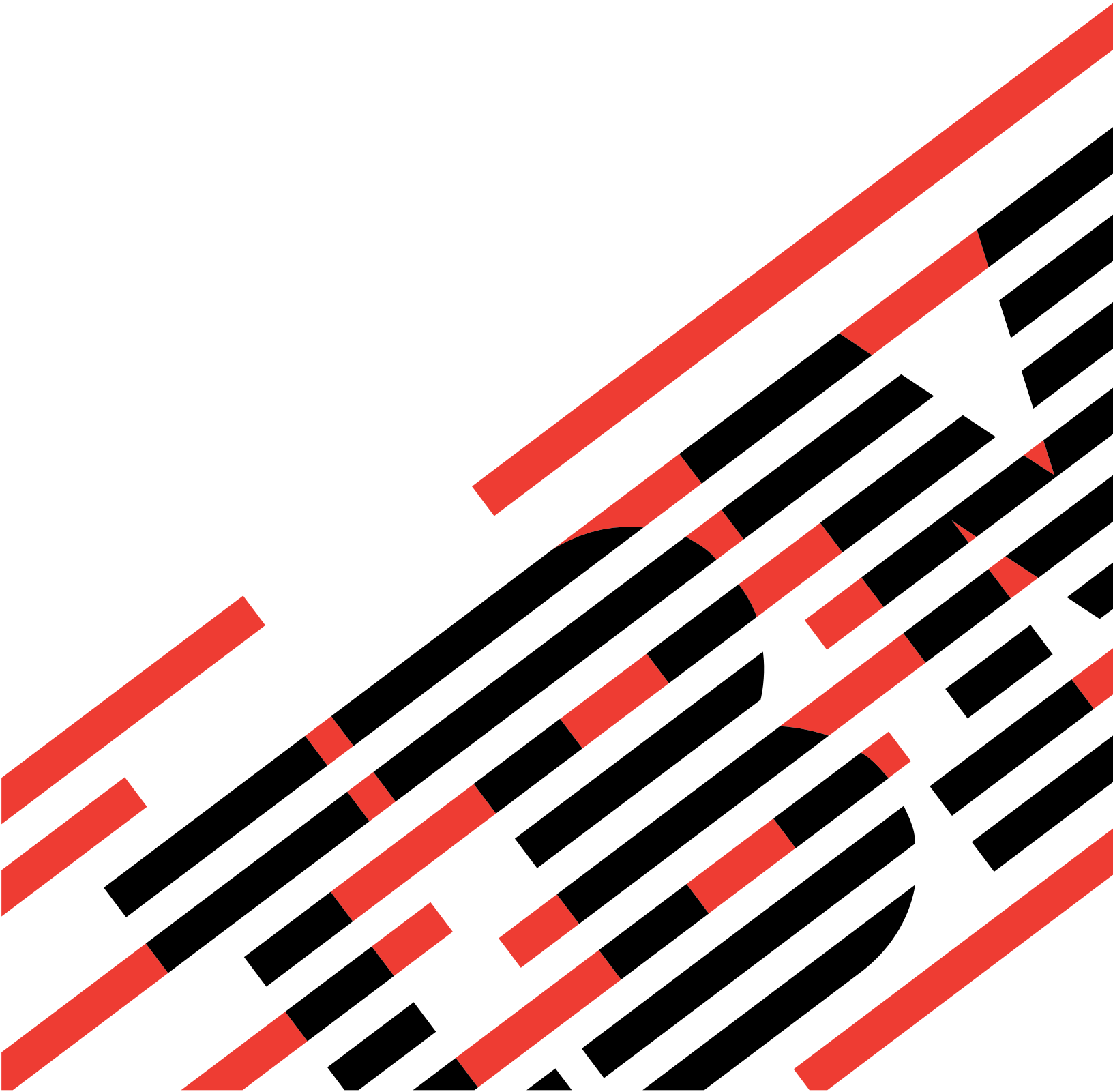
IBM

eserver

iSeries

Red privada virtual



IBM

@server

iSeries

Red privada virtual

Contenido

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.

OS/400 VPN es un componente opcionalmente instalable de iSeries Navigator, la interfaz gráfica de usuario (GUI) para OS/400. Permite crear un camino de extremo a extremo entre cualquier combinación de sistema principal y pasarela. OS/400 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 impacto que una VPN tendrá en toda su red. Es esencial realizar una buena planificación e implementación para que los resultados sean satisfactorios. Deberá revisar estos temas para asegurar que sabe cómo funcionan las VPN y cómo debe utilizarlas:

Novedades de V5R2
En este tema se describe qué información es nueva o ha cambiado significativamente en este release.

Imprimir este tema
Si prefiere disponer de una copia impresa de esta información, diríjase aquí para imprimir el archivo PDF.

Escenarios de VPN
Revise estos escenarios para estar familiarizado con los tipos de VPN básicos y los pasos que debe seguir para configurarlos.

Conceptos de VPN
Es importante que tenga al menos un conocimiento básico de las tecnologías VPN estándares. Este tema le ofrece información conceptual sobre los protocolos que VPN utiliza en su implementación.

Planificar 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 enlaces con un asesor de planificación que generará una hoja de trabajo de planificación personalizada para sus especificaciones.

Configurar VPN
Después de haber planificado la VPN, puede empezar a configurarla. Este tema le ofrece una visión general de lo que puede hacer con VPN y cómo llevarlo a cabo.

Gestionar VPN
En este tema se describen varias tareas que puede llevar a cabo para gestionar las conexiones VPN activas, incluyendo cómo modificarlas, cómo supervisarlas y cómo eliminarlas.

Resolución de problemas de VPN
Consulte este tema cuando tenga problemas con las conexiones VPN.

Información relacionada para VPN
Diríjase aquí para obtener enlaces a otras fuentes de información de VPN y temas relacionados.

Novedades de V5R2

Las mejoras de la Versión 5 Release 2 (V5R2) con respecto a la función de red privada virtual (VPN) son:

- IPSec compatible con NAT, también conocido técnicamente como encapsulación UDP, para direccionar las diversas incompatibilidades entre las tecnologías IPSec y NAT (conversión de direcciones de red). La encapsulación UDP permite que el iSeries se oculte detrás de un cortafuegos que utiliza NAT. A diferencia de los releases anteriores de OS/400 VPN, ya no es necesario situar el iSeries en el perímetro de la red, utilizar una dirección pública ni utilizar IP virtual para poder crear conexiones VPN.
- Filtros de políticas dinámicos. Ahora puede crear una VPN que no tenga asociada una norma de filtro de políticas. El sistema gestiona dinámicamente todos los filtros para la conexión, lo cual significa que no es necesario configurar normas de paquetes para poder disponer de una conexión VPN.
- Asistente Migrar filtros de políticas. Si ha actualizado el sistema desde V4R4 o V4R5 y desea utilizar las normas que ha cargado en ese sistema antes de la actualización, debe utilizar el asistente Migrar normas de política para eliminar los filtros de políticas de los archivos de normas de paquetes que ha creado. El asistente inserta filtros de políticas equivalentes en el conjunto de filtros de políticas generados por VPN. Esto ayudará a garantizar que los filtros de políticas antiguos y nuevos funcionen conjuntamente según lo esperado.
- Algoritmo AES (estándar de cifrado avanzado). Ahora, OS/400 VPN soporta AES para la protección de datos.

Los cambios de V5R2 con respecto al tema de VPN son:

- Escenarios adicionales para una mejor comprensión del funcionamiento de VPN en un entorno empresarial:
- Actualización del asesor de planificación VPN que le ayuda a determinar qué tipo de VPN debe crear para orientar sus necesidades comerciales específicas. El asesor también le aconseja los pasos que debe seguir para configurar su VPN.

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

.

Escenarios de VPN

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

- **Escenario de VPN: 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 sistemas iSeries que actúan como pasarelas VPN.

- **Escenario de VPN: 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.
- **Escenario de VPN: proteger un túnel voluntario L2TP con IPSec**
  Este escenario ilustra una conexión entre el sistema principal 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.
- **Escenario de VPN: utilizar la conversión de direcciones de red para VPN**
  En este escenario, la empresa desea intercambiar datos sensibles con uno de sus asociados comerciales mediante OS/400 VPN. Para preservar mejor la privacidad de la estructura de red de la empresa, ésta también utilizará NAT VPN para ocultar la dirección IP privada del iSeries que utiliza para alojar las aplicaciones a las que el asociado comercial tiene acceso.

Más escenarios de VPN
Para obtener más escenarios de VPN, consulte estos otros recursos de información VPN:

- **Escenario de QoS: resultados seguros y previsibles (VPN y QoS)**
  Puede crear políticas de calidad de servicio (QoS) con la VPN. Este ejemplo muestra la utilización conjunta de las dos.
- **OS/400 V5R1 Virtual Private Networks: Remote Access to the IBM e(logo)server iSeries Server with Windows 2000 VPN Clients, REDP0153**

  Este Redpaper de IBM proporciona un proceso paso a paso para configurar el túnel VPN utilizando VPN V5R1 y el soporte de L2TP e IPSec nativo de Windows 2000.
- **AS/400 Internet Security: Implementing AS/400 Virtual Private Networks, SG24-5404-00**

  Este libro rojo explora los conceptos VPN y describe su implementación utilizando IPSec (IP Security) y L2TP (Layer 2 Tunneling Protocol) en OS/400.
- **AS/400 Internet Security Scenarios: A Practical Approach, SG24-5954-00**

  Este libro rojo explora todas las funciones de seguridad nativas disponibles en el sistema AS/400, como pueden ser filtros IP, NAT, VPN, servidor proxy HTTP, SSL, DNS, retransmisión de correo, auditoría y anotaciones. Describe su utilización a través de ejemplos prácticos.

Escenario de VPN: conexión básica entre sucursales

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.

Nota importante:
Este escenario muestra las pasarelas de seguridad de iSeries 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. Revise el redbook AS/400 Internet Security Scenarios: A Practical Approach, SG24-5954-00

, para obtener una descripción detallada de varios métodos destinados a reducir estos riesgos.

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 servidores 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 Internet.

Objetivos

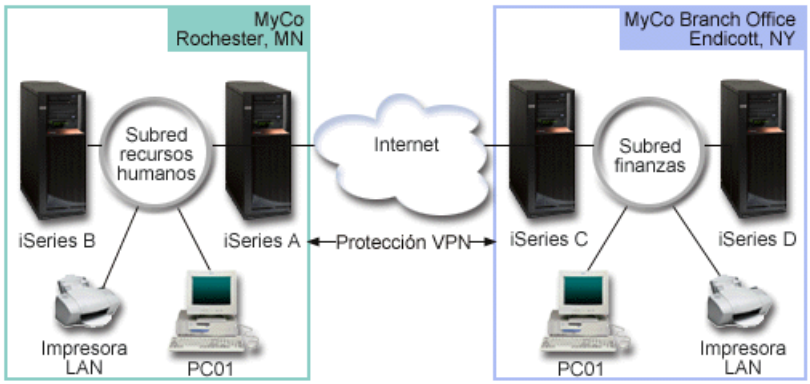
En este escenario, MyCo, Inc. desea establecer una VPN entre las subredes de sus departamentos de Recursos Humanos y Finanzas mediante un par de servidores iSeries. Ambos servidores actuarán como pasarelas de VPN. En términos de configuraciones de VPN, una pasarela realiza la gestión de claves y aplica 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 sistemas principales de cada red tienen acceso total a la red de los demás, incluyendo todas las aplicaciones.
- Los servidores 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

- iSeries-A se ejecuta en OS/400 Versión 5 Release 2 (V5R2) y actúa como la 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.
- iSeries-A se conecta a Internet mediante la dirección IP 204.146.18.227. Este es el punto final de conexión. Es decir, iSeries-A realiza la gestión de claves y aplica IPSec a los datagramas IP entrantes y salientes.
- iSeries-A se conecta a la subred con la dirección IP 10.6.11.1.
- iSeries-B es un servidor de producción de la subred de Recursos Humanos que ejecuta aplicaciones TCP/IP estándares.

Departamento de Finanzas

- iSeries-C se ejecuta en OS/400 Versión 5 Release 2 (V5R2) y actúa como la 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.
- iSeries-C se conecta con Internet mediante la dirección IP 208.222.150.250. Este es el punto final de conexión. Es decir, iSeries-C realiza la gestión de claves y aplica IPSec a los datagramas IP entrantes y salientes.
- iSeries-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:

1. Verificar el direccionamiento de TCP/IP para asegurar que los servidores de ambas pasarelas pueden comunicarse entre sí a través de Internet. Con esto se asegura de que los sistemas principales de cada subred efectúen el direccionamiento correctamente hacia las pasarelas respectivas para poder acceder a la subred remota.
   Nota: el direccionamiento no entra dentro del ámbito de este tema. Si tiene dudas, por favor consulte Direccionamiento y equilibrio de la carga de trabajo TCP/IP en Information Center.
2. Completar (Consulte 6) las hojas de trabajo de planificación y las listas de comprobación de ambos sistemas.
3. Configurar (Consulte 7) la VPN en la pasarela VPN de Recursos Humanos (iSeries-A).
4. Configurar (Consulte 8) la VPN en la pasarela VPN de Finanzas (iSeries-C).

5. Asegurarse de que los servidores VPN se han iniciado (Consulte 8).
6. Probar (Consulte 8) las comunicaciones entre ambas subredes remotas.

Detalles de configuración

Tras haber completado el primer paso, verificando que el direccionamiento de TCP/IP funciona correctamente y que los servidores de pasarela pueden comunicarse, ya está preparado para empezar a configurar la VPN.

Paso 2: 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: estas hojas de trabajo son aplicables a iSeries-A; para iSeries-C, repita el proceso invirtiendo las direcciones IP de la forma necesaria.

Lista de comprobación de los prerrequisitos	**Respuestas**
¿Su OS/400 es V5R2 (5722-SS1) o posterior?	Sí
¿Se encuentra instalada la opción de Digital Certificate Manager (5722-SS1 Opción 34)?	Sí
¿Está instalado Cryptographic Access Provider (5722-AC2 o AC3)?	Sí
¿Está instalado iSeries Access para Windows (5722-XE1)?	Sí
¿Está instalado iSeries Navigator?	Sí
¿Está instalado el subcomponente de red de iSeries Navigator?	Sí
¿Está instalado TCP/IP Connectivity Utilities para OS/400 (5722-TC1)?	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 iSeries (incluyendo las interfaces IP, rutas IP, el nombre del sistema principal 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 implementan el filtrado de paquetes IP, ¿soportan las normas de filtrado 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

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 Máscara: 255.255.0.0

Necesita esta información para configurar la VPN	Respuestas
¿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 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

Paso 3: configurar la VPN en iSeries-A

Utilice la información de sus hojas de trabajo para configurar la VPN en iSeries-A de la forma siguiente:

1. En iSeries Navigator, expanda **——>Red —>Políticas IP** de iSeries-A.
2. Pulse con el botón derecho del ratón **Red privada virtual** y seleccione **Nueva conexión** para iniciar el asistente Nueva conexión.
3. Revise la página de **Bienvenida** para obtener información acerca de los objetos que crea el asistente.
4. Pulse **Siguiente** para ir a la página **Nombre de la conexión**.
5. En el campo **Nombre**, especifique `HRgw2FINgw`.
6. (opcional) Especifique una descripción para este grupo de conexión.
7. Pulse **Siguiente** para ir a la página **Escenario de la conexión**.
8. Seleccione **Conectar su pasarela a otra pasarela**.
9. Pulse **Siguiente** para ir a la página **Política de intercambio de claves de Internet**.
10. Seleccione **Crear una nueva política** y, a continuación, seleccione **Equilibrar seguridad y rendimiento**.
11. Pulse **Siguiente** para ir a la página **Certificado para punto final de conexión local**.
12. Seleccione **No** para indicar que no utilizará certificados para autenticar la conexión.
13. Pulse **Siguiente** para ir a la página **Servidor de claves local**.
14. Seleccione **Dirección IP de Versión 4** en el campo **Tipo de identificador**.
15. Seleccione `204.146.18.227` en el campo **Dirección IP**.
16. Pulse **Siguiente** para ir a la página **Servidor de claves remoto**.
17. Seleccione **Dirección IP de Versión 4** en el campo **Tipo de identificador**.
18. Especifique `208.222.150.250` en el campo **Identificador**.
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 `10.6.0.0` en el campo **Identificador**.
23. Especifique `255.255.0.0` en el campo **Máscara de subred**.
24. Pulse **Siguiente** para ir a la página **Punto final de datos remoto**.
25. Seleccione **Subred IP versión 4** en el campo **Tipo de identificador**.
26. Especifique `10.196.8.0` en el campo **Identificador**.
27. Especifique `255.255.255.0` en el campo **Máscara de subred**.
28. Pulse **Siguiente** para ir a la página **Servicios de datos**.
29. Acepte los valores por omisión y, a continuación, pulse **Siguiente** para ir a la página **Política de datos**.

30. Seleccione **Crear una nueva política** y, a continuación, seleccione **Equilibrar seguridad y rendimiento**. Seleccione **Utilizar el algoritmo de cifrado RC4**.
31. Pulse **Siguiente** para ir a la página **Interfaces aplicables**.
32. Seleccione **TRLINE** en la tabla **Línea**.
33. Pulse **Siguiente** para ir a la página **Resumen**. Revise los objetos que creará el asistente para asegurar que son correctos.
34. Pulse **Finalizar** para completar la configuración.
35. Cuando aparezca el diálogo **Activar filtros de políticas**, seleccione **Si, activar los filtros de política generados** y, a continuación, seleccione **Permitir el resto de tráfico**. Pulse **Aceptar** para completar la configuración. Cuando se le solicite, especifique que desea activar las normas en todas las interfaces.

Ahora ha finalizado la configuración de VPN en iSeries-A. El siguiente paso es configurar la VPN en la pasarela VPN (iSeries-C) del Departamento de Finanzas.

Paso 4: configurar la VPN en iSeries-C

Siga los mismos pasos que para configurar iSeries-A, invirtiendo las direcciones IP de la forma apropiada. 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.

Paso 6: iniciar los servidores VPN

Para iniciar los servidores VPN, siga estos pasos:

1. En iSeries Navigator, expanda **el servidor —>Red —>Políticas IP**.
2. Pulse con el botón derecho del ratón **VPN (red privada virtual)** y seleccione **Iniciar**.

Paso 7: probar la conexión

Tras haber finalizado la configuración de ambos servidores y haber iniciado satisfactoriamente los servidores VPN, debe probar la conectividad. Para ello, siga estos pasos:

1. En iSeries Navigator, expanda **iSeries-A —>Red**.
2. Pulse dos veces **Configuración TCP/IP**, seleccione **Utilidades** y, a continuación, seleccione **PING**.
3. Desde el diálogo **Realizar PING desde**, especifique `iSeries-C` en el campo **PING**.
4. Pulse **Realizar PING ahora** para verificar la conectividad de iSeries-A con iSeries-C.
5. Pulse **Aceptar** cuando haya finalizado.

Escenario de VPN: conexión básica de empresa a empresa

Muchas empresas utilizan frame relay o líneas alquiladas para suministrar conexiones seguras a sus socios comerciales, sucursales y proveedores. Por desgracia, estas soluciones suelen ser caras y limitadas geográficamente. VPN ofrece una alternativa para las empresas que deseen disponer de comunicaciones privadas y a un bajo coste.

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 red privada virtual (VPN) que satisfaga las necesidades de ambas empresas.

Objetivos

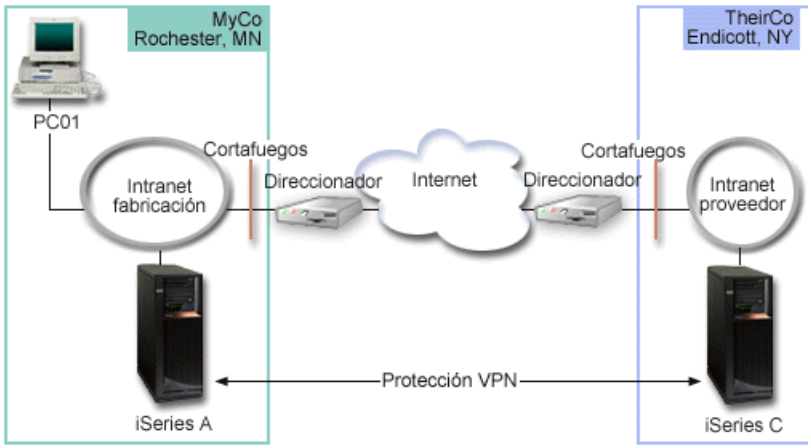
En este escenario, MyCo desea establecer una VPN entre un sistema principal de su división de componentes y un sistema principal del departamento de manufactura de uno de sus socios comerciales, TheirCo.

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.

Nota importante:
La intención de este escenario es introducir, mediante ejemplos, una configuración de VPN simple de sistema principal a sistema principal. 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

- iSeries-A se ejecuta en OS/400 Versión 5 Release 2 (V5R2).
- iSeries-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, iSeries-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.
- iSeries-A se encuentra en la subred 10.6.0.0 con la máscara 255.255.0.0
- Sólo iSeries-A puede iniciar la conexión con iSeries-C.

red de manufactura de TheirCo

- iSeries-C se ejecuta en OS/400 Versión 5 Release 2 (V5R2).

- iSeries-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, iSeries-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.
- iSeries-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:

1. Verificar el direccionamiento de TCP/IP para asegurar que iSeries-A y iSeries-C pueden comunicarse entre sí a través de Internet. Con esto se asegura de que los sistemas principales de cada subred efectúen el direccionamiento correctamente hacia las pasarelas respectivas para poder acceder a la subred remota. Deberá ser consciente de que, para este escenario, necesitará considerar el direccionamiento de direcciones privadas que puede no haber sido necesario con anterioridad.

   Nota: el direccionamiento no entra dentro del ámbito de este tema. Si tiene dudas, consulte el tema Direccionamiento y equilibrio de la carga de trabajo TCP/IP en Information Center.
2. Completar (Consulte 10) las hojas de trabajo de planificación y las listas de comprobación de ambos sistemas.
3. Configurar (Consulte 11) la VPN en iSeries-A en la red de suministro de MyCo.
4. Configurar (Consulte 12) la VPN en iSeries-C en la red de manufactura de TheirCo.
5. Activar (Consulte 12) las normas de filtrado en ambos servidores.
6. Iniciar (Consulte 13) la conexión desde iSeries-A.
7. Probar (Consulte 13) las comunicaciones entre ambas subredes remotas.

Detalles de configuración

Tras haber completado el primer paso, verificando que el direccionamiento de TCP/IP funciona correctamente y que los servidores pueden comunicarse, ya está preparado para empezar a configurar la VPN.

Paso 2: 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: estas hojas de trabajo son aplicables a iSeries-A, repita el proceso para iSeries-C, invirtiendo las direcciones IP de la forma necesaria.

Lista de comprobación de los prerrequisitos	Respuestas
¿Su OS/400 es V5R2 (5722-SS1) o posterior?	Sí
¿Se encuentra instalada la opción de Digital Certificate Manager (5722-SS1 Opción 34)?	Sí
¿Está instalado Cryptographic Access Provider (5722-AC2 o AC3)?	Sí
¿Está instalado iSeries Access para Windows (5722-XE1)?	Sí
¿Está instalado iSeries Navigator?	Sí
¿Está instalado el subcomponente de red de iSeries Navigator?	Sí
¿Está instalado TCP/IP Connectivity Utilities para OS/400 (5722-TC1)?	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 iSeries (incluyendo las interfaces IP, rutas IP, el nombre del sistema principal 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 implementan el filtrado de paquetes IP, ¿soportan las normas de filtrado 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

Necesita esta información para configurar la VPN	**Respuestas**
¿Qué tipo de conexión está creando?	de sistema principal a sistema principal
¿Cómo se denominará el grupo de claves dinámicas?	MyCo2TheirCo
¿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?	Sí
¿Cuál es el identificador del servidor de claves local?	Dirección IP: 10.6.1.1
¿Cuál es el identificador del punto final de datos local?	Dirección IP: 10.6.1.1
¿Cuál es el identificador del servidor de claves remoto?	Dirección IP: 10.196.8.6
¿Cuál es el identificador del punto final de datos remoto?	Dirección IP: 10.196.8.6
¿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

Paso 3: configurar la VPN en iSeries-A

Utilice la información de sus hojas de trabajo para configurar la VPN en iSeries-A de la forma siguiente:

1. En iSeries Navigator, expanda el servidor **—>Red —>Políticas IP**.
2. Pulse con el botón derecho del ratón **Red privada virtual** y seleccione **Nueva conexión** para iniciar el Asistente de conexión.
3. Revise la página de **Bienvenida** para obtener información acerca de los objetos que crea el asistente.
4. Pulse **Siguiente** para ir a la página **Nombre de la conexión**.
5. En el campo **Nombre**, especifique `MyCo2TheirCo`.
6. (opcional) Especifique una descripción para este grupo de conexión.
7. Pulse **Siguiente** para ir a la página **Escenario de la conexión**.
8. Seleccione **Conectar su sistema principal a otro sistema principal**.
9. Pulse **Siguiente** para ir a la página **Política de intercambio de claves de Internet**.
10. Seleccione **Crear una nueva política** y, a continuación, seleccione **Máxima seguridad, mínimo rendimiento**.
11. Pulse **Siguiente** para ir a la página **Certificado para punto final de conexión local**.
12. Seleccione **Sí** para indicar que utilizará certificados para autenticar la conexión. A continuación, seleccione el certificado que representa iSeries-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).

13. Pulse **Siguiente** para ir a la página **Identificador de punto final de conexión local**.
14. Seleccione **Dirección IP versión 4** como tipo de identificador. La dirección IP asociada deberá ser 10.6.1.1. De nuevo, esta información se define en el certificado que cree en el DCM.
15. Pulse **Siguiente** para ir a la página **Servidor de claves remoto**.
16. Seleccione **Dirección IP de Versión 4** en el campo **Tipo de identificador**.
17. Especifique `10.196.8.6` en el campo **Identificador**.
18. Pulse **Siguiente** para ir a la página **Servicios de datos**.
19. Acepte los valores por omisión y, a continuación, pulse **Siguiente** para ir a la página **Política de datos**.
20. Seleccione **Crear una nueva política** y, a continuación, seleccione **Máxima seguridad, mínimo rendimiento**. Seleccione **Utilizar el algoritmo de cifrado RC4**.
21. Pulse **Siguiente** para ir a la página **Interfaces aplicables**.
22. Seleccione **TRLINE**.
23. Pulse **Siguiente** para ir a la página **Resumen**. Revise los objetos que creará el asistente para asegurar que son correctos.
24. Pulse **Finalizar** para completar la configuración.
25. Cuando aparezca el 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 iSeries-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.

Ahora ha finalizado la configuración de VPN en iSeries-A. El siguiente paso es configurar la VPN en iSeries-C en la red de manufactura de TheirCo.

Paso 4: configurar la VPN en iSeries-C

Siga los mismos pasos que para configurar iSeries-A, invirtiendo las direcciones IP de la forma apropiada. Utilice las hojas de trabajo de planificación como guía. Cuando termine de configurar iSeries-C, deberá activar las normas de filtrado que el Asistente de conexión creó en cada servidor.

Paso 5: activar las normas de paquete

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 VPN. Para hacer esto en iSeries-A, siga estos pasos:

1. En iSeries Navigator, expanda **iSeries-A—>Red —>Políticas IP**.
2. Pulse con el botón derecho del ratón **Normas de paquetes** y seleccione **Activar**. De esta forma, se abrirá el diálogo Activar normas de paquetes.
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. En este caso, seleccione **Todas las interfaces**.
5. Pulse **Aceptar** en el 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. Para obtener información acerca de los mensajes asociados con un número de línea y archivo específico, puede pulsar el error con el botón derecho del ratón y seleccionar **Ir a línea** para resaltar el error en el archivo.
6. Repita estos pasos para activar las normas de paquetes en iSeries-C.

Paso 6: iniciar la conexión

Siga estos pasos para configurar la VPN MyCo2TheirCo desde iSeries-A:

1. En iSeries Navigator, expanda **iSeries-A—>Red —>Políticas IP**.
2. Si el servidor VPN no está iniciado, pulse con el botón derecho del ratón **Red privada virtual** y seleccione **Iniciar**. De esta forma, se iniciará el servidor VPN.
3. Expanda **Red privada virtual —>Conexiones de seguridad**.
4. Pulse **Todas las conexiones** para visualizar una lista de conexiones en el panel derecho.
5. Pulse con el botón derecho del ratón **MyCo2TheirCo** y seleccione **Iniciar**.
6. 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*.

Paso 7: probar la conexión

Tras haber finalizado la configuración de ambos servidores y haber iniciado satisfactoriamente la conexión, deberá probar la conectividad para asegurar que los sistemas principales remotos pueden comunicarse entre sí. Para hacer esto, siga estos pasos:

1. En iSeries Navigator, expanda **iSeries-A —>Red**.
2. Pulse dos veces **Configuración TCP/IP** y seleccione **Utilidades** y, a continuación, seleccione **PING**.
3. Desde el diálogo **Realizar PING desde**, especifique `iSeries-C` en el campo **PING**.
4. Pulse **Realizar PING ahora** para verificar la conectividad de iSeries-A con iSeries-C.
5. Pulse **Aceptar** cuando haya finalizado.

Escenario de VPN: proteger un túnel voluntario L2TP con IPSec

Suponga que su empresa tiene una pequeña sucursal en otro estado. A lo largo de cualquier día laboral, la sucursal necesitará tener acceso a información confidencial en un iSeries dentro de la intranet de su 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 de empresa, 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 de empresa. La funcionalidad del concentrador de acceso L2TP (LAC) reside en el cliente. El túnel es transparente para el suministrador de servicios de Internet (ISP) del cliente, o sea que ya no se necesita el ISP para soportar L2TP. Si desea leer más sobre los conceptos de L2TP, consulte Layer 2 Tunnel Protocol (L2TP).

Nota importante:
Este escenario muestra las pasarelas de seguridad de iSeries 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. Revise el redbook AS/400 Internet Security Scenarios: A Practical Approach, SG24-5954-00

, para obtener una descripción detallada de varios métodos destinados a reducir estos riesgos.

Objetivos

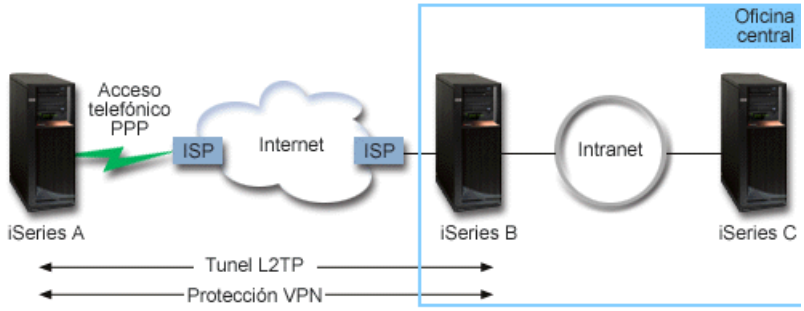
En este escenario, el iSeries de una sucursal se conecta con su red de empresa mediante una pasarela iSeries con un túnel L2TP protegido por VPN.

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 sistema principal, no de pasarela.
- El sistema de la oficina central es un sistema principal en la red de la empresa.

Detalles

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



iSeries-A

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

iSeries-B

- Debe tener acceso a las aplicaciones TCP/IP de iSeries-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, iSeries-B realiza la gestión de claves y aplica IPSec a los datagramas IP entrantes y salientes. iSeries-B se conecta a la subred con la dirección IP 10.6.11.1.

En términos de L2TP, *iSeries-A* actúa como iniciador de L2TP, mientras que *iSeries-B* actúa como terminador de L2TP.

Tareas de configuración

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

1. Configurar la VPN (Consulte 15) en iSeries-A.
2. Configurar un PPP perfil de conexión y una línea virtual (Consulte 17)para iSeries-A.
3. Aplicar (Consulte 18)el grupo de claves dinámicas al perfil PPP.
4. Configurar VPN (Consulte 18) en iSeries-B.
5. Configurar un PPP perfil de conexión y una línea virtual (Consulte 18) para iSeries-B.
6. Activar (Consulte 19) las normas de paquetes en iSeries-A e iSeries-B.
7. Iniciar (Consulte 20) la conexión desde iSeries-A.

Detalles de configuración

Tras haber verificado que TPC/IP funciona correctamente y los servidores iSeries pueden comunicarse, ya está preparado para empezar a configurar la conexión descrita en este escenario.

Paso 1: configurar la VPN en iSeries-A

Siga estos pasos para configurar la VPN en iSeries-A:

1. **Configurar la política de intercambio de claves de Internet**
   a. En iSeries Navigator, expanda iSeries-A **—> Red—> Políticas IP—> Red privada virtual—> Políticas de seguridad IP**.
   b. Pulse con el botón derecho del ratón **Políticas de intercambio de claves de Internet** y seleccione **Nueva política de intercambio de claves de Internet**
   c. 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**.
   d. En la página **Asociaciones**, seleccione **Clave precompartida** para indicar que esta conexión utiliza una clave precompartida para autenticar esta política.
   e. Especifique la clave precompartida en el campo **Clave**. Debe tratar la clave precompartida como si fuera una contraseña.
   f. 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. iSeries-B utiliza este identificador para identificar iSeries-A cuando éste inicia una conexión.
   g. En la página **Transformaciones**, pulse **Añadir** para añadir las transformaciones que iSeries-A propone a iSeries-B para proteger las claves y especificar si la política IKE utiliza la protección de identidad al iniciar las negociaciones de fase 1.
   h. En la página **Transformación de política IKE**, seleccione **Clave precompartida** para su método de autenticación, **SHA** para el algoritmo hash y **3DES-CBC** para el algoritmo de cifrado. Haga caducar las claves IKE y después acepte los valores del grupo Diffie-Hellman.
   i. Pulse **Aceptar** para volver a la página **Transformaciones**.
   j. Seleccione **Negociación de modalidad agresiva de IKE (sin protección de identidad)**
   k. Pulse **Aceptar** para guardar los cambios.
2. **Configurar la política de datos**
   a. Desde la interfaz VPN, pulse con el botón derecho del ratón **Políticas de datos** y seleccione **Nueva política de datos**.
   b. En la página **General**, especifique el nombre de la política de datos. Por ejemplo, `l2tpremoteuser`.
   c. 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.

d. Pulse **Añadir** para añadir una transformación de política de datos.

e. Seleccione **Transportar** para la modalidad de encapsulado.

f. Especifique un valor de caducidad para la clave

g. Pulse **Aceptar** para volver a la página **Transformaciones**.

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

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

4.

a. Desde la interfaz VPN, expanda **Conexiones de seguridad**.

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 sistemas principales**.

f. Vaya a la página **Política**. Seleccione la política de datos que creó en el paso 2, `l2tpremoteuser`, en la lista desplegable **Política de datos**.

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

Ahora, necesitará añadir una conexión al grupo que acaba de crear.

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

a. Desde la interfaz VPN, expanda **Por grupo**. De esta forma se visualizará una lista de todos los grupos de claves dinámicas que ha configurado en iSeries-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.

Ahora ha finalizado la configuración de VPN en iSeries-A. El siguiente paso es configurar un perfil PPP para iSeries-A.

Paso 2: Configurar un perfil de conexión PPP y una línea virtual en iSeries-A

En esta sección se describen los pasos que debe seguir para crear el perfil PPP para iSeries-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 iSeries-A:

1. En iSeries Navigator, expanda iSeries-A **—>Red—>Servicios de acceso remoto**.
2. Pulse con el botón derecho del ratón **Perfiles de conexión de originador** y seleccione **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 sistema principal local, etc. Se abrirá el 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 sistema principal local**, especifique el nombre del sistema principal del servidor de claves local, `iSeriesA`.
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 1, `l2tptocorp`, en la lista desplegable **Nombre de grupo de conexión**.
17. Vaya a la página **Valores 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, iSeries-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. Pulse **Aceptar** para cerrar el diálogo Direccionamiento.
25. Vaya a la página **Autenticación** para establecer el nombre y la contraseña de usuario para este perfil PPP.
26. En la sección de identificación del sistema local, seleccione **Permitir que el sistema remoto verifique la identidad de este sistema**.
27. Bajo **Protocolo de autenticación a utilizar**, seleccione **Se requiere contraseña cifrada (CHAP-MD5)**
28. Especifique el nombre de usuario, `iSeriesA` y una contraseña.
29. Pulse **Aceptar** para guardar el perfil PPP.

Paso 3: aplicar el 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 hacer esto, siga estos pasos:

1. Vaya a la interfaz VPN, expanda **Conexiones de seguridad—>Por grupo**.
2. Pulse con el botón derecho del ratón el grupo de claves dinámicas, `l2tptocorp` y seleccione **Propiedades**.
3. Vaya a la página **Interfaces** y seleccione **Aplicar este grupo** para el perfil PPP que creó en el paso 2, `toCorp`.
4. Pulse **Aceptar** para aplicar `l2tptocorp` al perfil PPP, `toCorp`.

Paso 4: configurar la VPN en iSeries-B

Siga los mismos pasos que para configurar iSeries-A, invirtiendo las direcciones IP y los identificadores de la forma apropiada. 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 iSeries-A. Por ejemplo, `thisisthekeyid`.
- Utilice *exactamente* la misma clave precompartida.
- Asegúrese de que sus transformaciones coinciden con las que ha configurado en iSeries-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.

Paso 5: Configurar un perfil de conexión PPP y una línea virtual en iSeries-B

Siga estos pasos para crear un perfil de conexión PPP para iSeries-B:

1. En iSeries Navigator, expanda iSeries-B **—>Red—>Servicios de acceso remoto**.

2. Pulse con el botón derecho del ratón **Perfiles de conexión de contestador** y seleccione **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 sistema principal local, etc. Se abrirá el diálogo **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 sistema principal local**, especifique el nombre del sistema principal del servidor de claves local, `iSeriesB`.
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 diálogo **Identificación del sistema local**.
22. Bajo **Protocolo de autenticación a utilizar**, seleccione **Se requiere contraseña cifrada (CHAP-MD5)**
23. Especifique el nombre de usuario, `iSeriesB` y una contraseña.
24. Pulse **Aceptar** para guardar el perfil PPP.

Paso 6: activar normas de paquete

VPN crea automáticamente las normas de paquetes que esta conexión requiere para funcionar adecuadamente. Sin embargo, deberá activarlas en ambos sistemas antes de poder iniciar la conexión VPN. Para hacer esto en iSeries-A, siga estos pasos:

1. En iSeries Navigator, expanda **iSeries-A—>Red —>Políticas IP**.
2. Pulse con el botón derecho del ratón **Normas de paquetes** y seleccione **Activar**. De esta forma, se abrirá el diálogo Activar normas de paquetes.
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. En este caso, seleccione **Todas las interfaces**.

5. Pulse **Aceptar** en el 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. Para obtener información acerca de los mensajes asociados con un número de línea y archivo específico, puede pulsar el error con el botón derecho del ratón y seleccionar **Ir a línea** para resaltar el error en el archivo.
6. Repita estos pasos para activar las normas de paquetes en iSeries-B.

Paso 7: iniciar la conexión

El último paso consiste en iniciar la conexión. Para poder iniciar una conexión L2TP, debe habilitar el terminador L2TP para que responda a las peticiones del iniciador. Tras asegurarse de que todos los servicios necesarios se han iniciado, inicie la conexión PPP en el extremo del terminador. Los siguientes pasos describen cómo iniciar la conexión PPP en iSeries-B:

1. En iSeries Navigator, expanda iSeries-B **—> Red—> Servicios de acceso remoto**.
2. Pulse **Perfiles de conexión del contestador** para visualizar una lista de los perfiles del contestador en el panel derecho.
3. Pulse con el botón derecho del ratón `tobranch` y seleccione **Iniciar**. Después de que se haya iniciado el perfil de la conexión, la ventana se renueva y muestra la conexión como `En espera de peticiones de conexión`. Ahora, iSeries-A puede contestar a las peticiones de conexión L2TP desde iSeries-B.

Siga estos pasos para iniciar la conexión L2TP en iSeries-A:

1. En iSeries Navigator, expanda iSeries-A **—> Red —>Servicios de acceso remoto**.
2. Pulse **Perfiles de conexión del originador** para visualizar una lista de perfiles de originador en el panel derecho.
3. Pulse con el botón derecho del ratón **toCORP** y seleccione **Iniciar**. Después de que se haya iniciado el perfil de la conexión, la ventana se renueva y muestra la conexión como `Estableciendo túnel L2TP`.
4. Pulse F5 para renovar la pantalla. Si el túnel L2TP se ha iniciado satisfactoriamente, el estado de la conexión mostrará `Conexiones activas`.

Escenario de VPN: utilizar la conversión de direcciones de red para VPN

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 iSeries que alberga las aplicaciones a las que el proveedor tiene acceso. La cuestión es: ¿cómo realizar este trabajo?

La respuesta: OS/400 VPN. Utilícela 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, NAT VPN realiza conversiones de direcciones antes de la validación SA, asignando una

dirección a la conexión cuando ésta se inicia.

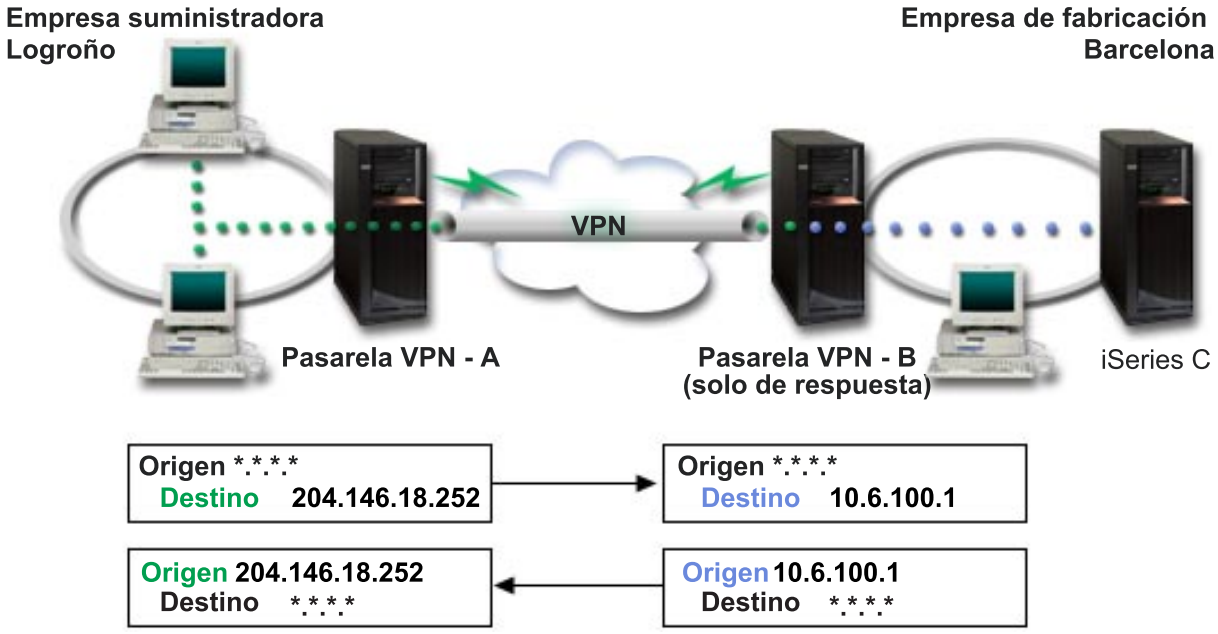
Objetivos

Los objetivos de este escenario son:

- permitir a los clientes de la red del proveedor el acceso a un sólo sistema principal iSeries de la red del fabricante a través de una conexión VPN de pasarela a pasarela.
- ocultar la dirección IP privada del sistema principal iSeries 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 a iSeries-C).
- iSeries-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 de iSeries-C, 10.6.100.1.
- La pasarela-B VPN convierte la dirección pública de iSeries-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 de iSeries-C, 204.146.18.252. En lo que concierne a los clientes de la red del proveedor, la dirección IP de iSeries-C es 204.146.18.252. Nunca deben tener 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 **iSeries-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 de 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 OS/400 VPN los utiliza:

- **Protocolos IPSec (IP Security)**
  IPSec proporciona una base estable y duradera para proporcionar seguridad de capa de red.
- **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.
- **L2TP (Layer 2 Tunneling Protocol)**
  Si tiene pensado utilizar una conexión VPN para asegurar las conexiones entre su red y los clientes remotos, deberá asimismo estar familiarizado con L2TP.
- **NAT VPN (Conversión de direcciones de red para VPN)**
  OS/400 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.
- **Encapsulación 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.
- **IPComp (Compresión IP)**
  IPComp reduce el tamaño de los datagramas comprimiéndolos para aumentar el rendimiento de la comunicación entre ambos socios VPN.
- **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.

Protocolos IPSec (IP Security)

IPSec proporciona una base estable y duradera para proporcionar seguridad de capa de red. 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 implementar 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 implementación 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.

Los principales protocolos IPSec se listan a continuación:

- **Protocolo de cabecera de autenticación (AH)**
- **Protocolo de carga útil de seguridad encapsulada (ESP)**
- **Protocolo de AH y ESP combinado**
- **Protocolo de intercambio de claves de Internet (IKE)**

IETF (Internet Engineering Task Force) define formalmente IPSec en RFC (Request for Comment) 2401, *Security Architecture for the Internet Protocol*. Puede visualizar esta RFC en Internet, en el siguiente sitio Web: 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) 2402, *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, por otra parte, no autentica la parte inicial de la cabecera IP o cualquier otra información que preceda a la cabecera ESP.

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

¿Qué algoritmos utiliza AH para proteger la información?
AH utiliza algoritmos conocidos como **HMAC (códigos de autenticación de mensajes con valores hash)**. De forma específica, VPN utiliza tanto HMAC-MD5 como HMAC-SHA. Tanto MD5 como SHA utilizan datos de entrada de longitud variable y una clave secreta para generar datos de salida de longitud fija (llamado valor hash). Si los valores hash de dos mensajes coinciden es muy probable que los mensajes sean idénticos. MD5 y SHA codifican la longitud del mensaje en la salida, aunque SHA está considerado como más seguro porque produce unos hash más grandes.

IETF (Internet Engineering Task Force IETF) define formalmente HMAC-MD5 en la RFC (Request for Comments) 2085, *HMAC-MD5 IP Authentication with Replay Prevention*. IETF (Internet Engineering Task Force IETF) define formalmente HMAC-SHA en la RFC (Request for Comments) 2404, *The use of HMAC-SHA-1-96 within ESP and AH*. Puede revisar estas RFC en Internet, en el siguiente sitio Web: 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 opcionaleses 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 mayor parte de casos, los sistemas principales 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. OS/400 VPN utiliza DES (estándar de cifrado de datos), triple DES (3DES), RC5, RC4 o AES (estándar de cifrado avanzado) para el cifrado.

IETF (Internet Engineering Task Force) define formalmente DES en RFC (Request for Comment) 1829, *The ESP DES-CBC Transform*. IETF (Internet Engineering Task Force) define formalmente 3DES en RFC 1851, *The ESP Triple DES Transform*. Puede consultar estas RFC y otras en Internet, en la siguiente dirección Web: http://www.rfc-editor.org

.

ESP utiliza los algoritmos HMAC-MD5 y HMAC-SHA para ofrecer funciones de autenticación. Tanto MD5 como SHA utilizan datos de entrada de longitud variable y una clave secreta para generar datos de salida de longitud fija (llamado valor hash). Si los valores hash de dos mensajes coinciden es muy probable que los mensajes sean idénticos. MD5 y SHA codifican la longitud del mensaje en la salida, aunque SHA está considerado como más seguro porque produce unos hash más grandes.

IETF (Internet Engineering Task Force IETF) define formalmente HMAC-MD5 en la RFC (Request for Comments) 2085, *HMAC-MD5 IP Authentication with Replay Prevention*. IETF (Internet Engineering Task Force IETF) define formalmente HMAC-SHA en la RFC (Request for Comments) 2404, *The Use of HMAC-SHA-1-96 within ESP and AH*. Puede consultar estas RFC y otras en Internet, en la siguiente dirección Web: http://www.rfc-editor.org

.

AH y ESP combinados
VPN permite combinar AH y ESP para conexiones de sistema principal a sistema principal 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.

Gestión de claves
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 IKE (intercambio de claves de Internet). 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 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 trataría 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 de Digital Certificate Manager (5722-SS1 Opción 34). Además, algunas soluciones de VPN necesitan la firma RSA para interaccionar. Por ejemplo, Windows 2000 VPN utiliza la firma RSA como el método de autenticación por omisión. Finalmente, la firma RSA proporciona más escalabilidad que las claves precompartidas. Los certificados que utilice deben provenir de autoridades certificadoras en las que confíen ambos servidores de claves.

Fase 2
La fase 2, por otro lado, 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 iSeries Navigator, 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):

- 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)*

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

.

Layer 2 Tunnel Protocol (L2TP)

Las conexiones L2TP (Layer 2 Tunneling Protocol), 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 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 ISP.

Con un **túnel obligatorio** L2TP, un sistema principal remoto inicia la conexión con su ISP (suministrador de servicios de Internet). 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 , típicamente 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 iSeries de una sucursal bancaria para que se conecte con la red de empresa mediante una pasarela iSeries con un túnel L2TP protegido por VPN.

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).

Conversión de direcciones de red para VPN

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 sistemas principales de su red acceder a los servicios y sistemas principales 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. NAT VPN 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 NAT VPN actualmente.

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

NAT VPN para evitar conflictos entre direcciones IP
Este tipo de NAT VPN 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 NAT VPN depende de si su servidor es el iniciador o el contestador de la conexión VPN. Cuando su servidor es el iniciador de la conexión, puede convertir las direcciones locales en direcciones compatibles con la dirección de la conexión VPN asociada. Cuando su servidor 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.

NAT VPN para ocultar direcciones locales
Este tipo de NAT VPN 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 NAT VPN, 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. NAT VPN para direcciones locales precisa que su servidor actúe como contestador de las conexiones.

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

1. ¿Tiene uno o varios servidores 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 NAT VPN para ocultar direcciones locales en el iSeries.

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

IPSec compatible con NAT

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 debe pasar todas las demás validaciones.

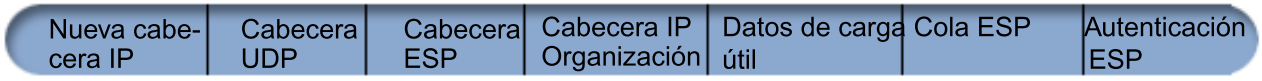
Sólo puede aplicar la encapsulación UDP a las VPN que vayan a utilizar IPSec ESP en modalidad de túnel o en modalidad de transporte. Además, en V5R2, iSeries sólo puede actuar como cliente de una encapsulación UDP. Es decir, sólo puede *iniciar* tráfico encapsulado UDP.

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:

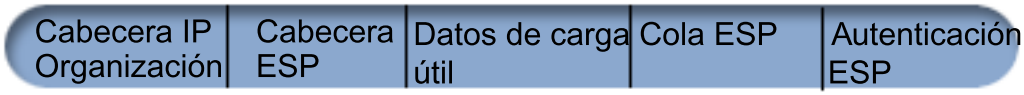
Después de aplicar la encapsulación UDP:



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 iSeries lo envía a su VPN asociada a través del puerto UDP 500. Recuerde que las VPN asociadas ya realizan las negociaciones IKE a través del puerto UDP 500. Al enviar el tráfico encapsulado UDP a través del mismo puerto, las dos VPN asociadas no necesitarán abrir puertos adicionales a través de sus cortafuegos ni escribir normas de paquetes para permitir el tráfico a través de la conexión. El terminal receptor de la conexión puede determinar si el paquete es un paquete IKE o un paquete encapsulado UDP debido a que los 8 primeros bytes de la carga útil de UDP se establecen en cero en un paquete encapsulado UDP. Ambos terminales de la conexión deben soportar la encapsulación UDP para que ésta funcione adecuadamente.

Compresión IP (IPComp)

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

.

VPN y filtrado IP

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.

A partir del release V5R1 del sistema operativo, VPN puede generar estas normas automáticamente. Siempre que sea posible, debe permitir 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 iSeries Navigator.

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:

- **Migrar filtros de políticas al release actual**
  En los releases V4R4 y V4R5 del sistema operativo, debía configurar las normas de paquetes VPN como un paso independiente. No se configuraban automáticamente como parte de las configuraciones VPN. Este tema detalla consideraciones especiales que deben tenerse en cuenta al migrar filtros de políticas de V4R4 y V4R5 al release actual e indica cómo hacerlo.
- **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. Este tema describe las razones por las que esto puede ser deseable e indica cómo llevarlo a cabo.

- **IKE implícito**
  Para que se produzcan negociaciones 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. Lea este tema para obtener más información acerca de este funcionamiento en iSeries.

Migrar filtros de política al release actual

En los releases V4R4 y V4R5 del sistema operativo, debía configurar las normas de paquetes VPN como un paso independiente de la interfaz Normas de paquetes de iSeries Navigator. No se configuraban automáticamente como parte de las configuraciones VPN. A partir del release V5R1 del sistema operativo, la GUI de VPN puede crear estas normas de paquetes automáticamente.

Hay varios elementos que debe tener en cuenta si ha creado normas de filtrado de políticas (normas en las que action=IPSec) en V4R4 o V4R5 y desea utilizar las mismas normas en el release actual. O puede que VPN *genere* las normas de filtrado de políticas del usuario, pero que éste necesite añadir normas adicionales que permitan otro tráfico IP, por ejemplo telnet, a través de la conexión. Siga estas recomendaciones que le ayudarán a evitar posibles errores de configuración.

Para clarificar: en este tema, las referencias al archivo de normas del *cliente* aluden a cualquier archivo de normas que haya creado mediante el editor de normas de paquete de iSeries Navigator. Compare éste con el archivo de normas *VPNPOLICYFILTERS*, que es el archivo de normas que VPN genera automáticamente como parte de las configuraciones VPN.

- Si tiene conexiones VPN de V4R4 o V4R5 y no tiene previsto configurar otras conexiones VPN en el release actual, puede activar sus normas de filtrado e iniciar las conexiones, como de costumbre.
- 

  Si tiene conexiones VPN de V4R4 o V4R5 y tiene previsto configurar nuevas conexiones en el release actual, debe utilizar el asistente **Migrar filtros de políticas**. El asistente elimina los filtros de políticas de los archivos de normas de paquetes que ha creado e inserta filtros de políticas equivalentes en VPNPOLICYFILTERS.I3P, generado por VPN. Para acceder al asistente, siga estos pasos:
  1. En iSeries Navigator, expanda el servidor **—>Red —>Políticas IP**.
  2. Pulse con el botón derecho del ratón **VPN (red privada virtual)** y seleccione **Migrar filtros de políticas**.
  3. Cuando haya completado el asistente, pulse **Finalizar**.
  4. Pulse **Ayuda** si tiene preguntas acerca de cómo cumplimentar una página o alguno de los campos.

  
- Si VPN ha generado sus normas de filtrado de políticas, pero necesita añadir algunas normas que no son de filtro VPN, debe configurar estas normas mediante el editor de normas de paquetes de iSeries Navigator. Si alguna de esas normas que no son de filtro VPN necesitan preceder a los filtros VPN, sus nombres de conjunto deben empezar por `PREIPSEC`. Por ejemplo, `PREIPSECMYRULES`. Esto ayuda al sistema a determinar el orden en el que debe procesar las normas de filtro. Los nombres de conjunto de todas las normas que no son VPN no deben tener el prefijo `PREIPSEC`. Por ejemplo, `MORERULES`.
- Debe permitir siempre que VPN cree las normas de filtro de políticas del usuario. Sin embargo, las normas VPN que no son de filtro deben permanecer en el archivo de normas del cliente. Recuerde que si alguno de estos filtros que no son VPN debe preceder a los filtros de políticas en el archivo de normas VPNPOLICYFILTERS.I3P, necesitará añadir el prefijo `PREIPSEC` al nombre del conjunto. De esta forma, se asegura de que las normas del cliente y las VPN funcionan conjuntamente de la forma que desea. Por ejemplo, VPN ha generado las normas de filtro de políticas (conjuntos VPN), pero el usuario ha añadido normas adicionales (conjuntos de usuario) para permitir otro tráfico IP a través de la conexión. Al cargar las normas en el sistema, éstas se ordenarán de la forma siguiente:

1. Conjuntos de usuario cuyos nombres empiecen por PREIPSEC
2. Conjuntos VPN cuyos nombres empiezan por PREIPSEC
3. Conjuntos VPN con ACTION=IPSEC (filtros de políticas)
4. Conjuntos de usuario con ACTION=IPSEC (filtros de políticas)
5. Conjuntos de usuario de cualquier otro tipo
6. Conjuntos VPN de cualquier otro tipo

Compruebe el archivo EXPANDED.OUT para visualizar el orden del archivo de salida fusionado. EXPANDED.OUT se escribe en el directorio donde se ubica el archivo de normas del cliente.

- 

  Mediante iSeries Navigator, puede elegir activar:
  - sólo el archivo de normas generadas por VPN, VPNPOLICYFILTERS.I3P
  - sólo el archivo de normas de cliente
  - tanto el archivo de normas generadas por VPN como el archivo de normas de cliente

- Active las normas de filtrado en todas las interfaces, en lugar de hacerlo en cada interfaz por separado. De esta forma, tendrá la garantía de que los filtros se activarán y que se establecerá el orden correcto de los filtros de políticas.
- Debe siempre verificar las normas de filtrado antes de intentar activarlas. Si la verificación se realiza sin errores, compruebe entonces el archivo EXPANDED.OUT para asegurar que están ordenadas de la forma que desea. Tras haber completado este paso, puede activar las normas.

Conexiones VPN sin filtros de políticas

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 paquete 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 servidor 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 establecer una conexión, la mayoría de las VPN requieren que se produzcan negociaciones IKE (Intercambio de claves de Internet) 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.

Planificar VPN

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**
  Antes de empezar, asegúrese de que cumple los requisitos mínimos para crear una VPN.
- **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. Este tema describe los diversos tipos de conexión que puede configurar.
- **Utilizar el asesor de planificación de VPN**
  El asesor de planificación le hará preguntas sobre la red y, basándose en sus respuestas, le hará recomendaciones para crear la VPN.
  Nota: utilice el asesor de planificación VPN sólo para conexiones que soporten el protocolo IKE (intercambio de claves de Internet). Utilice la hoja de planificación de conexiones manuales para sus tipos de conexión manual.
- **Completar las hojas de trabajo de planificación 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.

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

Requisitos de configuración de VPN

Para que funcione correctamente en iSeries y con clientes de red, asegúrese de que el iSeries y el PC cliente cumplen los siguientes requisitos:

Requisitos de iSeries en V5R2

- OS/400, Versión 5 Release 2 (5722-SS1), o posterior
- Digital Certificate Manager (5722-SS1 Opción 34)
- Cryptographic Access Provider (5722-AC2 o AC3)
- iSeries Access para Windows(5722-XE1) e iSeries Navigator
  - Componente de red de iSeries Navigator
- 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 sistema principal local y el nombre de dominio local deben estar configurados

Requisitos del cliente

- Una estación de trabajo con un sistema operativo Windows de 32 bits conectado correctamente al iSeries y configurado para TCP/IP
- Una unidad de proceso a 233 Mhz
- 32 MB de RAM para clientes Windows 95/98
- 64 MB de RAM para clientes Windows NT y 2000
- iSeries Access para Windows e iSeries Navigator instalados en el PC cliente
- Software que soporte el protocolo IPSec (IP Security)
- Software que soporte L2TP, si los usuarios remotos utilizarán L2TP para establecer una conexión con su sistema

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, si los puntos finales de *conexión* son 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). Por otra parte, 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 sistema principal.

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 sistema principal
IPSec protege el tráfico de datos mientras circula entre la pasarelay un sistema principal en una red remota. VPN no protege el tráfico de datos en la red local porque se considera de confianza.

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

De sistema principal a sistema principal
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 sistema principal de la red local y un sistema principal de la red remota. Este tipo de VPN proporciona protección IPSec de extremo a extremo.

Completar las hojas de trabajo de planificación VPN

Utilice las hojas de trabajo de planificación para recopilar información detallada sobre sus proyectos de utilización de la VPN VPN. Necesitará esta información para planificar su estrategia VPN de forma adecuada. También puede utilizar esta información para configurar la VPN. Seleccione la hoja de trabajo del tipo de conexión que desea crear.

- **Hoja de trabajo de planificación para conexiones dinámicas**
  Complete esta hoja de trabajo para configurar una conexión dinámica.
- **Hoja de trabajo de planificación para conexiones manuales**
  Complete esta hoja de trabajo para configurar una conexión manual.

- **Asesor de configuración de VPN**
  O, si lo prefiere, utilice el asesor que le ofrecerá una planificación interactiva y una guía para la configuración. El asesor de planificación le realizará preguntas sobre la red y, basándose en sus respuestas, le hará recomendaciones para crear la VPN.

  Nota: Utilice el asesor de planificación VPN sólo para conexiones dinámicas. Utilice la hoja de planificación de conexiones manuales para sus tipos de conexión manual.

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

Hoja de trabajo de planificación para conexiones dinámicas

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**.

Debe responder a cada pregunta antes de proceder con la configuración de la VPN.

Lista de comprobación de los prerrequisitos	**Respuestas**
¿Su OS/400 es V5R2 (5722-SS1) o posterior?	
¿Se encuentra instalada la opción de Digital Certificate Manager (5722-SS1 Opción 34)?	
¿Está instalado Cryptographic Access Provider (5722-AC2 o AC3)?	
¿Está instalado iSeries Access (5722-XE1)?	
¿Está instalado iSeries Navigator?	
¿Está instalado el subcomponente de red de iSeries Navigator?	
¿Está instalado TCP/IP Connectivity Utilities para OS/400 (5722-TC1)?	
¿Ha establecido en 1 el valor del sistema de retener datos de seguridad del servidor(QRETSVRSEC *SEC)?	
¿Está configurado TCP/IP en el iSeries (incluyendo las interfaces IP, rutas IP, el nombre del sistema principal 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 implementan el filtrado de paquetes IP, ¿soportan las normas de filtrado del cortafuegos o direccionador los protocolos AH y ESP?	
¿Están configurados los cortafuegos o los direccionadores para permitir los protocolos IKE (UDP puerto 500), AH y ESP?	
¿Están configurados los cortafuegos para habilitar el reenvío de IP?	

Necesita esta información para configurar una conexión VPN dinámica	**Respuestas**
¿Qué tipo de conexión está creando? • De pasarela a pasarela • De sistema principal a pasarela • De pasarela a sistema principal • De sistema principal a sistema principal	

¿Cómo se denominará el grupo de claves dinámicas?	
¿Qué tipo de seguridad y rendimiento del sistema necesita para proteger las claves? • Máxima seguridad, mínimo rendimiento • Equilibrar seguridad y rendimiento • 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 punto final de datos local?	
¿Cuál es el identificador del servidor de claves remoto?	
¿Cuál es el identificador del punto final de datos remoto?	
¿Qué tipo de seguridad y rendimiento del sistema necesita para proteger sus datos? • Máxima seguridad, mínimo rendimiento • Equilibrar seguridad y rendimiento • Mínima seguridad y máximo rendimiento	

Hoja de trabajo de planificación para conexiones manuales

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.

Debe responder a cada una de las siguientes preguntas antes de proseguir con la configuración de su VPN:

Lista de comprobación de los prerrequisitos	**Respuestas**
¿Su OS/400 es V5R2 (5722-SS1) o posterior?	
¿Se encuentra instalada la opción de Digital Certificate Manager (5722-SS1 Opción 34)?	
¿Está instalado Cryptographic Access Provider (5722-AC2 o AC3)?	
¿Está instalado iSeries Access (5722-XE1)?	
¿Está instalado iSeries Navigator?	
¿Está instalado el subcomponente de red de iSeries Navigator?	
¿Está instalado TCP/IP Connectivity Utilities para OS/400 (5722-TC1)?	
¿Ha establecido en 1 el valor del sistema de retener datos de seguridad del servidor(QRETSVRSEC *SEC)?	
¿Está configurado TCP/IP en el iSeries (incluyendo las interfaces IP, rutas IP, el nombre del sistema principal 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 implementan el filtrado de paquetes IP, ¿soportan las normas de filtrado 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?	

Necesita esta información para configurar una VPN manual	Respuestas
¿Qué tipo de conexión está creando? • De sistema principal a pasarela • De sistema principal a sistema principal • De pasarela a sistema principal • 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?	
¿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)? **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. 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. 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. 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. 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. El SPI entrante debe coincidir exactamente con el SPI saliente del servidor remoto.	

Necesita esta información para configurar una VPN manual	Respuestas
¿Cuál es el SPI saliente? El SPI saliente es una serie de caracteres hexadecimales de 4 bytes. El SPI saliente debe coincidir exactamente con el SPI entrante del servidor remoto.	

Configurar VPN

La interfaz de VPN le ofrece varias formas distintas de configurar las conexiones VPN. Siga leyendo para decidir qué tipo de conexión va a configurar y cómo va a hacerlo.

¿Qué tipo de conexión debo configurar?
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 (Consulte 39)** 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.

¿Cómo se configura una conexión dinámica VPN?
VPN es en realidad un grupo de objetos de configuración que definen las características de una conexión. Una conexión VPN dinámica necesita que cada uno de estos objetos funcione correctamente. Siga los enlaces que figuran a continuación para obtener información específica sobre cómo configurar cada uno de los objetos de configuración de VPN:

> **Consejo:**
> **Configure las conexiones con el asistente Nueva conexión**
> Por lo general, utilizará el asistente Conexión para crear todas las conexiones dinámicas. El asistente crea automáticamente cada uno de los objetos de configuración que VPN necesita para funcionar correctamente, incluyendo las normas de paquete. Si especifica que el asistente deberá activar las normas de paquetes VPN, puede saltar al paso 6 que se encuentra a continuación, *Iniciar la conexión*. En caso contrario, después de que el asistente haya terminado de configurar la VPN, debe activar las normas de paquetes y, a continuación, puede iniciar la conexión.

Si decide no utilizar el asistente para configurar las conexiones dinámicas VPN, siga estos pasos para completar la configuración:

1. **Configurar las políticas de seguridad VPN**
   Debe definir políticas de seguridad VPN para todas las conexiones dinámicas. La política IKE y la política de datos estipulan cómo IKE protege las negociaciones de fase 1 y fase 2.
2. **Configurar conexiones seguras**
   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, mientras que la **conexión de claves dinámicas** define las características de las conexiones de datos individuales entre pares de puntos finales. La conexión de claves dinámicas existe dentro del grupo de claves dinámicas.

   Nota: sólo necesita completar los siguientes dos pasos, *Configurar las normas de paquete* y *Definir una interfaz para las normas*, si selecciona la opción **La norma de filtrado de políticas se definirá**

en las normas de paquete en la página **Grupo de claves dinámicas - Conexiones** en la interfaz VPN. De lo contrario, estas normas se crearán como parte de las configuraciones VPN y se aplicarán a la interfaz que especifique.

Es aconsejable permitir siempre que la interfaz VPN cree sus normas de filtro de políticas. Llévelo a cabo seleccionando la opción **Generar el siguiente filtro de políticas para este grupo** en la página **Grupo de claves dinámicas - Conexiones**.

3. **Configurar las normas de paquete**
   Tras haber completado la configuración de VPN, deberá crear y aplicar las normas de filtrado que permiten al tráfico de datos fluir por la conexión. Las normas VPN **anteriores a IPSec** permiten todo el tráfico IKE en las interfaces especificadas, de forma que IKE pueda negociar las conexiones. La norma de **filtro de políticas** define qué direcciones, protocolos y puertos puede utilizar el nuevo grupo de claves dinámicas asociado.

   Si migra desde V4R4 o V4R5 y tiene conexiones VPN y filtros de políticas que desea seguir utilizando con el release actual, debe consultar el tema *Migrar filtros de políticas al release actual* para asegurarse de que los filtros de políticas antiguos y los nuevos funcionarán conjuntamente como tiene previsto.
4. **Definir una interfaz para las normas**
   Después de configurar las normas de paquetes y cualquier otra norma que necesite para habilitar la conexión VPN, debe definir una interfaz a la que aplicarlas.
5. **Activar las normas de paquete**
   Después de definir una interfaz para las normas de paquete, debe activarlas para poder iniciar la conexión.
6. **Iniciar la conexión**
   Complete esta tarea para iniciar las conexiones.

¿Cómo se configura una conexión VPN manual?

Tal como sugiere el nombre, una conexión manual es una conexión en la que deben configurarse a mano todas las propiedades de VPN, incluyendo las claves de entrada y salida. Siga los enlaces que figuran a continuación para obtener información específica sobre cómo configurar una conexión manual:

1. **Configurar conexiones manuales**
   Las conexiones manuales definen las características de una conexión, incluyendo los protocolos de seguridad y los puntos finales de conexión y de datos.

   Nota: sólo necesita completar los siguientes dos pasos, *Configurar la norma de filtro de políticas* y *Definir una interfaz para las normas*, si selecciona la opción **La norma de filtrado de políticas se definirá en las normas de paquete** en la página **Conexión manual - Conexión** en la interfaz VPN. De lo contrario, estas normas se crearán como parte de las configuraciones VPN.

   Es aconsejable permitir siempre que la interfaz VPN cree sus normas de filtro de políticas. Para ello seleccione la opción **Generar un filtro de políticas que coincida con los puntos finales de datos** en la página **Conexión manual - Conexión**.
2. **Configurar la norma de filtro de políticas**
   Tras haber completado la configuración de atributos de la conexión manual, deberá crear y aplicar la norma de filtro de políticas que permita al tráfico de datos fluir por la conexión. La norma de **filtro de políticas** define qué direcciones, protocolos y puertos puede utilizar la conexión asociada.
3. **Definir una interfaz para las normas**
   Después de configurar las normas de paquetes y cualquier otra norma que necesite para habilitar la conexión VPN, debe definir una interfaz a la que aplicarlas.
4. **Activar las normas de paquete**
   Después de definir una interfaz para las normas de paquete, debe activarlas para poder iniciar la conexión.
5. **Iniciar la conexión**
   Complete esta tarea para iniciar las conexiones que se inician localmente.

Configurar las conexiones VPN con el asistente Nueva conexión

El asistente Nueva conexión permite crear una red privada virtual (VPN) entre cualquier combinación de sistemas principales y pasarelas. Por ejemplo, de sistema principal a sistema principal, de pasarela a sistema principal, de sistema principal 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 paquete. Sin embargo, si necesita añadir más funciones a la VPN, como por ejemplo, registrar por diario o convertir direcciones de red para VPN (NAT VPN), 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**.

Complete el Asesor de planificación VPN antes de empezar. El asesor le ofrece una forma de reunir información importante que necesitará para crear la VPN.

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

1. En iSeries Navigator, expanda el servidor **—> Red—> Políticas IP**.
2. Pulse con el botón derecho del ratón **Red privada virtual** y seleccione **Nueva conexión** para iniciar el asistente.
3. Siga los pasos del asistente para crear una conexión VPN básica. Pulse el botón **Ayuda** si la necesita.

Configurar las políticas de seguridad VPN

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

- **Configurar una política IKE (intercambio de claves de Internet)**
  La política 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.
- **Configurar 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.

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

Configurar una política IKE (intercambio de claves de Internet)

Una política IKE define qué nivel de autenticación o 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. VPN utiliza tanto la modalidad de firma RSA como las 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 (5722-SS1 Opción 34). 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 iSeries Navigator, expanda el servidor **—> Red—> Políticas IP—> Red privada virtual—> 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 **Políticas IKE (intercambio de claves de Internet)** en el panel izquierdo y después pulse con el botón derecho del ratón la política que desee cambiar en el panel derecho 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.

Configurar 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).

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

1. En iSeries Navigator, expanda el servidor **—> Red—> Políticas IP—> Red privada virtual—> 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 **Políticas de datos** (en el panel izquierdo) y después pulse con el botón derecho del ratón la política de datos que desea cambiar (en el panel derecho) 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.

Configurar la 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 deben utilizarse, necesita crear conexiones de claves dinámicas individuales para las conexiones que inicie localmente.

Para configurar el objeto de conexión segura, complete estas tareas:

Parte 1: Configurar un grupo de claves dinámicas:

1. En iSeries Navigator, expanda el servidor **—> Red—> Políticas IP—> Red privada virtual—> Conexiones de seguridad**.
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 iSeries Navigator, expanda el servidor **—> Red —> Políticas IP—> Red privada virtual—> Conexiones de seguridad-> Por grupo**.
2. En el panel izquierdo de la ventana de iSeries Navigator, pulse con el botón derecho del ratón el grupo de claves dinámicas que ha creado en la parte 1 y seleccione **Nueva conexión 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.

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

Nota: en la mayor parte de casos, deberá permitir 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 paquete VPN mediante el editor de normas de paquete y, a continuación, activarlas.

Configurar una conexión manual

Tal como sugiere el nombre, una conexión manual es una conexión en la que deben configurarse a mano todas las propiedades de VPN. 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 iSeries Navigator, expanda el servidor **—> Red—> Políticas IP—> Red privada virtual—> Conexiones de seguridad**.
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 mayor parte de casos, deberá permitir 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.

Configurar normas de paquetes VPN

Si está creando una conexión por primera vez, debe permitir 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 iSeries Navigator, deberá crear 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 iSeries Navigator. 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.

- **Normas anteriores 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.
- **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 filtrado a una interfaz, el sistema añade automáticamente una norma DENY por omisión 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 filtrado apropiadas, debe definir la interfaz a la que se aplicarán y, a continuación, activarlas.

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

Si las normas de filtrado no permiten el tráfico de iSeries Navigator, iSeries Navigator no podrá comunicarse con el iSeries. Si se encuentra en esta situación, necesitará conectarse al iSeries 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.

Configurar la norma de filtro anterior a IPSec
Atención: 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 filtrado; 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 iSeries Navigator, expanda el servidor **—> Red—> Políticas IP**.

2. Pulse con el botón derecho del ratón **Normas de paquetes** y seleccione **Editor de normas**. De esta forma se visualizará el editor Normas de paquete, que le permitirá crear o editar normas NAT y de filtro para el iSeries.
3. En el diálogo de Bienvenida, seleccione **Crear un nuevo archivo de normas de paquete** y pulse **Aceptar**.
4. En el editor Normas de paquete, seleccione **Insertar —> Filtro**.
5. En la página **General**, especifique un nombre de conjunto para las normas de filtrado VPN. Le recomendamos que cree al menos tres conjuntos distintos: uno para las normas de filtrado anteriores a IPSec, uno para las normas de filtrado de políticas y otra para las normas de filtrado DENY y PERMIT misceláneas. El conjunto que contiene las normas de filtro anteriores a IPSec deben llevar el prefijo *preipsec*. Por ejemplo, preipsecfilters.
6. En el campo **Acción**, seleccione **PERMIT** en la lista desplegable.
7. En el campo **Acción**, seleccione **OUTBOUND** en la lista desplegable.
8. 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.
9. 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.
10. En la página **Servicios**, seleccione **Servicio**. De esta forma se habilitan los campos **Protocolo**, **Puerto origen** y **Puerto destino**.
11. En el campo **Protocolo**, seleccione **UDP** en la lista desplegable.
12. Para **Puerto origen**, seleccione **=** en el primer campo y, a continuación especifique `500` en el segundo campo.
13. Repita el paso anterior para **Puerto destino**.
14. Pulse **Aceptar**.
15. 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.

Configurar una norma de filtro de políticas

Atención: sólo debe realizar esta tarea si ha especificado que no desea que VPN genere la norma 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 cuarto paso.

1. En iSeries Navigator, expanda el servidor **—> Red—> Políticas IP**.
2. Pulse con el botón derecho del ratón **Normas de paquetes** y seleccione **Editor de normas**. De esta forma se visualizará el editor Normas de paquete, que le permitirá crear o editar normas NAT y de filtro para el iSeries.
3. En el diálogo de Bienvenida, seleccione **Crear un nuevo archivo de normas de paquete** y pulse **Aceptar**.

4. En el editor Normas de paquete, seleccione **Insertar —> Filtro**.
5. En la página **General**, especifique un nombre de conjunto para las normas de filtrado VPN. Le recomendamos que cree al menos tres conjuntos distintos: uno para las normas de filtrado anteriores a IPSec, uno para las normas de filtrado de políticas y otra para las normas de filtrado DENY y PERMIT misceláneas. Por ejemplo, `policyfilters`.
6. En el campo **Acción**, seleccione **IPSEC** en la lista desplegable. El campo **Dirección** toma OUTBOUND por omisión y no puede cambiarlo. A pesar de que este campo toma OUTBOUND por omisión, en realidad es bidireccional. El valor OUTBOUND aparece para clarificar la semántica de los valores de entrada. Por ejemplo, los valores origen son valores locales y los valores destino son valores remotos.
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 **Nombre de la conexión**, seleccione la definición de conexión a la que se aplican estas normas de filtrado.
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 filtrado.

Nota: al añadir normas de filtrado para una interfaz, el sistema añade automáticamente una norma DENY por omisión 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.

Definir 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 filtrado 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 iSeries Navigator, expanda el servidor **—> Red—> Políticas IP**.
2. Pulse con el botón derecho del ratón **Normas de paquetes** y seleccione **Editor de normas**. De esta forma se visualizará el editor Normas de paquete, que le permitirá crear o editar normas NAT y de filtro para el iSeries.
3. En el diálogo de Bienvenida, seleccione **Crear un nuevo archivo de normas de paquete** y pulse **Aceptar**.
4. En el editor Normas 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 de iSeries 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 paquete, el mandato suprimirá todos los archivos que se encuentren dentro de este directorio.

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

Activar 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 iSeries Navigator, expanda el servidor **—> Red—> Políticas IP**.
2. Pulse con el botón derecho del ratón **Normas de paquetes** y seleccione **Activar**. De esta forma, se abrirá el diálogo Activar normas de paquetes.
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 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. Para obtener información acerca de los mensajes asociados con un número de línea y archivo específico, puede pulsar el error con el botón derecho del ratón y seleccionar **Ir a línea** para resaltar el error en el archivo.

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

Iniciar una conexión VPN

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

1. En iSeries Navigator, expanda el servidor **—> Red—> Políticas IP**.
2. Si el servidor VPN no está iniciado, pulse con el botón derecho del ratón **Red privada virtual** y seleccione **Iniciar**. De esta forma, se iniciará el servidor VPN.
3. Asegúrese de que las normas de paquetes están activadas.
4. Expanda **Red privada virtual—> Conexiones de seguridad**.
5. Pulse **Todas las conexiones** para visualizar una lista de conexiones en el panel derecho.
6. 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**.

Gestionar VPN

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

- **Iniciar una conexión VPN**
  Complete esta tarea para iniciar las conexiones que se inician localmente.
- **Establecer los atributos por omisión de las conexiones**
  Los valores por omisión se rellenan los paneles que utilizará para crear nuevas políticas y conexiones. Puede establecer los valores por omisión 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.
- **Restablecer las conexiones en estado de error**
  El restablecimiento de las conexiones con errores las devuelve al estado de desocupado.
- **Visualizar la información de errores**
  Complete esta tarea que le ayudará a determinar por qué la conexión da error.
- **Visualizar los atributos de las conexiones activas**
  Complete esta tarea para comprobar el estado y otros atributos de las conexiones activas.
- **Utilizar el rastreo del servidor VPN**
  El servidor VPN permite configurar, iniciar, detener y visualizar el gestor de conexiones VPN y los rastreos del servidor del gestor de claves VPN. Esto es parecido a utilizar el mandato TRCTCPAPP *VPN desde la pantalla verde, excepto que el rastreo se puede ver mientras la conexión está activa.
- **Visualizar 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.
- **Detener conexiones**
  Complete esta tarea para detener las conexiones activas.
- **Visualizar los atributos de las SA (asociaciones de seguridad)**
  Complete esta tarea para visualizar los atributos de las SA (asociaciones de seguridad) que están asociadas con una conexión habilitada.
- **Suprimir objetos de configuración de VPN**
  Antes de suprimir una conexión VPN debe conocer el efecto de la conexión sobre otras conexiones VPN y grupos de conexiones.

Establecer los atributos por omisión de las conexiones

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

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

1. En iSeries Navigator, expanda el servidor **—>Red —>Políticas IP**.
2. Pulse con el botón derecho del ratón **VPN (red privada virtual)** y seleccione **Valores por omisión**.

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.

Restablecer conexiones en estado de error

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

1. En iSeries Navigator, expanda el servidor **—> Red—> Políticas IP—> Red privada virtual—> Conexiones de seguridad**
2. Pulse **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 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**.

Visualizar la información de errores

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

1. En iSeries Navigator, expanda el servidor **—> Red—> Políticas IP—> Red privada virtual—> Conexiones de seguridad**
2. Pulse **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**.

Visualizar los atributos de las conexiones activas

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

1. En iSeries Navigator, expanda el servidor **—> Red—> Políticas IP—> Red privada virtual—> Conexiones de seguridad**
2. Pulse **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 **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 iSeries Navigator. Por omisión, los únicos atributos que se visualizarán son Estado, Descripción y Tipo de conexión. Puede modificar qué datos se visualizarán siguiendo estos pasos:

1. En iSeries Navigator, expanda el servidor **—> Red—> Políticas IP—> Red privada virtual—> Conexiones de seguridad**
2. Pulse **Todas las conexiones** para visualizar una lista de conexiones en el panel derecho.
3. Desde el menú **Objetos**, seleccione **Columnas**. De esta forma, se abrirá un diálogo que le permite seleccionar qué atributos desea visualizar en la ventana de iSeries Navigator.

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.

Utilizar el rastreo del servidor VPN

Para ver el rastreo del servidor VPN, siga estos pasos:

1. En iSeries Navigator, expanda el servidor **—> Red—> Políticas IP**.
2. Pulse con el botón derecho del ratón **Red privada virtual**, seleccione **Herramientas de diagnóstico** y, a continuación, **Rastreo del servidor**.

Para especificar qué tipo de rastreo deben generar el gestor de claves de VPN y el gestor de conexiones de VPN, siga estos pasos:

1. En la ventana **Rastreo de VPN (red privada virtual)**, pulse

   (Opciones).
2. En la página **Gestor de conexiones**, especifique qué tipo de rastreo debe ejecutar el servidor del gestor de conexiones.
3. En la página **Gestor de claves**, especifique qué tipo de rastreo debe ejecutar el servidor del gestor de claves.
4. Pulse **Ayuda** si tiene preguntas acerca de cómo cumplimentar una página o alguno de los campos.
5. Pulse **Aceptar** para guardar los cambios.
6. Pulse

   (Inicio) para iniciar el rastreo.Pulse

   (Renovar) periódicamente para ver la información de rastreo más reciente.

Visualizar las anotaciones de trabajo del servidor 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 iSeries Navigator, expanda el servidor **—> Red—> Políticas IP**.
2. Pulse con el botón derecho del ratón **VPN (red privada virtual)**, seleccione **Herramientas de diagnóstico** y seleccione las anotaciones de trabajo del servidor que desee ver.

Visualizar los atributos de las SA (asociaciones de seguridad)

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

1. En iSeries Navigator, expanda el servidor **—> Red—> Políticas IP—> Red privada virtual—> Conexiones de seguridad**
2. Pulse **Todas las conexiones** 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** La ventana resultante permite ver las propiedades de cada una de las SA asociadas a una conexión específica.

Detener una conexión VPN

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

1. En iSeries Navigator, expanda el servidor **—> Red—> Políticas IP—> Red privada virtual—> Conexiones de seguridad**
2. Pulse **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**.

Suprimir objetos de configuración de VPN

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

1. En iSeries Navigator, expanda el servidor **—> Red—> Políticas IP—> Red privada virtual—> Conexiones de seguridad**

2. Pulse **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

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:

- **Cómo empezar a solucionar los problemas de VPN**
  Diríjase aquí para empezar a encontrar y corregir sus problemas de conexión VPN.
- **Errores de configuración habituales de VPN y cómo solucionarlos**
  Este tema identifica los errores de usuario más habituales y ofrece posible soluciones.
- **Resolución de problemas de VPN con el diario QIPFILTER**
  Este tema ofrece información sobre las normas de filtrado VPN.
- **Resolución de problemas de VPN con el diario QVPN**
  Este tema ofrece información sobre las conexiones y el tráfico IP.
- **Resolución de problemas de VPN con las las anotaciones de trabajo de VPN**
  En este tema se describen las distintas anotaciones de trabajo que utiliza VPN.
- R**esolución de problemas de VPN con el rastreo de comunicaciones de OS/400**
  En este tema se describe cómo rastrear los datos de una línea de comunicación.

Cómo empezar la resolución de problemas de VPN

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 comunicaciones en iSeries le ofrece otro lugar donde puede 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.

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 sistema principal 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 sistema principal local al sistema principal 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 Internet 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 filtrado 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 los mensajes de error en la ventana de Normas de Paquetes de iSeries Navigator. Asegúrese de que las normas de filtrado 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**, prosiga al paso 4. Si la respuesta es **no**, compruebe si hay errores en las anotaciones de trabajo QTOVMAN y las anotaciones de trabajo QTOKVPNIKE.
   Cuando utilice la VPN, su suministrador 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 deseaba. 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 deseado.

Errores de configuración de VPN habituales y cómo solucionarlos

En esta sección se describen algunos de los problemas más habituales que se producen en VPN y proporciona enlaces a las recomendaciones sobre cómo resolverlos.

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.

Mensajes de error habituales que puede encontrar

Mensaje	**Síntoma:**
TCP5B28	Al intentar activar las normas de filtrado en una interfaz, recibe este mensaje: TCP5B28 Violación de orden CONNECTION_DEFINITION
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**.

EL PARÁMETRO PINBUF NO ES VÁLIDO	Al intentar iniciar una conexión, obtiene el mensaje **EL PARÁMETRO PINBUF NO ES VÁLIDO...**
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.
No puede actualizarse 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.
No se puede 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.
CPF9821	Al intentar expandir o abrir el contenedor de políticas IP en iSeries Navigator, aparece el mensaje CPF9821- No autorizado para el programa QTFRPRS en la biblioteca QSYS.

Otros problemas con los que puede encontrarse

Error	**Síntoma:**
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.
Aparece un inicio de sesión para un sistema distinto	La primera vez que utiliza la interfaz de normas de paquetes de iSeries Navigator, aparece una pantalla de inicio de sesión para un sistema distinto del actual.
Ningún estado de la conexión	En la ventana de iSeries Navigator, hay una conexión que no tiene ningún valor en la columna **Estado**.
Las conexiones detenidas aún están habilitadas	Después de detener una conexión, la ventana de iSeries Navigator indica que la conexión todavía está habilitada.
3DES no es una opción para el cifrado	Si trabaja con una transformación de políticas IKE, una transformación de políticas de datos o una conexión manual, el algoritmo de cifrado 3DES no podrá seleccionarse.
Visualización de columnas inesperada	Ha configurado las columnas que desea visualizar en la ventana de iSeries Navigator para las conexiones VPN; a continuación, cuando vuelve a visualizarlas, aparecen columnas distintas.
Se ha producido una anomalía al desactivar las normas de filtrado activas	Al intentar desactivar el actual conjunto de normas de filtrado, aparece el mensaje `Se ha producido una anomalía al intentar desactivar las normas activas` en la ventana de resultados.

El grupo de claves dinámicas 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.

Mensaje de error de VPN: TCP5B28

Síntoma:

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

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

Posible resolución:

Las normas de filtrado 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

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:

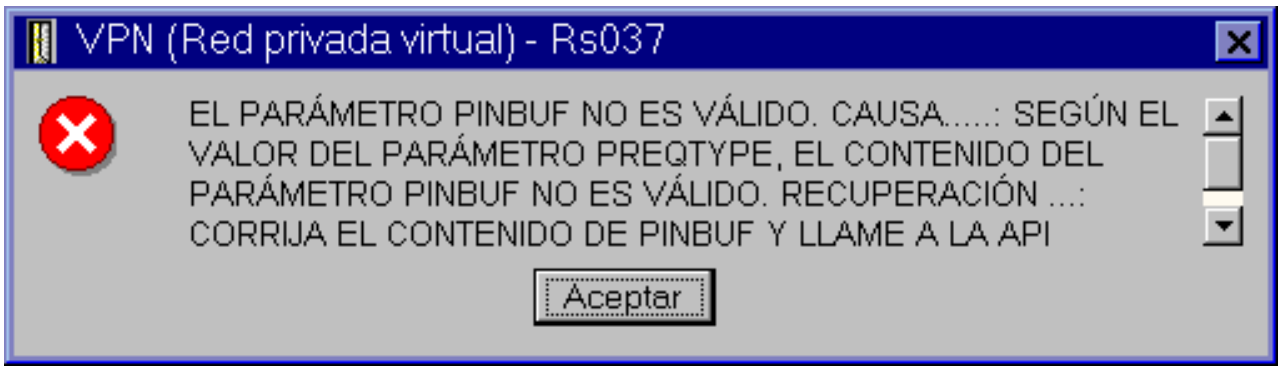
Posible resolución:

- 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 de comunicación entre el servidor VPN y el iSeries. Muchos de los objetos que aparecen en la ventana Red privada virtual 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 por omisión). 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

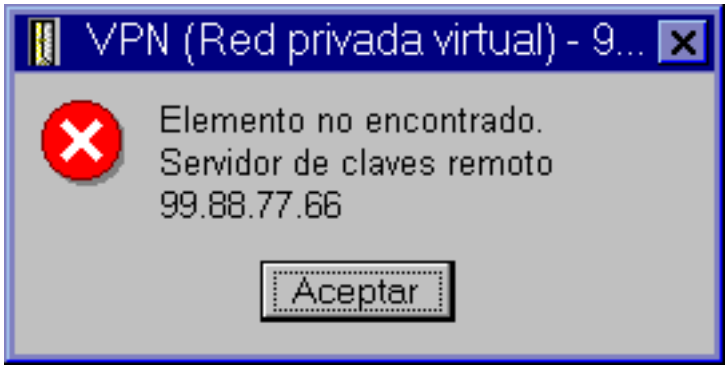
Síntoma:
Al intentar iniciar una conexión, aparece un mensaje parecido al siguiente:



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...

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

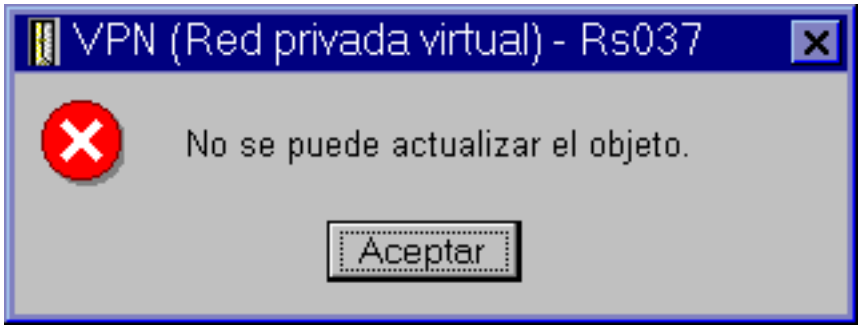


Posible resolución:
Esto se produce al crear una conexión con un identificador de servidor de claves remoto determinado y, a continuación, el servidor de claves remoto se elimina de su grupo de claves dinámicas. Para solucionar este error, pulse **Aceptar** en el mensaje de error. De esta forma, se abrirá 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

Síntoma:

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



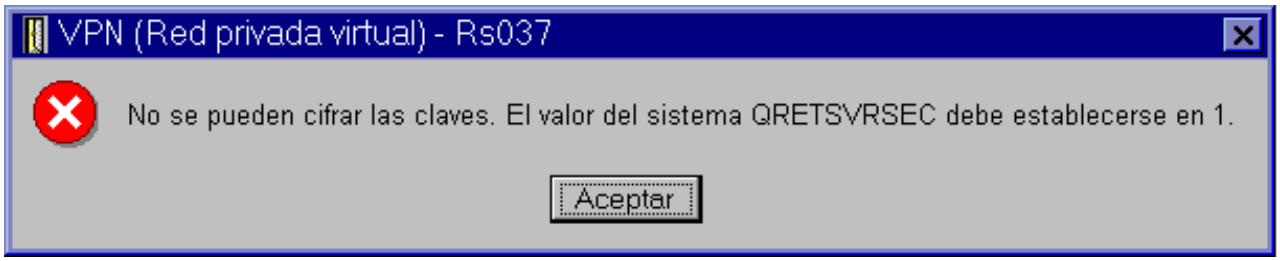
Posible resolución:

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...

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**.

Mensaje de error de VPN: CPF9821

Síntoma:

Al intentar expandir o abrir el contenedor de políticas IP en iSeries Navigator, 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 disponer de autorización *IOSYSCFG. Ahora, deberá tener acceso a las funciones de Normas de paquetes en iSeries Navigator.

Error de VPN: Todas las claves 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.

Error de VPN: Al utilizar las normas de paquetes aparece el inicio de sesión de un sistema distinto

Síntoma:

La primera vez que utilice las normas de paquete, aparecerá una pantalla de inicio de sesión para un sistema distinto del actual.

Posible resolución:

Las normas de paquetes utilizan unicode para almacenar las normas de seguridad de paquetes en el sistema de archivos integrado. El inicio de conexión adicional permite a Client Access Express obtener la tabla de conversión adecuada para unicode. Esto deberá ocurrir sólo una vez.

Error de VPN: estado de la conexión en blanco en la ventana de iSeries Navigator

Síntoma:

En la ventana de iSeries Navigator, hay una conexión que no tiene ningún valor en la columna **Estado**.

Posible resolución:

El valor de estado en blanco indica que la conexión se encuentra en la fase de inicio. O sea, aún no se encuentra en funcionamiento, pero tampoco se ha producido ningún error. Al renovar una ventana, la conexión deberá visualizar un estado de `Error`, `Habilitado`, `Por solicitud` o `Desocupado`.

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

Síntoma:

Después de detener una conexión, la ventana de iSeries Navigator indica que la conexión todavía está habilitada.

Posible resolución:

Esto suele ocurrir cuando aún no se ha renovado la ventana de iSeries Navigator. Por lo tanto, la ventana contiene información anticuada. Para solucionar esto, en el menú **Visualizar**, seleccione **Renovar**.

Mensaje de error de VPN: ·3DES no es una opción para el cifrado

Síntoma:

Si trabajó con una transformación de políticas IKE, una transformación de políticas de datos o una conexión manual, el algoritmo de cifrado 3DES no podrá seleccionarse.

Posible resolución:

Es muy probable que sólo tenga instalado en su sistema Cryptographic Access Provider AC2 (5722-AC2) y no Cryptographic Access Provider AC3 (5722-AC3). AC2 sólo acepta el algoritmo de cifrado DES (estándar de cifrado de datos) debido a las restricciones en la longitud de las claves.

Error VPN: visualización de columnas inesperada en la ventana de iSeries Navigator

Síntoma:

Ha configurado las columnas que desea visualizar en la ventana de iSeries Navigator para las conexiones VPN; a continuación, cuando vuelve a visualizarlas, aparecen columnas distintas.

Posible resolución:
Al cambiar las columnas a visualizar, los cambios no son específicos para un usuario o PC determinado, sino que más bien, afectan a todo el sistema. Por lo tanto, si alguien más cambia las columnas de la ventana, los cambios afectarán a todos los que visualicen las conexiones en el sistema.

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

Síntoma:
Al intentar desactivar el actual conjunto de normas de filtrado, 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 deberá poder desactivar las normas de filtrado.

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

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

El diario QIPFILTER está ubicado en la biblioteca QUSRSYS y contiene información sobre los conjuntos de normas de filtrado, 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 filtrado.

Cómo habilitar el diario de filtro de paquetes IP
Utilice el editor de normas de paquetes de iSeries Navigator 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 iSeries Navigator, expanda el servidor **—> Red—> Políticas IP**.
2. Pulse con el botón derecho del ratón **Normas de paquetes** y seleccione **Configuración**. Se visualizará la interfaz de normas de paquetes.
3. Abra un archivo de normas de filtrado existente.

4. Pulse dos veces la norma de filtro que desee registrar por diario.
5. En la página **General**, seleccione **FULL** en el campo **Registro por diario**, como en el 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 filtrado modificado.

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

Cómo utilizar el diario QIPFILTER
OS/400 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 filtrado cuya opción de registro por diario se haya establecido en FULL. Por ejemplo, si configura únicamente las normas de filtrado 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 filtrado. Una vez que los conjuntos de filtros se hayan comprobado, reduzca el registro por diario a un subconjunto útil de entradas.

Consulte Campos del diario QIPFILTER para obtener una tabla que describe el archivo de salida QIPFILTER.

Campos de diario QIPFILTER
La siguiente tabla describe 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	
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 6 es TCP 17 es UDP 50 es ESP 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*

Resolución de problemas de VPN con el diario QVPN

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.

Cómo habilitar el diario VPN

Utilice la opción de red privada virtual de iSeries Navigator 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 iSeries Navigator, expanda el servidor **—> Red—> Políticas IP—> Red privada virtual—> Conexiones de seguridad**.
2. Para los grupos de claves dinámicas, expanda **Por grupo** y, a continuación, 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, expanda **Todas las conexiones** y, a continuación pulse con el botón derecho del ratón la conexión manual cuyo registro por diario desea habilitar.
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.

Cómo utilizar el diario VPN

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.

Consulte Campos del diario QVPN para obtener una tabla que describe los campos del archivo de salida QVPN.

Campos de diario QVPN

La siguiente tabla describe los campos del archivo de salida VPN:

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	
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	

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 servidores iSeries. Si una conexión dinámica sufre una anomalía al iniciarse, le será útil comprender lo que sucede en el sistema remoto.

Los trabajos VPN, QTOVMAN y QTOKVPNIKE se ejecutan en el subsistema QSYSWRK. Puede visualizar sus anotaciones de trabajo respectivas desde OS/400 Operations Navigator.

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).

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.

Mensajes de error habituales del gestor de conexiones VPN

En esta sección se describen algunos de los mensajes de error más habituales del gestor de conexiones VPN.

En general, 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 iSeries Navigator 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. 2. Corrija los errores y vuelva a intentar la petición. 3. Utilice iSeries Navigator para visualizar el estado de la conexión. Las conexiones que no se han podido iniciar estarán en 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. 2. Corrija los errores y vuelva a intentar la petición. 3. Utilice iSeries Navigator para visualizar el estado de la conexión. Las conexiones que no se han podido iniciar estarán en en estado de error.

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 sistema principal remoto en una dirección IP. *2* - No se ha podido convertir el nombre del sistema principal 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. 2. Corrija los errores y vuelva a intentar la petición. 3. Utilice iSeries Navigator 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. 2. Verifique que la interfaz *LOOPBACK esté activa mediante el mandato NETSTAT OPTION(*IFC). 3. Finalice el servidor VPN mediante el mandato ENDTCPSVR SERVER(*VPN). A continuación, reinicie el servidor VPN mediante el mandato STRTCPSRV SERVER(*VPN). **Nota:** esto hace que finalicen todas las conexiones VPN actuales.

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. 2. Corrija los errores y vuelva a intentar la petición. 3. Utilice iSeries Navigator 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 hay que aplicar la NAT no es una única dirección IP. *2* - Se han utilizado todas las direcciones disponibles.	1. Compruebe si hay más mensajes en las anotaciones de trabajo. 2. Corrija los errores y vuelva a intentar la petición. 3. Utilice iSeries Navigator 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. 2. Asegúrese de que el punto final de conexión local está definido e iniciado mediante el mandato NETSTAT OPTION(*IFC). 3. Corrija los errores y vuelva a intentar la petición.

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. 2. Asegúrese de que el punto final de conexión local está definido e iniciado mediante el mandato NETSTAT OPTION(*IFC). 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. 2. Utilice iSeries Navigator para modificar la política VPN asociada con esta conexión VPN. 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. 2. Utilice iSeries Navigator 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. 3. Corrija los errores y vuelva a intentar la petición.
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. 2. Utilice iSeries Navigator 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. 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. 2. Utilice iSeries Navigator para visualizar la política asociada con esta conexión y especifique una clave secreta distinta. 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 sistema principal 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. 2. Utilice iSeries Navigator 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. 3. Corrija los errores y vuelva a intentar la petición.
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. 2. Utilice iSeries Navigator para visualizar los filtros de políticas activos. Compruebe la norma de filtro de políticas de esta conexión. 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. 2. Utilice iSeries Navigator para incrementar el número de direcciones NAT asignadas a esta conexión VPN. 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. 2. Compruebe las anotaciones de trabajo asociadas con la conexión PPP. 3. Corrija los errores y vuelva a intentar la petición.

Resolución de problemas de VPN con el rastreo de comunicaciones de OS/400

iSeries 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 por omisión 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 por omisión 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. Por omisión, 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, deberá filtrar 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 por omisión 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.

Información relacionada para VPN

Para obtener otros escenarios y descripciones, consulte estas otras fuentes de información:

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

  Este Redpaper de IBM proporciona un proceso paso a paso para configurar el túnel VPN utilizando VPN V5R1 y el soporte de L2TP e IPSec nativo de Windows 2000.
- **AS/400 Internet Security: Implementing AS/400 Virtual Private Networks, SG24-5404-00**

  Este libro rojo explora los conceptos VPN y describe su implementación utilizando IPSec (IP Security) y L2TP (Layer 2 Tunneling Protocol) en OS/400.
- **AS/400 Internet Security Scenarios: A Practical Approach, SG24-5954-00**

  Este libro rojo explora todas las funciones de seguridad nativas disponibles en el sistema AS/400, como pueden ser filtros IP, NAT, VPN, servidor proxy HTTP, SSL, DNS, retransmisión de correo, auditoría y anotaciones. Describe su utilización a través de ejemplos prácticos.
- **Red privada virtual: asegurar las conexiones**

  Esta página Web pone de relieve las noticias VPN más actuales, lista los últimos PTF y contiene enlaces a otros sitios de interés.
- **Otros manuales y libros rojos relacionados con la seguridad**
  Diríjase aquí para obtener una lista de la información en línea disponible relacionada con la seguridad.

Para guardar un archivo PDF en su estación de trabajo para visualizarlo o imprimirlo:

1. Pulse con el botón derecho del ratón sobre el archivo PDF del navegador (pulse el enlace anterior).
2. Pulse **Guardar destino como...**
3. Desplácese al directorio en el cual desee guardar el archivo PDF.
4. Pulse **Guardar**.

Si necesita Adobe Acrobat Reader para ver o imprimir estos PDF, puede bajar una copia desde sitio Web de Adobe (www.adobe.com/prodindex/acrobat/readstep.html)

.

Impreso en España