IBM eNetwork Firewall para Windows NT

Guía del usuario

Versión 3 Release 2.1.1

GC10-3279-01

IBM eNetwork Firewall para Windows NT

Guía del usuario

Versión 3 Release 2.1.1

GC10-3279-01

Nota: Antes de utilizar esta información y el producto al que da soporte, lea cuidadosamente la información general que encontrará en Apéndice A, “Avisos” en la página 127.

Segunda edición (junio 1998)

Esta edición se aplica a la Versión 3 Release 2.1.1 del the IBM eNetwork Firewall para Windows NT (número de producto 5765-C16). Esta edición sustituye a la GC10-3279-00.

Contenido

Acerca de este manual

En este manual se describe cómo configurar y administrar el IBM eNetwork Firewall en un sistema Windows NT** para poder evitar comunicaciones no deseadas o no autorizadas en ambos sentidos de la red protegida.

Este manual va dirigido a los administradores de la red o de la seguridad del sistema que se encargan de instalar, administrar y utilizar el IBM Firewall. Aunque se describe cómo acceder al cortafuegos mediante la utilización de programas de cliente, no se trata de una guía del usuario para los programas de cliente. Para utilizar programas de cliente, como telnet o FTP, consulte la guía del usuario de los programas de cliente TCP/IP.

Siga las Instrucciones de instalación que se incluyen en el estuche del CD-ROM para instalar el producto antes de utilizar este manual.

Tras iniciar el cliente de configuración, la información de la ayuda en línea le ayudará a cumplimentar los campos del cliente de configuración y a moverse de un cuadro de diálogo a otro.

Conocimientos previos

Es importante disponer de amplios conocimientos en direccionamientos TCP/IP, máscaras y administración de la red antes de instalar y configurar el IBM Firewall. Puesto que va a definir y configurar un cortafuegos que controla el acceso de entrada y salida de la red, primero deberá entender el funcionamiento de la red. En especial, deberá entender los elementos básicos de las direcciones IP, los nombres calificados al completo y las máscaras de subred.

Un excelente manual sobre TCP/IP que cubre netstat, arp, ifconfig, ping, nslookup, DNS, sendmail, el direccionamiento y muchas más materias es *TCP/IP Network Administration*. Consulte el apartado *Bibliografía* para obtener más detalles.

Un excelente manual para los encargados de realizar la administración UNIX, que también ofrece una excelente visión general acerca de TCP/IP y del direccionamiento, del hardware para la red, DNS y sendmail es *UNIX System Administration Handbook*. Consulte la Bibliografía para obtener más detalles.

Características de este release

El IBM eNetwork Firewall para Windows NT ofrece una rica selección de características e incluye las tres arquitecturas del cortafuegos:

1. Proxies de aplicación
   - FTP
   - HTTP, incluyendo Gopher y WAIS
   - Telnet
   - SafeMail

   HTTP, Telnet y FTP tienen posibilidad de autentificación.

2. Pasarela a nivel de circuito a través del protocolo Socks versión 5, un estándar de Internet
3. Filtro—un amplio y sólido conjunto de criterios sobre qué tráfico puede permitirse o denegarse. Los criterios incluyen la dirección TCP/IP, la puerta, el protocolo, la dirección, el adaptador (protegido/no protegido) y otros.

   Existen numerosos servicios predefinidos que hacen que la configuración resulte más rápida.

Protocolo Socks, Versión 5

Además de su simplicidad y flexibilidad, el protocolo Socks, versión 5, ofrece las ventajas siguientes:

- Fácil desarrollo de los métodos de autentificación y cifrado
- Asociación UDP, que crea un circuito proxy virtual para atravesar circuitos proxy basados en UDP.
- Socks V5 Watcher, que muestra información del rendimiento del socks en tiempo real

Conversión de dirección de red

Con el crecimiento explosivo de Internet, el agotamiento de direcciones de IP se ha convertido en un problema de primer orden. La conversión de direcciones de red (NAT) proporciona una solución al problema del agotamiento de direcciones de IP gracias a la reutilización de direcciones.

La ventaja de la NAT es que permite a la red que utiliza direcciones privadas o ilegales comunicarse de forma transparente con sistemas principales en Internet, logrando de hecho que la red privada tenga un mayor espacio de dirección. Además, al utilizar la NAT, las direcciones en la red privada quedan ocultas del resto del mundo, con lo que se proporciona un nivel de seguridad adicional.

Sencilla administración

Mediante la utilización de una aplicación Java**, que puede administrarse desde una máquina remota, se pueden realizar fácilmente actualizaciones en la configuración del cortafuegos. También es posible asignar a los distintos administradores distintos niveles de autorización para ejercer mayor control sobre el acceso al cortafuegos. Esta interfaz gráfica de usuario (GUI) sencilla y fácil de entender puede utilizarse para administrar el Windows NT Firewall y el AIX Firewall.

Delimitación de NT

Cuando se instala el cortafuegos, los protocolos no TCP/IP está inhabilitado, los servicios del sistema que no se necesitan están inhabilitados y las conexiones locales desde perfiles que no son el administrador están inhabilitadas.

Sólida autentificación

Se ofrece soporte para todos los mecanismos de autentificación basados en contraseñas más conocidos, como SecurID, Clave SecureNet y otros.

Programas de utilidad de informes

Los programas de utilidad de informes le permiten ejecutar una consulta SQL en el registro del sistema cuando se ha exportado a una máquina de bases de datos.

Alertas, supervisión y registro

El extenso y detallado registro incluye toda la actividad del cortafuegos y las direcciones TCP/IP, ID de usuarios, TOD, nombres de archivos, números de puertas, etc. Se incluye un Supervisor de registro para observar actividades sospechosas y enviarle alertas cuando se han excedido los umbrales.

Aislamiento de varias redes

Mediante la utilización de Tarjetas de interfaz de red (NIC) en el cortafuegos, se pueden aislar varias subredes.

Soporte al idioma nacional

El soporte al idioma nacional se ofrece para el inglés, japonés, coreano, francés, chino simplificado, chino tradicional, italiano, español y portugués de Brasil.

Entrada de direcciones IP

Cuando configure el cortafuegos, se le solicitará que especifique direcciones IP. Debe especificar una dirección IP con puntos decimales completa, compuesta de 4 octetos, en el formato:

```
nnn.nnn.nnn.nnn
```

donde cada `nnn` es un conjunto de tres números que se encuentran en el rango 000–255.

Cómo ponerse en contacto con IBM para recibir servicio

El centro de asistencia de IBM le proporciona ayuda telefónica para el diagnóstico y resolución de problemas. Puede llamar al centro de asistencia de IBM en cualquier momento; volverán a llamarle dentro de las siguientes ocho horas laborables (Lunes a viernes, de las 08:00 a las 17:00 horas, horario local del cliente). El número al que puede llamar es el 1-800-237-5511.

Si se encuentra fuera de los Estados Unidos o de Puerto Rico, póngase en contacto con el representante de IBM de su localidad o con su concesionario de IBM autorizado.

Capítulo 1. Presentación del IBM Firewall

El IBM eNetwork Firewall es un programa de seguridad de la red para AIX y Windows NT**. Básicamente, un cortafuegos es un bloqueo entre una o más redes internas privadas, protegidas, y otras redes (no protegidas) o Internet. La finalidad de un cortafuegos es evitar las comunicaciones no deseadas o no autorizadas dentro o fuera de la red protegida. El cortafuegos desempeña tres funciones:

- Refuerza las políticas de seguridad para Internet
- Permite a los usuarios utilizar sus propios recursos con autorización de utilización de la red desde la red externa sin comprometer los datos de la red ni otros recursos
- Mantiene fuera de la red a los usuarios no autorizados

Conceptos del cortafuegos

El hecho de que Internet admita cualquier tipo de conectividad puede implicar muchos riesgos para la seguridad. Necesita proteger sus datos privados y también el acceso a las máquinas que se encuentran en el interior de la red privada para evitar una utilización externa abusiva. El primer paso para lograr esta protección es limitar el número de puntos de conexión de la red privada a Internet. Una configuración en la que la red privada se conecta a Internet mediante una única pasarela le ofrece control sobre el tráfico de entrada y salida que desea admitir de Internet. Nosotros llamamos cortafuegos a esta pasarela.

Para comprender el funcionamiento de un cortafuegos ponemos este ejemplo. Imagínese un edificio cuyo acceso desea restringir y controlar las personas que entran en el mismo. El vestíbulo del edificio es el único punto de entrada. En el vestíbulo, cuenta con varios recepcionistas que dan la bienvenida a las personas que entran en el edificio, algunos guardias de seguridad encargados de la vigilancia, cámaras de vídeo para grabar sus movimientos y lectores de distintivos para autentificar su identidad.

Este método es bastante eficaz para controlar la entrada a un edificio privado. Pero, si una persona no autorizada logra atravesar el vestíbulo, no existe forma alguna de proteger el edificio contra las acciones de esta persona. Sin embargo, si supervisa los movimientos de esa persona, podrá detectar cualquier comportamiento que le resulte sospechoso.

Al definir la estrategia del cortafuegos, probablemente pensará que es suficiente para prohibir todo acceso que represente un riesgo para la organización y permitir el acceso al resto. Sin embargo, y a consecuencia de la aparición de nuevos métodos de ataque, debe anticiparse para prevenir tales ataques y, como sucedía en el caso del edificio, debe supervisar si existen signos que indiquen que sus defensas han quedado expuestas de algún modo. Por lo general, resulta más perjudicial y costoso recuperarse de una intromisión que evitarla primero.

Herramientas de IBM Firewall

El IBM Firewall es como una caja de herramientas que se utiliza para implementar distintas arquitecturas de cortafuegos. Cuando ha elegido la arquitectura y la estrategia de seguridad, ha de seleccionar las herramientas del IBM Firewall que necesita. El cliente de configuración IBM Firewall proporciona una interfaz gráfica de usuario de sencilla utilización para la administración. IBM Firewall proporciona un registro completo de todos los sucesos significativos, como los cambios administrativos y los intentos de infringir la seguridad.

Puesto que el IBM Firewall es básicamente una pasarela IP, divide todo en dos o más redes: una o más redes no protegidas y una o más redes protegidas. La red no protegida es, por ejemplo, Internet. Las redes protegidas suelen ser sus redes IP corporativas. Entre las herramientas que el IBM Firewall ofrece se encuentran:

- Filtros especiales
- Servidores proxy
- Servidores socks
- Servicios específicos, como el servicio de denominación de dominios (DNS) y SafeMail

Filtros especiales

Los filtros especiales son herramientas que inspeccionan los paquetes a nivel de sesión basándose en varios criterios, como la hora, la dirección IP y la subred. Las normas de filtro funcionan conjuntamente con la función de pasarela IP, por lo que la máquina necesita tener dos o más interfaces de red, cada una en una subred o red IP por separado. Un grupo de interfaces se declara no protegido y el otro conjunto se declara protegido. Los filtros actúan entre estos dos conjuntos de interfaces, como se muestra en la Figura 1.

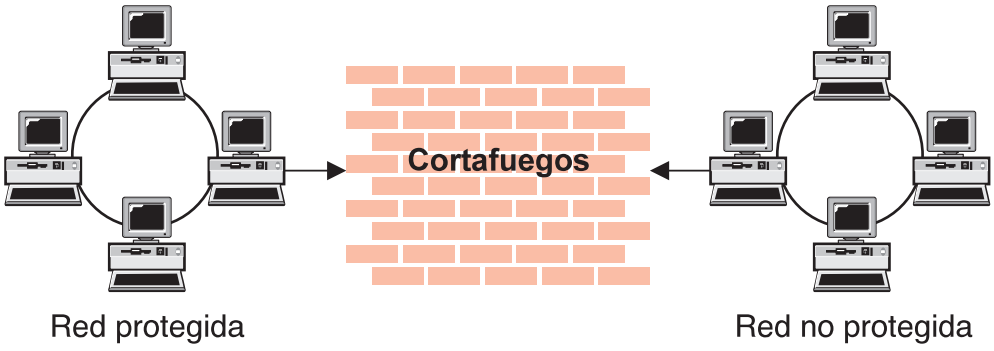

Figura 1. Cortafuegos con filtrado especial

Objetivos de los filtros especiales

El filtrado especial proporciona el mecanismo de protección básico del cortafuegos. Los filtros le permiten determinar qué tráfico pasa a través del cortafuegos basándose en los detalles de la sesión IP, protegiendo de este modo la red protegida de amenazas externas, como la exploración de servidores protegidos o fraudes en la dirección IP. Piense que el recurso de filtrado es la base sobre la que se construyen las demás herramientas.

Servidores proxy

A diferencia del filtrado, que simplemente inspecciona los paquetes que pasa a través del cortafuegos, los servidores proxy son aplicaciones que forman parte del cortafuegos y que realizan funciones TCP/IP específicas para un usuario de la red. El usuario se pone en contacto con el servidor proxy utilizando una de las aplicaciones TCP/IP (Telnet o FTP). El servidor proxy se pone en contacto con el sistema principal remoto por el usuario, controlando así el acceso a la vez que se oculta la estructura de la red a los usuarios externos. La Figura 2 muestra un servidor proxy Telnet que intercepta una petición de un usuario externo.

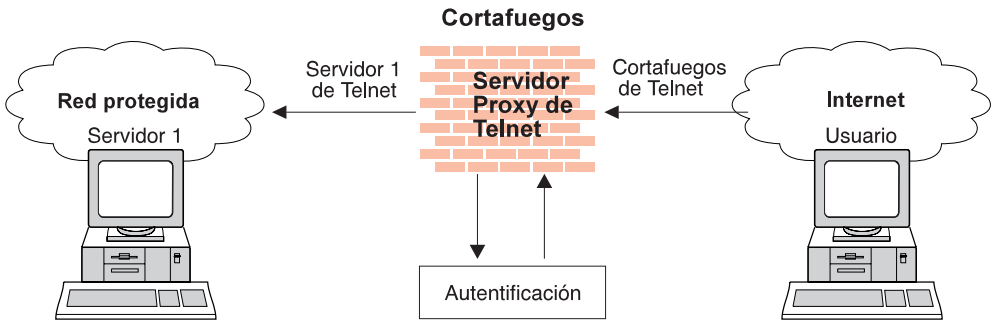

Figura 2. Cortafuegos con un servidor proxy

Los servicios proxy disponibles son telnet, FTP, HTTP, WAIS, GOPHER y HTTPS y SafeMail.

Los servidores proxy del IBM Firewall pueden autentificar usuarios utilizando gran diversidad de métodos de autentificación. Los usuarios pueden acceder a la útil información de Internet sin comprometer la seguridad de sus redes internas.

Objetivos de los servidores proxy

Cuando se conecta mediante un servidor proxy, las conexiones TCP/IP quedan interrumpidas en el cortafuegos, reduciendo la posibilidad de comprometer la red protegida. Puede que los usuarios también tengan que autentificarse utilizando uno de los numerosos métodos de autentificación.

Una de las principales ventajas de los servidores proxy es la ocultación de la dirección. Todas las conexiones proxy de salida utilizan la dirección del cortafuegos. Otra importante ventaja del servidor proxy es la seguridad. Los expertos de IBM han desarrollando estos servidores proxy para proteger los puntos débiles de la seguridad, que podrían encontrarse en la máquina del cliente.

Otra ventaja del servidor proxy es que no necesitará una versión especial del programa cliente en la maquina del cliente. Por lo tanto, cuando haya instalado el cortafuegos, cada usuarios que se haya registrado en el cortafuegos podrá acceder a la red no protegida sin necesidad de instalar ningún software adicional.

Servidor Socks

Socks es un estándar para pasarelas a nivel de circuito que ofrece ocultación de la dirección pero que no necesita la actividad general de un servidor proxy más convencional.

El servidor Socks es similar a un servidor proxy en que la sesión se interrumpe en el cortafuegos. La diferencia es que socks puede dar soporte a todas las apli-

caciones en lugar de necesitar un proxy exclusivo para cada aplicación. De manera transparente, el cliente Socks inicia una sesión con el servicio socks de Windows NT en el sistema principal del IBM Firewall y a continuación valida que la dirección de origen y el ID de usuario tengan permiso para establecer conexiones progresivas en la red no protegida y a continuación crea la segunda sesión.La Figura 3 muestra un cortafuegos con un servidor socks.

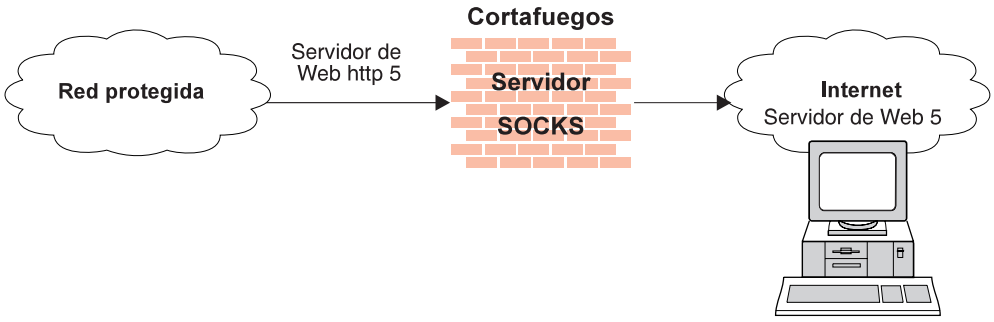

Figura 3. Cortafuegos con un servidor socks

Los clientes con capacidad de Socks (clientes, que reconocen Socks) están disponibles con muchas aplicaciones como Netscape Navigator** o Microsoft** Internet Explorer, o mediante software de TCP/IP como Aventail** AutoSocks**.

Objetivos del servidor socks

Para las sesiones de salida, (de un cliente protegido a un servidor no protegido) el servidor socks tiene los mismos objetivos que un servidor proxy, es decir, interrumpir la sesión en el cortafuegos y proporcionar una puerta segura donde los usuarios deben probar su identidad para poder traspasarla. Para el usuario, su ventaja es su simplicidad, con poco trabajo administrativo adicional.

Servicio de denominación de dominios

El acceso a los registros de nombres de dominios de la red protegida resulta de gran ayuda a los intrusos, pues les ofrece una lista de sistemas principales que pueden atacar. Un servidor del servicio de denominación de dominios intervenido también puede ofrecer una ruta de acceso a un intruso. Desde la red externa, el servidor de nombres del cortafuegos sólo se reconoce a sí mismo y nunca proporciona información acerca de la red IP interna. Desde la red interna, este servidor de nombres reconoce la red Internet y resulta muy útil para acceder a cualquier máquina en Internet por su nombre.

Objetivos del servidor DNS

La ejecución del servidor DNS en el cortafuegos ofrece la doble ventaja de evitar que las peticiones de resolución de nombres fluyan por el cortafuegos y de ocultar los sistemas principales de la red protegida ante todo lo no protegido.

SafeMail

El correo es una de las principales razones por las que una organización deseará acceder a Internet. SafeMail es una pasarela de correo de IBM diseñada para ocultar los nombres de dominios de la red interna. La función SafeMail no almacena correo en la pasarela ni se ejecuta bajo el ID del usuario raíz. El nombre de dominio público de la pasarela del cortafuegos se sustituye por el nombre de usuario en el correo de salida para que el correo parezca proceder de la dirección

del cortafuegos en lugar de la dirección de la dirección del usuario. SafeMail da soporte al Protocolo simple de transferencia de correo (SMTP) y a las Extensiones de correo de Internet para varias finalidades (Multipurpose Internet Mail Extensions, MIME).

Utilización de la Comprobación de la seguridad de la red

La Comprobación de la seguridad de la red explora la red en busca de vacíos en la seguridad o errores de configuración. La Comprobación de la seguridad de la red explora los servidores y los cortafuegos para ofrecer una lista de problemas o puntos vulnerables, como las puertas abiertas y otros elementos de riesgo, y compila una lista para que pueda hacer las correcciones. La Comprobación de la seguridad de la red puede utilizarse como escáner periódico de los sistemas principales críticos o como herramienta para obtener información en un momento determinado. La administración de la Comprobación de la seguridad de la red se realiza a través de una interfaz de la línea de mandatos de sencilla utilización. Con la Comprobación de la seguridad de la red, el cortafuegos se mantiene bajo vigilancia.

Entre las funciones de la Comprobación de la seguridad de la red se incluyen:

- Lectura con escáner de las puertas TCP y UDP
- Reconocimiento de servidores en puertas que no son estándar
- Informe de servicios peligrosos, puntos vulnerables conocidos, versiones obsoletas de los servidores y servidores o servicios que no se ajustan a la política personalizada de la ubicación
- Generación de informes en HTML para facilitar su examen

Capítulo 2. Planificación

Antes de configurar el IBM Firewall, utilice la lista de comprobación y las hojas de trabajo para la planificación como ayuda para entender la configuración de la red.

Lista de comprobación de planificación

1. Defina sus objetivos. Desea:
   - ¿Acceder a Internet (telnet, anonymous FTP, etc.)?
   - ¿Particionar partes de la red interna?
   - ¿Proporcionar acceso *externo* a su red?
2. Evalúe la topología de la red a nivel de subred IP.
   - ¿Constituyen una interfaz protegida y una interfaz no protegida una configuración correcta?
   - ¿Es capaz su dirección de dar soporte a máscaras de subred en las normas?
3. Decida cómo va a utilizar el DNS. Consulte Capítulo 6, “Gestión del Servicio de denominación de nombres” en la página 31.
4. Decida cómo va a utilizar el safemail. Consulte Capítulo 7, “SafeMail” en la página 39.
5. Si desea utilizar socks, asegúrese de que los clientes socks, como Netscape Navigator o el navegador de Microsoft, estén instalados. Para obtener información acerca de la utilización de los socks, consulte el Capítulo 11, “Configuración del servidor Socks” en la página 69.
6. ¿Qué tipo de autentificación se necesita?
   - Si va a utilizar el Security Dynamics** ACE/Server** para la autentificación de los usuarios, instale el código del cliente ACE/Server en el sistema principal del cortafuegos. Le sugerimos instalar el código de servidor de ACE/Server en otro sistema principal que se encuentre en el interior de la red protegida.

     Para obtener información acerca de la instalación y utilización de un Security Dynamics ACE/Server y de la tarjeta SecurID**, consulte la información que proporciona Security Dynamics Technologies Inc.
   - Si va a utilizarse la tarjeta AssureNet Pathways** SecureNetKey**, adquiera las tarjetas con independencia del IBM Firewall.
   - Si utiliza un método de autentificación propio, consulte el capítulo Cómo suministrar sus propios métodos de autentificación en el manual *IBM eNetwork Firewall - Manual de consulta*.
   - Debe configurar el código de cliente de Windows que implementa la posibilidad de buscar dominios de Windows NT fiables para realizar la autentificación, para utilizar TCP en lugar de NETBIOS. NETBIOS se inhabilitará. Los servidores de Windows NT fiables deben tener nombres de sistemas principales y direcciones TCP/IP y disponer de conectividad TCP/IP entre ellos y el cortafuegos. El administrador del cortafuegos necesita crear conexiones entre el cortafuegos y los servidores de Windows NT fiables para permitir el flujo del tráfico entre ambos.

Defina esta conexión utilizando los servicios predefinidos siguientes:

a. Autentificación de controlador de dominio - que permite la utilización del Controlador de dominio para la autentificación del usuario

b. Difusiones generales de los Servicios de nombres NetBT - que permiten difusiones generales de los Servicios de nombres NetBIOS sobre TCP/IP

Y utilice los programas de utilidad de configuración NT para definir las relaciones de fiabilidad.

7. Si utiliza filtros, empiece con normas de filtros sencillas y haga que cada vez sean más restrictivas. Familiarícese con las puertas y los protocolos que utilizan los servicios que necesita.
8. Decida el método que desea utilizar para archivar los archivos de registro. El archivo es el candidato ideal para un trabajo planificado del servicio Windows NT Scheduler (Planificador de Windows NT). Consulte el Capítulo 15, “Gestión de registros y archivos” en la página 109.

Hoja de trabajo de la planificación de la configuración de la red

Cumplimente la información siguiente como parte de la planificación de la configuración de IBM Firewall.

Nombre del sistema principal del cortafuegos _____

Interfaz o interfaces de la red protegida (conectadas a la red protegida interna)

Dirección IP _____ Máscara de subred _____

Dirección IP _____ Máscara de subred _____

Dirección IP _____ Máscara de subred _____

Dirección IP _____ Máscara de subred _____

Interfaz o interfaces de la red no protegida (conectadas a una red no protegida)

Dirección IP _____ Máscara de subred _____

Dirección IP _____ Máscara de subred _____

Dirección IP _____ Máscara de subred _____

Dirección IP _____ Máscara de subred _____

Nombre del direccionador _____

Dirección del direccionador _____

Nombre del dominio protegido _____

Dirección IP del servidor de denominación de dominios (DNS)
no protegidos _____

Dirección IP del servidor o servidores de denominación de dominios
(DNS) no protegidos _____

Servidor de correo protegido
_____

Nombre de dominio público
_____

Dirección IP del cliente de configuración _____

Dirección IP del cliente o clientes remotos _____

Directorio raíz del Windows NT Firewall _____
(Nos referimos a este directorio como ROOTDIR en toda la
documentación)

c:\winnt (Asumimos que Windows NT está instalado en este directorio)

Capítulo 3. Puesta a punto del servidor de configuración y del cliente de configuración

En este capítulo se explica cómo preparar el servidor de configuración y el cliente de configuración, que es la interfaz gráfica de usuario (GUI) para el IBM Firewall.

Puesta a punto del servidor de configuración

El servidor de configuración es la interfaz del cliente de configuración para el cortafuegos. El servidor de configuración procesa las peticiones del cliente de configuración. Se ejecuta en una máquina del cortafuegos y puede manejar peticiones de clientes de configuración que se encuentren en máquinas locales o remotas. Una vez configurado, debe considerarse parte integrante de la máquina del cortafuegos.

El número de puerta del servidor de configuración se especifica en el archivo de servicios NT que se encuentra en el directorio en que ha instalado el sistema operativo Windows: `c:\winnt\system32\drivers\etc\services`. El número de puerta toma 1014 por omisión, pero puede cambiarlo, para reforzar la seguridad, deteniendo el servicio del servidor de configuración, modificando el archivo de servicios y reiniciando el servicio del servidor de configuración.

El servidor de configuración está configurado inicialmente para aceptar sólo las peticiones de los clientes de configuración de la máquina local. Las peticiones iniciales no están cifradas. Para cambiar estas opciones, utilice `fwcfgsrv cmd=change` desde la línea de mandatos.

localonly= Indica si el cortafuegos sólo puede administrarse desde una máquina local.

- **localonly=yes** La configuración sólo puede realizarse en la máquina local; es el valor por omisión.
- **localonly=no** La configuración puede realizarse desde cualquier máquina.

encryption Indica si el servidor de configuración espera que los datos de entrada se cifren a través de la capa de sockets protegidos (ssl) o no.

Si cambia la opción de cifrado o el archivo ssl, deberá detener y reiniciar el servicio del servidor de configuración.

- **encryption=none** No se realizará ningún cifrado; es el valor por omisión.
- **encryption=ssl** Se realizará el cifrado SSL.

sslfile= Indica el nombre del archivo de claves SSL que ha de utilizarse con el cifrado SSL; el valor por omisión es `ROOTDIR\config\fwkey.kyr`. *ROOTDIR* es el directorio que ha seleccionado durante el proceso de instalación como ubicación de destino para IBM Firewall. Para obtener información acerca de cómo crear el archivo de claves, consulte el manual *IBM eNetwork Firewall - Manual de consulta*

Si un cliente de configuración no puede conectarse a la máquina del cortafuegos, y está en una máquina distinta, utilice `fwcfgsrv cmd=list` para comprobar si se ha establecido `localonly=no`. Además, el idioma que utiliza el cliente y el servidor debe coincidir. Para finalizar, asegúrese de que el servicio del servidor de configuración esté en ejecución visualizando el panel de los servicios y comprobando su estado. Para ello, vaya al panel del control y efectúe una doble pulsación en el icono Servicios para comprobar el estado de cada servicio. Si no está en ejecución, el servicio debe reiniciarse.

Puesta a punto del Cliente de configuración (GUI)

Cuando inicialmente instala IBM Firewall, el cliente de configuración se instala automáticamente. El cliente de configuración también puede instalarse por separado en cualquier máquina Windows NT sin el cortafuegos, lo que le permite realizar la administración remota. Para iniciar el cliente de configuración, efectúe una doble pulsación sobre el icono del cliente de configuración, que se encuentra en el grupo de programas del IBM Firewall. Cuando se inicia el cliente de configuración, el primer paso es conectarse al cortafuegos utilizan un perfil de administrador de Windows NT.

Sólo los administradores de Windows NT y los administradores del cortafuegos que dispongan de la autentificación administrativa adecuada pueden utilizar el cliente de configuración para conectarse al cortafuegos.

Tras la instalación del cortafuegos, todos los administradores de Windows NT se designarán como administradores principales del cortafuegos. Utilice le cliente de configuración para conectarse al servidor de configuración utilizando un nombre de administrador principal del cortafuegos y defina nombres de usuario de administradores del cortafuegos adicionales, si es necesario. Consulte el Capítulo 12, “Administración de los usuarios en el cortafuegos” en la página 75 para obtener información acerca de cómo definir administradores de cortafuegos utilizando el cliente de configuración.

Para establecer el valor del tiempo de espera de conexión para máquinas más rápidas o más lentas, haga los siguientes cambios pulsando el icono del cliente de configuración y acto seguido **Propiedades**. Modifique las propiedades utilizando la pestaña **Método abreviado**. Cambie el parámetro `timeout` para que sea *20*, donde 20 es igual al número de segundos a esperar a que se produzca una conexión. Las máquinas más rápidas puede establecerse en 10 y las máquinas más lentas deben aceptar el valor por omisión.

Para incrementar el nivel de la información de depuración en la consola JAVA, ejecute `ibmfw.bat` en `ROOTDIR\cfgcli\gui` en vez de utilizar el icono del cliente de configuración. Sin embargo, tenga en cuenta que la habilitación del registro de consola puede influir negativamente en el rendimiento.

Conexión al cliente de configuración

Para conectarse al cliente de configuración (en la máquina local o remota):

- El usuario debe ser un administrador del cortafuegos
- Deberá haberse definido un esquema de autentificación para el administrador del cortafuegos. Consulte “Métodos de autentificación de usuario” en la página 81.

- El usuario debe dispone de autorización para realizar funciones de configuración específicas

Habilitación de la configuración remota mediante el cliente de configuración

Para habilitar la configuración remota mediante el cliente de configuración, asegúrese de que para el administrador que va a conectarse se hayan definido los atributos siguientes en la máquina del cortafuegos:

- Si el administrador se encuentra en la parte protegida de la red y utiliza una interfaz protegida en la máquina del cortafuegos, el administrador deberá definirse con el métodos de autentificación adecuado para la administración protegida. (No puede definirse como denegar todo). Esto también se aplica a la conexión local al cortafuegos.
- De forma similar, si el administrador se encuentra en la parte no protegida y utiliza una interfaz no protegida en la máquina del cortafuegos, el administrador deberá definirse con el método de autentificación adecuado para la administración no protegida. (No puede definirse como denegar todo).

Todos los atributos de usuario pueden definirse mediante el cuadro de diálogo Modificar usuario del cliente de configuración o utilizando el mandato `fwuser`. Tras la instalación del cortafuegos, se habrán definido de forma adecuada todos los campos anteriores para los administradores del cortafuegos. Consulte el Capítulo 12, “Administración de los usuarios en el cortafuegos” en la página 75 para obtener más información.

Ejemplo de salida del registro para el servidor de configuración remota

El siguiente es un ejemplo de la salida del registro para el servidor de configuración remota:

```
Feb 03 13:52:15 1998 mr16n18: ICA9005i: Iniciando
servidor de configuración remota.

Feb 03 13:52:21 1998 mr16n18: ICA2024i: El administrador del usuario
ha realizado la autentificación satisfactoriamente usando
la autentificación NT de la red protegida:127.0.0.
Feb 03 13:52:21 1998 mr16n18: ICA2169i: El administrador del
usuario ha realizado satisfactoriamente la autentificación del
Servidor de administración remoto utilizando la red protegida de NT:
127.0.0.1.
```

Capítulo 4. Utilización del cliente de configuración

Utilice el cliente de configuración, que es una interfaz gráfica de usuario, para configurar y administrar el IBM Firewall.

Cuando instala por primera vez el IBM Firewall, éste está configurado para aceptar sólo peticiones del cliente de configuración en la máquina local. Sin embargo, puede instalar el cliente de configuración en otra máquina y administrar el cortafuegos de forma remota. Consulte “Puesta a punto del servidor de configuración” en la página 11 para obtener información acerca de cómo hacerlo.

Para definir el cliente de configuración para que se inicie en el idioma de su escenario específico, pulse en el icono del cliente de configuración del IBM Firewall y pulse a continuación en **Propiedades**. Modifique las propiedades utilizando la pestaña **Método abreviado**. Por omisión, se utiliza el escenario de la máquina del sistema principal. El IBM Firewall da soporte a estos entornos nacionales:

- en_US - Ingles de los EE.UU.
- ja_JP - Japonés PC
- ko_KR - Coreano
- zh_CN - Chino simplificado EUC
- zh_TW - Chino tradicional (Big 5)
- fr_FR - Francés
- it_IT - Italiano
- pt_BR - Portugués de Brasil
- es_ES - Español PC

Para utilizar el cliente de configuración se necesita un ratón.

El botón **Ayuda** se encuentra junto a la parte superior del panel principal del cliente de configuración. Pulse en **Ayuda** para obtener información acerca de cualquier función.

Conexión al cliente de configuración

1. En Tipo de conexión, seleccione Local si se encuentra en la misma máquina que el cortafuegos. Local es el valor por omisión. Seleccione Remota si desea acceder a otro cortafuegos de forma remota. Remota necesita que se especifique un nombre de sistema principal.
2. Si selecciona la conexión Remota, será necesario especificar el nombre del sistema principal o la dirección IP de la máquina con la que desea conectarse.
3. Seleccione SSL o ninguno, según el cifrado que se utilice para el cortafuegos. Para el Cliente, el valor por omisión para Local es Ninguno y el valor por omisión para Remota es SSL.
4. Especifique el nombre de usuario de un administrador del cortafuegos o de un administrador de Windows NT.

5. Especifique el número de puerta al que atiende el servidor. El valor por omisión es 1014.
6. Para la Modalidad, seleccione Sistema principal si desea configurar una máquina de cortafuegos de Windows NT a la que se conecta. Con la administración del sistema principal, el administrador puede actualizar local o remotamente un cortafuegos cada vez. Seleccione Empresa (Enterprise) para la administración de la Gestión del cortafuegos de la empresa (EFM) de cortafuegos AIX.
7. Tras haberse conectado, verá mensajes de autentificación y puede que se le solicite que entre una contraseña si ese es el método de autentificación definido para su nombre de usuario. Si se le solicita una contraseña, escríbala en el campo Respuesta de usuario y pulse Intro o efectúe una pulsación en Someter. Si escribe una contraseña incorrecta, aparecerá un mensaje. Pulse en Cerrar y vuelva a iniciar el proceso de conexión. Si no se le solicita ninguna contraseña, puede que su método de autentificación de usuario se haya definido como permitir todo. En este caso, accederá inmediatamente al panel del cliente de configuración de IBM Firewall.
8. Tras haberse autentificado satisfactoriamente, verá el panel principal de configuración.

Figura 4. Panel de conexión del cliente de configuración

Árbol de navegación

El cliente de configuración dispone de una ayuda para la navegación en forma de árbol que puede desglosarse y recogerse en el lado izquierdo, como se muestra en la Figura 5 en la página 17.

Si un nodo o función tiene elementos, aparecerá un icono de carpeta de archivos a la izquierda del nodo. Para ver las subfunciones, puede ampliar la vista efectuando una doble pulsación en el icono. Vuelva a efectuar una doble pulsación en el icono para recoger la vista de este nodo y volver así a la vista original.

Cualquier función sobre la que efectúe una pulsación se considerará seleccionada y aparecerá resaltada. Puede ampliar y recoger los nodos sin realizar ningún cambio en la vista de la ventana de la derecha. Cuando el árbol ampliado excede del espacio vertical disponible, aparece una barra de desplazamiento a la derecha del árbol de navegación. Si algún nombre de función no cabe en el árbol de navegación, aparecerá una barra de desplazamiento horizontal.

Figura 5. Árbol de navegación del cliente de configuración

Funciones generales del panel principal

Sobre la **Visualización de alertas** verá los tres botones siguientes, como se muestra en la Figura 5.

Ayuda El botón **Ayuda** se encuentra junto a la parte superior del panel principal del cliente de configuración. Pulse en **Ayuda** para ver qué ha de hacer para la puesta en marcha de IBM Firewall.

Guía del usuario El botón **Guía del usuario** se encuentra junto a la parte superior del panel principal del cliente de configuración. Pulse en **Guía del usuario** para ver esta publicación en copia software.

Consulta El botón **Consulta** se encuentra junto a la parte superior del panel principal del cliente de configuración. Pulse en **Consulta** para ver esta publicación en copia software.

Los otros botones que verá en el panel principal son:

Última El botón **Última** se encuentra en la parte inferior del panel principal del cliente de configuración. Pulse en **Última** para ver las alertas más recientes.

Desconectar/Conectar

El botón **Desconectar/Conectar** se encuentra en el ángulo superior derecho del cliente de configuración. Es un botón de reconexión. Puede volver a iniciar la secuencia de conexión para conectarse a un cortafuegos distinto o para conectarse como un administrador distinto.

Para desconectarse, pulse en Desconectar, pulse en Cancelar en el panel de conexión y cierre la aplicación.

Visor de registros El botón **Visor de registros** se encuentra en el ángulo inferior derecho del cliente de configuración. Le permite examinar los registros del cortafuegos.

Anterior El botón **Anterior** se encuentra en la parte inferior del panel principal del cliente de configuración. Pulse en **Anterior** para ver las alertas anteriores.

Visualización de alertas

Puede ver los registros de alertas que ha generado el supervisor de registro del sistema en la parte inferior derecha de la ventana principal del cliente de configuración, como se muestra en la Figura 6 en la página 19.

Los registros de alertas que se visualizan se han obtenido del archivo que se identifica como el primer recurso de `registro de alertas` definido en `ROOTDIR\config\syslog.conf`. Si no se ha definido ningún recurso de `registro de alertas`, verá una pantalla en blanco. Consulte el apartado “Adición de recursos de registro” en la página 110 para obtener ayuda acerca de la definición de un recurso de `registro de alertas`.

El panel le muestra el nombre del archivo de alertas y los números de las líneas que actualmente se visualizan de ese archivo. Puede pulsar en **Última** para ver las alertas más recientes. Pulse en **Anterior** para ver las alertas anteriores.

Cada línea visualizada muestra la fecha y la hora de la alerta, el nombre del sistema principal del cortafuegos en el que se ha producido la alerta, el código del mensaje de alerta y el texto del mensaje de alerta. El código es una indicación del tipo de alerta.

Figura 6. Visualización de alertas

Visor de registros

Cuando pulsa en **Visor de registros** aparece una ventana del visor de registros, como se muestra en la Figura 7 en la página 20. El visor de registros le permite ver los registros de anotaciones del cortafuegos. Puede especificar un archivo de registro y un recuento de registros (el valor por omisión es 25).

El registro por omisión es el archivo que identifica el primer recurso de `registro del cortafuegos` definido en `ROOTDIR\config\syslog.conf`. Puede seleccionar un archivo de registro de destino distinto en el menú desplegable del campo de nombre de archivo o puede especificar el nombre del archivo que ha de visualizarse.

Para solicitar una línea de inicio específica, pulse en **Empezar desde línea:**, tras escribir el número de la línea en el campo que aparece al lado. Para solicitar la últimas líneas, pulse en **Fin**, que le llevará al final del archivo. **Siguiente** le lleva al siguiente conjunto de líneas del archivo. **Anterior** le devuelve al conjunto de líneas anterior del archivo. **Principio** le lleva al principio del archivo. Si selecciona **Sí**, podrá ampliar opcionalmente los registros del cortafuegos para convertirlos en texto legible.

Consulte el apartado “Creación y archivo del archivo de registro utilizando el cliente de configuración” en la página 109 y el Capítulo 14, “Supervisión del registro del cortafuegos” en la página 99 para obtener más información acerca de los archivos de registro, los recursos, la supervisión y las alertas.

Figura 7. Visor de registros

Otras funciones

El campo **Búsqueda** se encuentra junto al ángulo superior izquierdo de algunos de los paneles. Puede especificar un texto para la búsqueda y pulsar en **Buscar**.

Otros botones que verá en muchos de los cuadros de diálogo del cliente de configuración son:

Aplicar Pulse en **Aplicar** para poblar el campo del panel anterior con la selección actual o para guardar los cambios que ha realizado en el panel. El botón **Aplicar** no hará que desaparezca la ventana.

Fin Pulse en **Fin** para ir al final de un panel.

Cancelar Pulse en **Cancelar** para cerrar la ventana sin guardar ningún cambio realizado.

Cerrar Pulse en **Cerrar** para que la ventana no aparezca en la pantalla.

Copiar El botón **Copiar** ahorra tiempo cuando se añaden nuevos elementos a la lista. Tras seleccionar un elemento de la lista, pulse en **Copiar** para crear un elemento que sea similar al elemento seleccionado. Cuando se pulse en **Copiar** para crear un elemento que sea similar al elemento seleccionado, se abrirá un nuevo elemento que copiará los valores de los campos del elemento seleccionado en la lista. Entonces podrá modificar los valores de los campos según sea necesario para el nuevo elemento.

Suprimir Pulse en **Suprimir** para suprimir un elemento seleccionado en la lista.

Mover abajo Seleccione un elemento de la lista y pulse en **Mover abajo** para cambiar la posición relativa del elemento para que ocupe una posición inferior en la lista. Cada pulsación hará que el elemento descienda una posición.

Mover arriba Seleccione un elemento de la lista y pulse en **Mover arriba** para cambiar la posición relativa del elemento para que ocupe una posición superior en la lista. Cada pulsación hará que el elemento ascienda una posición.

Bien Pulse en **Bien** para guardar los cambios y cerrar la ventana.

Abrir Tras seleccionar un elemento de la lista, pulse en **Abrir** para ver o modificar ese elemento. Para añadir un nuevo elemento, pulse en el elemento **NUEVO** de la lista y en **Abrir**.

Renovar Pulse en **Renovar** para volver a acceder a los datos del cortafuegos y para que en el panel vuelvan a visualizarse los datos.

Eliminar Pulse en **Eliminar** para eliminar un elemento seleccionado en una lista. Esta acción sólo eliminará el elemento de la lista. Esta acción no tendrá ningún efecto en los otros lugares en los que se haya definido el elemento.

Seleccionar Pulse en **Seleccionar** para acceder a una lista de los posibles elementos que son válidos para esta función.

Principio Pulse en **Principio** para ir al principio de un panel.

Campos comunes

Los campos comunes que verá en muchos de los cuadros de diálogo del cliente de configuración son:

Salida A medida que continúe la ejecución del mandato que ha iniciado, aquí aparecerá la información del progreso.

Nombre Especifique un nombre para este elemento. Este nombre de elemento debe ser exclusivo para esta función en particular en el cortafuegos. El nombre NO debe contener el símbolo de la barra vertical (|), el carácter de comillas simples (o apóstrofo) (') o un carácter de comillas (") porque estos símbolos se utilizan como delimitadores de archivo y de SMIT. La utilización de estos caracteres puede dar lugar a que los datos no sean fiables.

Descripción Este campo es opcional y se proporciona para permitirle facilitar un comentario o información adicional acerca de este elemento.

Funciones exclusivas

Existen diversas funciones exclusivas del cliente de configuración que debe conocer.

Para un cliente de configuración de Windows 95 o Windows, el aspecto del cliente de configuración es mejor con una resolución mínima de 1024 pixels x 768 pixels.

Si mantiene pulsado el botón izquierdo del ratón para continuar utilizando un selector cíclico y arrastra accidentalmente el ratón alejándolo sin haber liberado el botón del ratón, el selector cíclico continuará. Para detenerlo, pulse una vez en las flechas de dirección del selector cíclico con el botón izquierdo del ratón.

Si se conecta con el Firewall dos o más veces en rápida sucesión mediante SSL, se le negará la conexión. Salga y vueva a arranquar el cliente de configuración.

Capítulo 5. Iniciación al IBM Firewall

Este este capítulo se describen los pasos básicos de la configuración que deberá seguir para configurar el IBM Firewall. Se explica cómo definir una interfaz protegida, cómo determinar la política de seguridad y cómo definir objetos de red.

Pasos básicos de la configuración

Para realizar una configuración básica de IBM Firewall:

1. Planifique la configuración de IBM Firewall. Decida de antemano qué funciones del cortafuegos desea utilizar y cómo desea utilizarlas. Le resultarán muy útiles estos apartados:

   - Capítulo 1, “Presentación del IBM Firewall” en la página 1
   - Capítulo 2, “Planificación” en la página 7
   - “Consideraciones para la planificación” en la página 53

2. Indique al cortafuegos cuáles de sus interfaces se han conectado a las redes protegidas. Para que el funcionamiento del cortafuegos sea correcto, debe tener una interfaz protegida y una interfaz no protegida. Desde el árbol de navegación del cliente de configuración, abra la carpeta Administración del sistema y pulse en **Interfaces** para ver una lista de las interfaces de red del cortafuegos. Para cambiar el estado de seguridad de una interfaz, seleccione una interfaz y pulse en **Cambiar**. Consulte el apartado “Designación de la interfaz de red” en la página 24 para obtener más información.

   Si desea conectarse a Internet, contacte con el ISP para obtener una dirección registrada de IP para la interfaz no protegida del cortafuegos.

3. Defina la política de seguridad general accediendo al diálogo **Política de seguridad** de la carpeta Administración del sistema. Para obtener información sobre las configuraciones del cortafuegos habituales consulte:

   - Permitir consultas DNS
   - Denegar mensaje de difusión general a la interfaz no protegida
   - Denegar Socks a los adaptadores no protegidos

   Consulte el apartado “Utilización del cliente de configuración para definir una política de seguridad” en la página 25 para obtener más información.

4. Defina el servicio de denominación de dominios y el servicio de correo. Acceda a estas funciones desde la carpeta Administración del sistema del árbol de navegación del cliente de configuración. Lea primero el apartado Capítulo 6, “Gestión del Servicio de denominación de nombres” en la página 31.

5. Defina los elementos clave de la red o redes para el cortafuegos utilizando la función **Objetos de red** del árbol de navegación del cliente de configuración. Los Objetos de red controlan en tráfico a través del cortafuegos. Defina los elementos clave siguientes como objetos de red:

   - Interfaz protegida del cortafuegos
   - Interfaz no protegida del cortafuegos
   - Red protegida
   - Cada subred de la red protegida

- Un objeto de red del sistema principal para los servidores SDI y servidores de dominio NT, si se aplica

Consulte el apartado “Objetos de red” en la página 27 para obtener más información.

6. Habilite los servicios en el cortafuegos. Son los métodos que permiten a los usuarios de la red protegida acceder a la red no protegida (como socks o proxy). Los servicios que han de implantarse dependen de las decisiones que tome en el momento de la planificación. La implementación de un servicio a menudo necesita la definición de algunas configuraciones de conexión para permitir determinados tipos de tráfico. Por ejemplo, si desea permitir a los usuarios protegidos navegar por las webs de Internet utilizando el Proxy HTTP, no sólo deberá configurar el daemon del Proxy HTTP en el cortafuegos, sino que también deberá configurar las conexiones para permitir el tráfico HTTP. Consulte Capítulo 9, “Ejemplos de servicios” en la página 53 para obtener más información acerca de cómo configurar las conexiones que dan soporte a determinados servicios.
7. Defina los usuarios del cortafuegos. Si va a necesitar autentificación para funciones tales como el acceso a una Web de salida o para los administradores del cortafuegos, deberá definir estos usuarios para el cortafuegos. Consulte el Capítulo 12, “Administración de los usuarios en el cortafuegos” en la página 75 para obtener más información.
8. Si desea utilizar contraseñas de dominio de Windows NT para la autentificación, deberá configurar el código del cliente de Windows que implementa la posibilidad de búsqueda de dominios de Windows NT fiables para la autentificación, para utilizar TCP en lugar de NETBIOS. NETBIOS se inhabilitará. Los servidores de Windows NT fiables deben tener nombres de sistemas principales y direcciones TCP/IP y disponer de conectividad entre éstos y el cortafuegos. El administrador del cortafuegos debe crear conexiones entre el cortafuegos y los servidores de Windows NT fiables para permitir el flujo de tráfico entre ambos.
9. Si desea utilizar la conversión de direcciones de red, contacte primero con su proveedor de servicios de Internet para obtener una dirección registrada de Internet que pueda utilizar con la conversión de direcciones Many-to-one. Luego, vaya al panel de *Añadir configuración NAT Configuration* para añadir la dirección registrada de Internet en el campo*Dirección IP Many-to-one*. Para obtener más información, consulte elCapítulo 16, “Conversión de direcciones de red” en la página 117.

El seguimiento de estos pasos le ayudará a realizar la puesta en marcha de la configuración básica del cortafuegos. IBM Firewall proporciona otras funciones, como los registros del sistema, que le ayudan a garantizar la seguridad de la red. Consulte el Capítulo 15, “Gestión de registros y archivos” en la página 109 para obtener más información.

Designación de la interfaz de red

En este manual se hace una distinción entre las interfaces protegidas y no protegidas, las redes y los sistemas principales. Las interfaces protegidas conectan el sistema principal del IBM Firewall a la red de sistemas principales de la red interna, la red que desea proteger. **Para que el funcionamiento del cortafuegos sea correcto, debe tener, como mínimo, una interfaz protegida.** Las interfaces no

protegidas conectan el IBM Firewall a una o más redes externas, o a Internet. El IBM Firewall debe tener, como mínimo, una interfaz no protegida.

Todas las redes que se conectan a través de una interfaz protegida se consideran redes protegidas. Para realizar distinciones entre las diversas subredes que se conectan a la interfaz protegida, utilice las normas de filtros especiales para denegar o permitir el acceso entre varias subredes en la misma interfaz basándose en la dirección IP o en una máscara de dirección.

Para designar interfaces protegidas o no protegidas, utilice la carpeta Administración del sistema del árbol de navegación del cliente de configuración. Se mostrarán todas las interfaces (adaptadores) conocidas, identificándose como protegidas o no protegidas.

Debe proporcionar un nombre para cada interfaz antes de poder llevar a cabo un filtrado de las interfaces específico.

Para identificar una interfaz de red como no protegida o no protegida:

1. Seleccione una interfaz y pulse en **Cambiar**.
2. Repita esta acción según sea necesario.
3. Pulse en **Cerrar**.

Para identificar la interfaz como protegida o no protegida y para proporcionar un nombre significativo para esa interfaz, pulse en **Abrir**. Este nombre lo utilizarán los filtros para el filtrado de la interfaz específica.

Utilización del cliente de configuración para definir una política de seguridad

Uno de los primeros aspectos que han de considerarse durante la configuración del IBM Firewall es la política de seguridad general de la instalación.

El IBM Firewall le proporciona un cuadro de diálogo que le ayuda a definir la política de seguridad, como se muestra en la Figura 8 en la página 26.

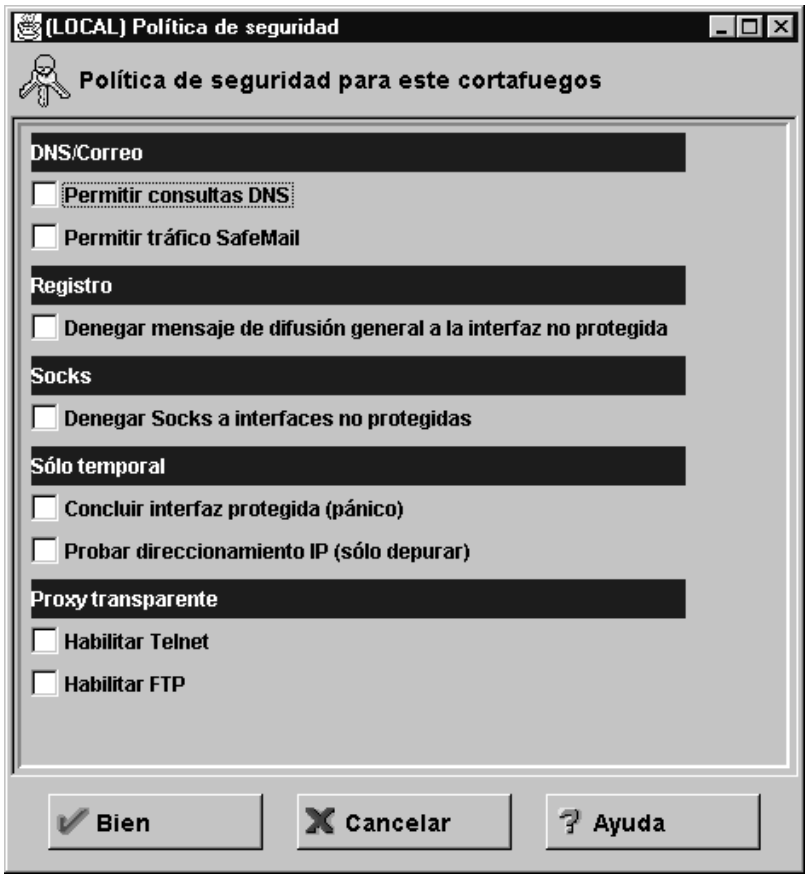

Figura 8. Política de seguridad

Pulse en Ayuda para conocer más detalles acerca del panel de la política de seguridad.

La Política de seguridad proporciona a los administradores una forma rápida y sencilla de definir políticas generales para el cortafuegos. La mayoría de los cuadros de selección que se visualizan en la ventana de la política de seguridad ofrecen un método rápido para seleccionar determinados Servicios predefinidos que se aplicarán a todo el tráfico de la red que reciba el cortafuegos. Las excepciones son las opciones de Proxy transparente, que actúan simplemente para habilitar o inhabilitar Telnet transparente y FTP transparente.

Cuando selecciona una política de seguridad, el cortafuegos crea las normas de filtros, que deben activarse. El cortafuegos habilita los servicios seleccionados y hace que estén disponibles a nivel global.

Tenga en cuenta que siempre que seleccione un cuadro de selección que corresponda a un Servicio predefinido y pulse en **Bien**, deberá activar estos cambios a través de la ventana Activación de la conexión. No será necesario activar la selecciones de Proxy transparente, pues no pertenecen a Servicios predefinidos. Consulte “Servicios predefinidos” en la página 63 para obtener una lista de servicios predefinidos.

Se le presentará la siguiente lista de cuadros de selección, donde podrá seleccionar atributos que reflejen la política de seguridad de su ubicación. Los atributos

seleccionados se aplicarán a todas las direcciones en ambos extremos del IBM Firewall.

- Seleccione **Permitir consultas DNS** para permitir peticiones de resolución y respuestas del Servicio de denominación de dominios.
- Seleccione **SafeMail** para permitir que el tráfico de correo fluya a través del cortafuegos.
- Seleccione **Denegar mensaje de difusión general a interfaces no protegidas** para impedir que en la puerta no protegida se reciban mensajes de difusión general. Si la interfaz no protegida del cortafuegos se conecta a Internet, este servicio puede ayudar a reducir la cantidad de registros del cortafuegos.
- Seleccione **Denegar Socks a adaptadores no protegidos** para no permitir que el tráfico del socks entre en el cortafuegos desde la red no protegida.
- Seleccione **Concluir interfaz protegida (pánico)** para no permitir ningún tráfico en el cortafuegos a través de las interfaces protegidas. Sólo se utiliza en casos de emergencia.
- Seleccione **Probar direccionamiento IP (sólo depurar)** para permitir todo el tráfico en el cortafuegos a través de cualquier interfaz. Tenga en cuenta que si cambia el valor de este cuadro de selección, deberá guardarlo pulsando en **Bien** y activarlo mediante la ventana Activación de la conexión. **La utilización de este Servicio puede dar lugar a que la seguridad del cortafuegos quede expuesta. Utilícelo con extremo cuidado.**
- Seleccione **Habilitar Telnet** para admitir Telnets de Proxy transparente.
- Seleccione **Habilitar FTP** para admitir FTP de Proxy transparente.

Objetos de red

Los objetos de red son representaciones de componentes que existen en la red, como los sistemas principales, las redes, los direccionadores, las redes privadas virtuales o los usuarios. Los objetos de red designan las direcciones de origen y de destino de los servicios cuando crea las conexiones.

Los objetos pueden identificarse con un nombre, representación de icono, tipo y descripción. Existen varios tipos de objetos de red, pero Sistema principal y cortafuegos son los más comunes. El objeto de red por omisión que se entrega con IBM es "Mundo". Se trata de un objeto global que engloba a todas las posibles direcciones IP. Tras haber cumplimentado las hojas de trabajo de la configuración de la red (consulte el apartado “Hoja de trabajo de la planificación de la configuración de la red” en la página 8), estará preparado para crear objetos.

Puede crear objetos individuales o de grupo. Todos los objetos de red se definen mediante una dirección IP y una máscara de dirección (máscara de subred), de modo que es posible que un objeto represente a todo un rango de direcciones de red.

Utilización del cliente de configuración para definir objetos de red

Para definir un único objeto de red, seleccione **Objetos de red** en el árbol de navegación del cliente de configuración. Aparecerá el cuadro de diálogo Objetos de red. Efectúe una doble pulsación en **NUEVO**. Aparecerá el cuadro de diálogo **Añadir un objeto de red**, como se muestra en la Figura 9.

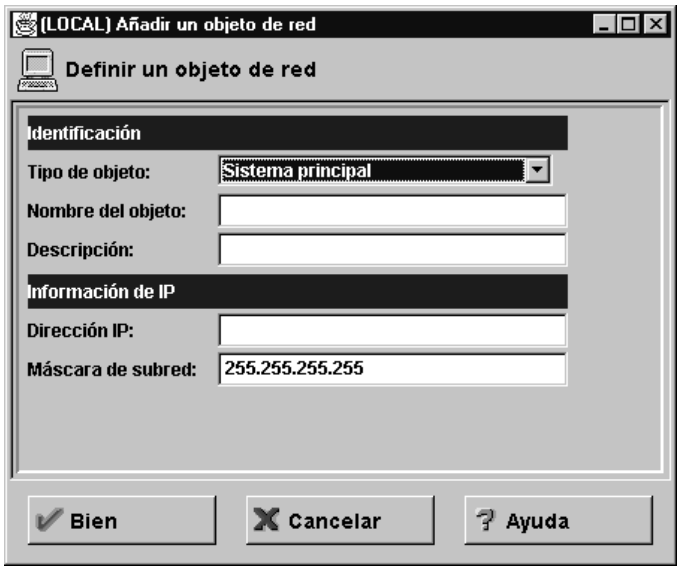

Figura 9. Añadir un objeto de red

1. Especifique el tipo de objeto. Pulse en la flecha **Tipo de objeto** para ver los tipos de objetos que puede crear. Por razones de rendimiento, es mejor crear objetos de tipo red que objetos de tipo sistema principal. Los tipos de objetos que puede crear son:
   - Sistema principal - un nodo determinado de la red con una máscara de 255.255.255.255.
   - Red - un rango colectivo de direcciones de red que se caracteriza por un rango de direcciones y una máscara de subred específica.
   - Cortafuegos - una única máquina en la que se ha instalado un cortafuegos con una máscara de 255.255.255.255. Sólo un objeto de red de cortafuegos puede ser el destino de un túnel de IBM o manual.
   - Direccionador - un sistema principal que direcciona el tráfico entre dos o más reces con una máscara de 255.255.255.255.
   - Interfaz - un adaptador de red de una máquina con una máscara de 255.255.255.255. No tiene que se necesariamente un adaptador del cortafuegos.
2. Escriba el nombre del objeto.
3. Escriba la descripción. Este campo es opcional.
4. Especifique una dirección IP decimal con puntos para este objeto.
5. Especifique una máscara de subred que indique los bits de la dirección para la comparación con la dirección del paquete IP.
6. Pulse en **Bien**.

Grupos de objetos de red

Un grupo representa un conjunto de objetos de red. Los grupos se utilizan para facilitar la configuración de las conexiones y pueden eliminar el trabajo repetitivo. Un ejemplo de ello sería agrupar varias direcciones, representadas individualmente por objetos de red, en un grupo de objetos de red para representar un departamento. Este departamento puede utilizarse como la dirección de origen o de destino de una conexión.

Para definir un grupo de objetos de red, seleccione Objetos de red en el árbol de navegación del cliente de configuración. Aparecerá el cuadro de diálogo **Objetos de red**. Efectúe una doble pulsación en **NUEVO GRUPO**. Aparecerá el cuadro de diálogo **Añadir un objeto de red**.

1. Escriba el nombre del grupo.
2. Escriba una descripción. Este campo es opcional.
3. Pulse en **Seleccionar** para seleccionar objetos para el grupo.
4. Pulse en **Bien**.

Sugerencia: Resulta muy conveniente englobar rangos de direcciones contiguas en un único objeto de red siempre que sea posible. Con ello mejorará el rendimiento del proceso de la norma de conexión. Se muestra en el ejemplo siguiente.

```
DEPARTAMENTO DE CONTABILIDAD
   Máquina de Jorge  191.1.10.1
   Máquina de Susana 191.1.10.3
   Máquina de Elena  191.1.10.5
   Máquina de Pedro  191.1.10.7
   Máquina de Juan   191.1.10.9
```

Para crear un objeto de red para este departamento de contabilidad, debe entrar la información de dirección IP para este grupo de la forma siguiente: 191.1.10.0 con una Máscara de subred de: 255.255.255.0. Este objeto de red, el departamento de contabilidad, puede utilizarse como el origen o el destino de una conexión.

Copia de seguridad de la configuración del cortafuegos

El cortafuegos almacena todos los archivos de configuración en `ROOTDIR\config`. Si quiere hacer una copia de seguridad de la configuración del cortafuegos sin hacer una copia de seguridad de todos los archivos del cortafuegos, haga una copia de seguridad de todos los contenidos del directorio `ROOTDIR\config`.

Si quiere restaurar una configuración del cortafuegos de la que se ha hecho una copia de seguridad, suprima todos los archivos existentes en el directorio `ROOTDIR\config` y a continuación restaure las versiones de las que se han hecho copias de seguridad de los archivos. Deberá regenerar y activar las normas de filtros antes de que la configuración restaurada tenga efecto.

Los archivos de configuración laves del cortafuegos se listan a continuación. Es posible que el directorio `\config` de su cortafuegos no contenga todos los archivos listados aquí. Tenga en cuenta que aunque la mayoría de archivos de configuración del cortafuegos son archivos de texto de muestra que se pueden ver con un editor de textos, **la edición manual de estos archivos no recibe soporte**.

- carriers.cfg - Definiciones del proveedor de telefonía del buscapersonas

- cfgfilt.output
- explode.cfg
- filters.active - Indica si el filtrado está activo
- fwadpt.cfg - Definiciones de interfaces de red
- fwconfig.map - Contiene nombres de archivos de configuración
- fwconns.cfg - Definiciones de conexiones de filtros
- fwfilters.cfg - Filtros activos actualmente
- fwhttp.cfg - Configuración del proxy HTTP
- fwmail.conf - Configuración de SafMail
- fwobjects.cfg - Definiciones de objetos de red
- fwpolicy.cfg - Opciones de política de seguridad
- fwrules.cfg - Definiciones de plantillas de normas de filtros
- fwservices.cfg - Definiciones de servicios
- fwsocks.cfg - Normas de Socks 5 del cliente de configuración
- fwtdefn.conf - Definiciones de alerta
- fwtpproxy.cfg - Definiciones de proxies transparentes
- fwusrdb.cfg - Base de datos de usuarios del cortafuegos
- logmgmt.cfg - Definiciones de archivado
- modems.cfg - Definiciones de módem
- pager.cfg - Definiciones de buscapersonas
- rcsfile.cfg - Parámetros del servicio de configuración
- Socks5.conf - archivo de configuración Socks 5 generado
- Socks5.header.cfg - Porciones suministradas por el usuario del Socks5.conf generado
- syslog.conf - Definiciones del recurso de registro

Capítulo 6. Gestión del Servicio de denominación de nombres

En este capítulo se explica cómo configurar el Servicio de denominación de dominios (DNS) en relación al IBM Firewall. la finalidad del DNS es proporcionar un completo servicio de denominación de dominios a los sistemas principales del interior de la red protegida y, al mismo tiempo, no proporcionar ninguna información a los sistemas principales del exterior de la red protegida. Esto permite a los usuarios del interior de la red protegida acceder a todos los servicios que Internet ofrece. Sin embargo, al denegarse la divulgación de información acerca de la red protegida, ello hace que resulte muy difícil que un intruso pueda localizar un sistema para atacarlo.

Para ello se necesitan tres servidores de denominación de dominios:

1. Uno en el IBM Firewall
2. Uno en el interior de la red protegida
3. Uno fuera de la red protegida

Consulte la Figura 10 para conocer el funcionamiento del DNS con el IBM Firewall.

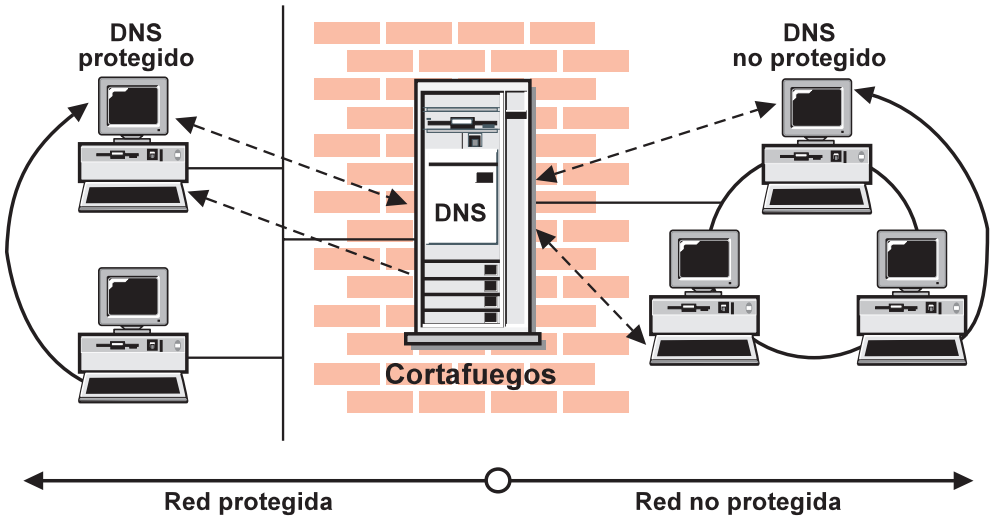

Figura 10. DNS

El cortafuegos se configura para actuar como pasarela entre el servidor o servidores de nombres de la red protegida y los que proporcionan servicio a la red no protegida. El término oficial que describe la función del cortafuegos es *servidor de nombres de sólo antememoria*, ya que el DNS del cortafuegos no contiene ningún archivo de bases de datos.

La Figura 10 muestra la función del cortafuegos. Cada vez que el cortafuegos necesita resolver un nombre para uso propio, pregunta a los servidores de nombres de la ubicación protegida. Cada vez que se reenvía una consulta al cortafuegos, éste reenvía la consulta a los servidores de nombres no protegidos.

Cuando un cliente de la red protegida solicita información de la ubicación protegida, éste envía su petición al DNS de la ubicación protegida, que responde.

Cuando el mismo cliente solicita información de la ubicación no protegida, éste envía la petición al mismo DNS de la ubicación protegida. Puesto que la consulta solicita información no protegida, el DNS de la ubicación protegida no puede responder, por ello, reenvía la consulta al cortafuegos. En caso de que un DNS no protegido fuera a reenviar una petición al cortafuegos, esa petición se reenviaría al dominio DNS no protegido, por lo tanto, y una vez más, no se divulgaría ninguna información sensible.

Configuración de DNS utilizando el cliente de configuración

Para configurar el DNS, seleccione Administración del sistema en el árbol de navegación del cliente de configuración. Efectúe una doble pulsación en el icono de la carpeta de archivos para ampliar la vista. Seleccione **Servicios de denominación de dominios**. El IBM Firewall visualiza la configuración actual del DNS, que puede modificarse.

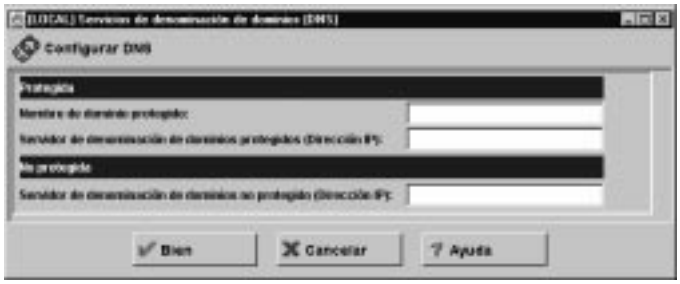

Figura 11. Servicio de denominación de dominios

Nota: Cuando añade DNS, el cortafuegos guarda y cambia el nombre de cualquier archivo de configuración del servicio de denominación de dominios existente.

1. El campo **Nombre de dominio protegido** identifica el nombre del dominio al que el cortafuegos añadirá cualquier nombre de sistema principal no cualificado.
2. El campo **Servidor de denominación de dominios protegidos** hace referencia al servidor que resuelve nombres y direcciones IP para los sistemas principales que el IBM Firewall protege de Internet. Puede especificar direcciones IP decimales con puntos, separadas por espacios.
3. El campo **Servidor de denominación de dominios no protegidos** hace referencia al servidor o servidores que le proporciona el proveedor de servicio para resolver la información acerca de la red no protegida. Puede especificar direcciones IP decimales con puntos, separadas por espacios.

Nota: Cuando se inicializa un servidor de nombres, éste envía una consulta para obtener la lista de los servidores de nombres del usuario raíz. La mayoría de las implementaciones retiene esta lista en la memoria. Sin embargo, la implementación de Microsoft vuelve a grabar esta lista en el archivo de configuración. Esto no modifica el comportamiento del servidor de nombres, pero cambiará los valores que se visualizarán en el campo **Servidor de nombres no protegidos**. Esto no es motivo de preocupaciones.

Configuración del servidor de nombres protegidos

El servidor de nombres protegidos debe configurarse para reenviar consultas no resueltas al cortafuegos. Si tiene implementaciones BIND estándar, añada una sentencia *forwarders* y una sentencia *cache* al archivo *boot* del servidor de nombres protegidos:

```
forwarders      aaa.bbb.ccc.ddd
cache           .               named.cache
```

Cree el archivo "cache", *named.cache*, para que señale al cortafuegos:

```
. 99999999 IN NS firewall.private.com
firewall.private.com   99999999 IN A aaa.bbb.ccc.ddd
```

donde *private.com* es el nombre de dominio que se utiliza de la ubicación protegida y *aaa.bbb.ccc.ddd* es la dirección IP del cortafuegos.

Además, puede que desee añadir el nombre del sistema principal del cortafuegos a las bases de datos DNS. De esta forma, los usuarios pueden acceder al servidor Socks del cortafuegos, proxy HTTP, proxy Telnet y proxy FTP utilizando el nombre del sistema principal del cortafuegos en lugar de su dirección IP. Esto requiere dos pasos adicionales, como se describe en el *Capítulo 4* de *DNS y BIND*. Consulte la *Bibliografía* para obtener más detalles acerca de este manual.

Primero añada un registro A al archivo de bases de datos de dominios:

```
firewall.private.com     IN A aaa.bbb.ccc.ddd
```

A continuación, añada un registro PTR al archivo de consulta invertida:

```
ddd.ccc.bbb.aaa.in-addr.arpa.     IN PTR   firewall.private.com.
```

Si no utiliza el DNS para la red protegida, el cortafuegos todavía debe ser capaz de resolver su propia información. Configure el cortafuegos como se describe para su configuración normal, pero liste la interfaz protegida del cortafuegos en el campo **Servidor de nombres protegidos**. A continuación, añada la línea siguiente a `c:\winnt\system32\dns\boot`.

```
primary ccc.bbb.aaa.in-addr.arpa c:\winnt\system32\dns\fwnamed.rev
```

A continuación, cree *fwnamed.rev* de forma que sea similar al siguiente:

```
ccc.bbb.aaa.in-addr.arpa  IN SOA firewall.private.com. root.public.com. (
                          9        ; Serie
                          86400    ; Renovar después de 1 día
                          300      ; Reintentar transcurridos 5 minutos
                          654000   ; Caduca en 1 semana
                          3600  )  ; TTL mínimo de 1 día
ccc.bbb.aaa.in-addr.arpa.          IN NS    firewall.private.com.
ddd.ccc.bbb.aaa.in-addr.arpa.      IN PTR   firewall.private.com.
```

Configuración de los clientes de configuración

Los clientes de la red protegida deben configurarse para enviar sus consultas al servidor de nombres protegidos, no al cortafuegos. Esto es importante porque garantiza que no se almacenará ninguna información de la ubicación protegida en la antememoria incorporada del cortafuegos. Además, ahorra carga de trabajo en el cortafuegos, pues el cortafuegos no se implicará a menos que una consulta conlleve el reenvío de una consulta desde la ubicación protegida a la ubicación no protegida.

Si no utiliza el DNS para la red protegida, los clientes tendrán que señalar al cortafuegos como su servidor de nombres.

Publicación de servicios al público

Muchas organizaciones desea publicar servicios particulares al público de Internet. Con frecuencia, estos servicios incluyen servidores de correo electrónico y de Webs, aunque puede utilizarse cualquier tipo de servidor TCP/IP. Para que tales servicios estén disponibles, no sólo debe colocar el servidor en la red que permite el acceso al mismo, sino que debe listar ese servidor con el DNS público para que los usuarios puedan obtener la información correcta.

Existen dos formas de hacerlo. O bien el proveedor de servicio listará sus servidores como parte de su dominio (y, por lo tanto, en sus servidores de nombres) o deberá proporcionar su propio servidor de nombres y registrarlo con Internet. Resulta mucho más fácil que sea el Proveedor de servicio de Internet (ISP) el que se encargue de proporcionar este servicio. Si puede elegir esta opción, será necesario que les proporcione los nombres de los sistemas principales y direcciones IP que desea que se listen. Por ejemplo, si su servidor de la web público funciona como *www.public.com* y su dirección IP es *50.100.150.200*, deberá solicitar a su ISP que liste *www.public.com en 50.100.150.200*.

Además, si desea recibir correo electrónico, deberá solicitar a su ISP que liste su cortafuegos como programa de *intercambio de correo* para su dominio de correo electrónico público. El ISP necesita saber el nombre del sistema principal *(pasarela.public.com)*, su dirección IP *(50.100.150.201)* y el nombre de dominio que desea utilizar para recibir correo electrónico *(public.com)*.

Si su ISP no desea encargarse de proporcionar estos servicios, tendrá que hacerlo personalmente. Nuevamente, aquí tiene dos opciones. Puede colocar un servidor DNS en su DMZ o puede utilizar el cortafuegos como ese servidor de nombres. La utilización del cortafuegos no implica riesgos adicionales de seguridad porque los archivos de bases de datos que colocará aquí no contienen ninguna información acerca de su red protegida. La única información que se almacenará estará relacionada con los servicios públicos que elija ofrecer.

Los detalles que implica la configuración de un servidor DNS se explican en el capítulo 4 de *DNS y BIND*, que se listan en la *Bibliografía*. La lectura de ese capítulo se recomienda especialmente, y los capítulos anteriores, si fuera necesario. La configuración de un servidor DNS no es una tarea fácil y, con frecuencia, es mejor que se encarguen de ello expertos. Si puede disponer de un experto con esas características, considere seriamente beneficiarse de su experiencia y conocimientos.

Consulte el “Configuraciones de muestra” en la página 35 para obtener más información.

Instalación del Servidor DNS de Microsoft

Para instalar el Servidor DNS de Microsoft, diríjase al panel de control, pulse en **Red**, pulse en la **pestaña Servicios**, pulse en **Añadir** y seleccione **Servidor DNS de Microsoft**. Necesitará el CD-ROM de instalación.

Resolución de problemas de DNS

El manual *IBM eNetwork Firewall - Manual de consulta* contiene un capítulo dedicado a la resolución de problemas del cortafuegos. En ese capítulo, existe un apartado específico para los problemas de DNS. Ese apartado proporciona sugerencias para la utilización del mandato *nslookup* para identificar el segmento erróneo del sistema DNS.

Configuraciones de muestra

Esta sección ilustra algunas configuraciones de muestra en las que se podría utilizar un cortafuegos. La mayoría de estos ejemplos se centran en la configuración necesaria para el funcionamiento de DNS. Es poco probable que uno de estos ejemplos ilustre su red, así que intente comprender cada ejemplo y aplicar los conceptos adecuados a su instalación particular.

Ejemplo 1: Servidor DNS en un DMZ de una interfaz no protegida

El primer ejemplo ilustra los archivos necesarios para utilizar el servidor de nombres en un DMZ ubicado dentro de la red no protegida, como se muestra en Figura 12.

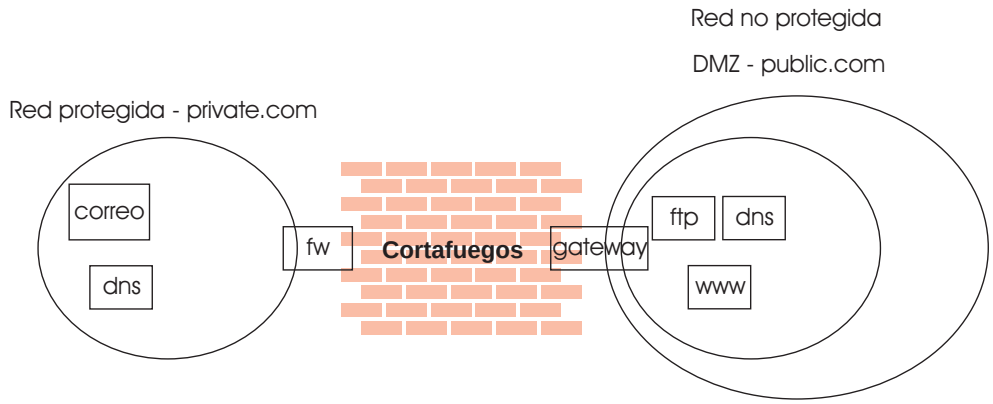

Figura 12. Servidor de nombres en una DMZ dentro de una red no protegida

Esta figura ilustra una red privada, *private.com*, detrás de un IBM Firewall cuya interfaz protegida se llama *fw.private.com* y cuya interfaz no protegida se llama *gateway.public.com*. El DMZ de la empresa está conectado a una interfaz no protegida y contiene un servidor de nombres *dns.public.com*, un servidor FTP *ftp.public.com*, y un servidor web *www.public.com*. Los archivos de *dns.public.com* para aplicar este escenario son los siguientes:

db.public

```
public.com.   IN SOA dns.public.com. admin.public.com.  (
                 1           ; número de serie
                 10800       ; renovar cada 3 horas
                  3600        ; reintentar después de 1 hora
                 604800      ; caduca en 1 semana
                 86400 )     ; TTL mínimo de 1 día
;
; Servidores de nombres
;
public.com           IN NS  dns.public.com.
;
; Sistemas principales en DMZ
;
dns.public.com.      IN A 50.100.150.202
gateway.public.com.  IN A 50.100.150.201
www.public.com.      IN A 50.100.150.200
ftp.public.com.      IN A 50.100.150.203
;
; Entradas relacionadas con el correo
;
public.com.          IN MX  0  gateway.public.com.
public.com.          IN CNAME gateway.public.com.
```

db.50.100.150

```
150.100.50.in-addr.arpa.   IN SOA dns.public.com. admin.public.com.  (
                 1           ; número de serie
                 10800       ; renovar cada 3 horas
                 3600        ; reintentar después de 1 hora
                 604800      ; caduca en 1 semana
                 86400 )     ; TTL mínimo de 1 día
202.150.100.50.in-addr.arpa.      IN NS dns.public.com.
203.150.100.50.in-addr.arpa.      IN PTR  ftp.public.com.
202.150.100.50.in-addr.arpa.      IN PTR  dns.public.com.
201.150.100.50.in-addr.arpa.      IN PTR  gateway.public.com.
200.150.100.50.in-addr.arpa.      IN PTR  www.public.com.
```

db.127.0.0

```
0.0.127.in-addr.arpa.   IN SOA dns.public.com. admin.public.com.  (
                 1           ; número de serie
                 10800       ; renovar cada 3 horas
                 3600        ; reintentar después de 1 hora
                 604800      ; caduca en 1 semana
                 86400 )     ; TTL mínimo de 1 día
0.0.127.in-addr.arpa.   IN NS  dns.public.com.
1.0.0.127.in-addr.arpa.   IN PTR localhost.
```

db.cache

La mejor opción para este archivo es realizar un FTP de la lista de servidores de nombres root actuales de *ftp://ftp.rs.internic.net/domain/named.root*.

boot

```
primary public.com                  db.public
primary 150.100.50.in-addr.arpa     db.50.100.150
primary 0.0.127.in-addr.arpa        db.127.0.0
cache   .                           db.cache
```

Para establecer el filtro de tráfico para permitir el tráfico de DNS adecuado, habilite *Permitir Consultas de DNS* en el panel **Política de seguridad**.

Ejemplo 2: DNS en un DMZ en una interfaz dedicada

En el segundo ejemplo, el DNS del DMZ aún está en un servidor de nombres dedicado, pero esta vez el DMZ está conectado a una interfaz diferente en vez de la misma interfaz que la red no protegida.

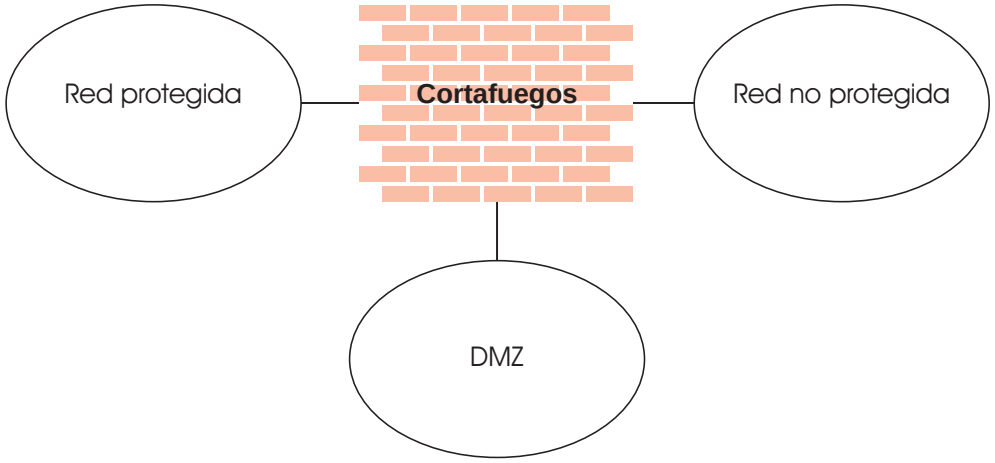

Figura 13. DNS en un DMZ en una interfaz dedicada

Los archivos de datos de DNS de *dns.public.com* son los mismos que el ejemplo anterior. Para hacer que el servidor de nombres sea accesible a la red pública, sin embargo, hace falta abrir el filtro de tráfico o llevar a cabo una transferencia de zona para copiar los archivos de datos en el cortafuegos.

Para abrir el filtro de tráfico, copie las tres plantillas de normas tituladas *Consultas del servidor DNS*, *Respuestas de DNS*, y *Consultas de clientes DNS*. Cambie los valores de direccionamiento de cada norma de *local* a *routed*. A continuación incluya las tres nuevas plantillas de normas de un servicio y establezca los indicadores de flujo de la siguiente manera:

- Consultas de clientes de DNS: --->
- Respuestas de DNS: <---
- Consultas del servidor de DNS: --->
- Consultas del servidor de DNS: <---

Incluya este servicio en una conexión que utilice *El mundo* como objeto de origen y *dns.public.com* como objeto de destino.

Para llevar a cabo una transferencia de zona, deberá establecer el filtro de tráfico y dar instrucciones a los servidores de nombres para que copien los archivos adecuados. Para establecer el filtro de tráfico:

1. En el panel **Política de seguridad**, habilite *Permitir consultas DNS*.
2. Añada una conexión desde *dns.public.com* (objeto de origen) a la interfaz DMZ del cortafuegos (objeto de destino), que incluye el servicio titulado *Transferencias de DNS*.

Para activar la transferencia de zona, añada las siguientes líneas al archivo *boot* del cortafuegos en `c:\winnt\system32\dns`:

```
secondary public.com     50.100.150.202 db.public
secondary 150.100.50.in-addr.arpa  50.100.150.202 db.50.100.150
```

A continuación vaya al Gestor del control de servicios y detenga y reinicie el servicio del Servidor DNS.

Ejemplo 3: Uso del cortafuegos como el Servidor de nombres protegido

Para utilizar el cortafuegos como su servidor de nombres protegido, sitúe los archivos de la base de datos que normalmente residirían en el servidor protegido del cortafuegos. A continuación sus clientes pueden apuntar al cortafuegos como su servidor de DNS. Los riesgos asociados con este enfoque son que el servidor de DNS no puede diferenciar una petición del lado protegido de una petición del lado no protegido. Por lo tanto, proporcionará esta información del lado protegido a cualquier cliente que la pida; ya no podrá ocultar su información de DNS protegida.

Para aplicar este enfoque, empiece por la configuración del recurso de DNS del cortafuegos utilizando el cliente de configuración. Para el campo *Nombre de dominio protegido*, liste el nombre de dominio que utilizará en su red protegida. Para el *Servidor de nombres protegido*, liste la interfaz protegida del cortafuegos. Para el *Servidor de nombres no protegido*, liste el servidor de nombres proporcionado por su ISP, como siempre. A continuación debe crear un archivo de consulta inversa en el cortafuegos para complementar esta configuración.

Cree el archivo `c:\winnt\system32\dns\fwnamed.rev` para que se parezca al siguiente ejemplo.

Para este ejemplo, la interfaz protegida del cortafuegos se denomina *fw.private.com* y su dirección IP es *10.100.100.1*.

```
100.100.10.in-addr.arpa.   IN SOA fw.private.com. admin.fw.private.com. (
                  1           ; número de serie
                  10800       ; renovar cada 3 horas
                  3600        ; reintentar después de 1 hora
                  604800      ; caduca en 1 semana
                  86400 )     ; TTL mínimo de 1 día
1.100.100.10.in-addr.arpa.         IN NS fw.private.com.
1.100.100.10.in-addr.arpa.         IN A  fw.private.com.
```

A continuación añada la siguiente línea a `c:\winnt\system32\dns\boot`:

```
primary 100.100.10.in-addr.arpa     fwnamed.rev
```

En este escenario sus cliente deben estar configurados para indicar el cortafuegos (10.100.100.1) como su servidor de DNS. Su cortafuegos le asistirá en la resolución de información externa, pero no habrá ninguna resolución de la información del lado protegido. Esto significa que los clientes del lado protegido que quieran conectarse al servidor de configuración o a cualquiera de los servidores proxy del cortafuegos debe consultar el cortafuegos por dirección IP, no por el nombre del servidor.

Capítulo 7. SafeMail

La pasarela SafeMail del IBM Firewall proporciona una pasarela para el tráfico SMTP. Retransmite los mensajes del servidor o servidores de correo protegido a la ubicación no protegida, ocultando los nombres de los dominios sensibles en su trayectoria. Retransmite los mensajes de la ubicación no protegida al dominio de correo protegido y aísla la red protegida de ataques.

Aunque SafeMail no realiza protección del contenido, SafeMail proporciona una salida de usuario a través de la cual puede realizarse la protección del contenido. Para obtener más información, consulte el “Salida de usuario de SafeMail” en la página 41.

SafeMail retransmite los mensajes en tiempo real desde el emisor al receptor. Con ello se evitan los riesgos y la complejidad que implica el mantenimiento de una cola de mensajes en el Cortafuegos. Esto necesita determinados requisitos de configuración en los dominios de correo adyacentes. En algunos casos, estos requisitos no podrán aplicarse a una instalación en particular. Si así fuera, puede adquirirse cualquiera de los diversos servidores SMTP por separado e instalarlo en lugar de SafeMail. Si opta por instalar un servidor totalmente SMTP, configúrelo pensando en la seguridad. Consulte el “Utilización de un servidor SMTP en lugar de SafeMail” en la página 42 para obtener más información.

Configuración de SafeMail utilizando el cliente de configuración

Para configurar el SafeMail, seleccione Administración del sistema en el árbol de navegación del cliente de configuración. Efectúe una doble pulsación en el icono de la carpeta de archivos para ampliar la vista. Seleccione **SafeMail**. El IBM Firewall visualizará la lista de servidores de correo y dominios configurados. Deberá configurar una entrada para cada dominio de correo de la ubicación privada que esté configurándose.

1. Para añadir un dominio, seleccione **NUEVO** y pulse en **Abrir**. Aparecerá el cuadro de diálogo **Añadir servidor de correo**.
2. El campo **Nombre de dominio protegido** contiene el nombre por el que los usuarios de la ubicación protegida del cortafuegos conocen al dominio de correo que está describiéndose.
3. El campo **Nombre de servidor de correo protegido** contiene el nombre del sistema principal o la dirección IP decimal con puntos del servidor de correo al que se aplica esta entrada. Este servidor debe encontrarse en una de las redes protegidas. Sólo podrá listar un único servidor de correo para un dominio determinado.
4. El campo **Nombre de dominio público** contiene el nombre por el que los usuarios de la ubicación no protegida del cortafuegos conocen al dominio de correo que está describiéndose. Este nombre sustituirá al nombre de dominio protegido para ocultar la topografía de la red protegida.
5. Pulse en **Bien**.

Cambio de una entrada de la configuración del correo

Para cambiar una entrada de la configuración del correo, seleccione una entrada de la lista y pulse en **Abrir**. Aparecerá el cuadro de diálogo **Cambiar configuración de servidor de correo**.

El campo **Nombre de dominio protegido** está inhabilitado, pero puede cambiar los demás campos, como se describe en el apartado “Configuración de SafeMail utilizando el cliente de configuración” en la página 39.

Notas:

1. Si había configurado anteriormente el SafeMail y especifica aquí un servidor de correo protegido, este servidor de correo sustituirá al que había configurado previamente.
2. Si anteriormente *no* ha configurado SafeMail y especifica aquí un servidor de correo protegido, este servidor de correo se añadirá a la configuración.

Supresión de una entrada de la configuración del correo

Para suprimir una entrada de la configuración de SafeMail, seleccione una entrada de la lista y pulse en **Suprimir**. Antes de realizarse la supresión, recibirá un aviso. Pulse en **Bien** para suprimirla o en **Cancelar** si ha cambiado de idea.

Configuración de los servidores protegidos

Deberá configurar los servidores de correo protegido para que el Cortafuegos se liste como su pasarela para los dominios desconocidos. Esto dará lugar a que el correo destinado a la red no protegida se reenvíe al Cortafuegos. Adicionalmente, cada servidor deberá configurarse para aceptar los mensajes dirigidos a su nombre de dominio público además de a su nombre de dominio privado. Cuando el Cortafuegos reenvíe una nota desde la red no protegida, todos los destinatarios aparecerán listados con sus nombres de dominio de la ubicación pública.

Si tiene más de un dominio de correo distinto en el interior de la red protegida, también deberá configurar cada servidor para el reenvío del correo destinado a otro dominio de la ubicación protegida directamente a ese servidor, no a través del Cortafuegos. Esto libera al Cortafuegos de cargas de trabajo innecesarias y permite que el mecanismo de entrega en tiempo real del Cortafuegos funcione correctamente.

Configuración del dominio público

La única configuración necesaria en la red no protegida es hacer que el Cortafuegos se liste como el elemento para el intercambio de correo de la red. Solicite a su proveedor de servicio que añada la información necesaria a sus servidores DNS. Consulte Capítulo 6, “Gestión del Servicio de denominación de nombres” en la página 31 para obtener detalles específicos adicionales que se necesitan para este procedimiento.

El objetivo es listar el Cortafuegos como el elemento para el *intercambio de correo* para cada nombre de dominio público para el que desea aceptar correo. Por ejemplo, si utiliza el nombre de dominio *private.com* en el interior de la red protegida y *public.com* en el exterior de la red protegida, podría denominar al

cortafuegos *gateway.public.com*. En este caso, deberá solicitar a su proveedor que liste el nombre del sistema principal y la dirección IP del Cortafuegos como sistema principal (que normalmente se listará con los registros "A" y los registros "PTR"). A continuación, puesto que desea aceptar el correo dirigido a *usuario@public.com*, deberá solicitar a su proveedor que añada un registro MX para el dominio *public.com* que lista *gateway.public.com* como el elemento para el intercambio de correo para ese dominio. Si también desea recibir el correo dirigido a *usuario@otracosa.com*, puede listar un registro MX adicional que también señale al Cortafuegos.

Salida de usuario de SafeMail

SafeMail proporciona una salida de usuario mediante la que una instalación puede adaptar SafeMail para rechazar el tráfico potencialmente negativo. Consulte el manual *IBM eNetwork Firewall - Manual de consulta* para obtener una descripción completa del Software Developers Kit proporcionado este fin.

Esta característica le permite crear una función, *UsrCheck()*, que se llama cada vez que SafeMail recibe un paquete del emisor. La función recibe una estructura que contiene varios campos relacionados con el estado del sistema. Esta estructura incluye un ID de sesión exclusivo, las direcciones IP de los servidores emisores y receptores, indicadores para los mandatos anteriormente recibidos y un almacenamiento intermedio de texto normal que contiene el paquete que está analizándose.

Algunos de los tipos de comprobaciones que pueden implementarse en esta función son:

- listas de sistemas principales de *cabecera*
- exploración de secuencias de caracteres no permitidas, como la utilización de un lenguaje no apropiado o nombres de códigos de proyectos
- examen de las series entrecomilladas intercaladas
- restricciones de longitud de mensajes

Si se desea, la salida de usuario también puede utilizarse para implementar una interfaz a un producto de protección de contenido de otro proveedor.

Si la función de salida de usuario decide que un mensaje no debe procesarse, la función devuelve un código de razón nuevamente a SafeMail. SafeMail inmediatamente rechazará la conexión con el servidor SMTP emisor. Al mismo tiempo. se grabará un mensaje en el registro del cortafuegos, incluyendo el código de razón que ha devuelto la salida de usuario.

Cuando se escriba una salida de usuario, recuerde que esta función se llamará para cada paquete recibido. Escríbala de la forma más eficaz posible; con ello evitará un impacto negativo en el rendimiento del sistema. Recuerde también que esta función se ejecutará en un entorno de varias hebras y, por lo tanto, debe escribirse de forma que ofrezca seguridad a las hebras. Puede escribir la salida de usuario con cualquier compilador que dé soporte a la operación de varias hebras y puede utilizar el convenio de enlaces *_cdecl*. Se proporcionan ejemplos de makefiles para IBM Visual Age C++ y para Microsoft Visual C++.

Utilización de un servidor SMTP en lugar de SafeMail

Inhabilitación de SafeMail

Para inhabilitar SafeMail para evitar conflictos con otro producto de servidor SMTP, inhabilite el servicio SafeMail en el **Gestor de controles de servicios**. Desde el menú **Inicio** de Windows, seleccione **Configuración, Panel de control, Servicios**. Desplácese para seleccionar *Servidor SafeMail del Firewall*. Pulse en **Inicio**. En el campo **Tipo de inicio**, seleccione **Inhabilitado**. Pulse en **Bien**.

Configuración de un servidor SMTP

Al instalar un servidor totalmente SMTP en lugar de SafeMail debe considerar varios aspectos. En este apartado se describen las funciones de seguridad de SafeMail, en un intento de permitirle configurar el servidor SMTP para que realice funciones similares. Puede que determinados productos de servidor SMTP no puedan realizar algunas de estas tareas, por lo tanto, estudie las opciones disponibles y sus necesidades cuidadosamente antes de adquirir un producto.

Existen algunos ataques que intentan desbordar o dañar la cola del correo. Aunque ningún servidor que se precie puede funcionar sin una cola de correo, los riesgos que se asocian a la cola de correo se reducen si se puede dedicar un volumen del disco exclusivamente a esa tarea. Con ello se minimizan las posibilidades de que una cola desbordada pueda influir en las otras operaciones del cortafuegos.

También es importante que el servidor de correo oculte la información de la red protegida. De acuerdo con las normas del SMTP, cada servidor que reenvía correo debe insertar una línea de cabecera *Recibido:*. Estas líneas de cabecera puede utilizarlas un intruso para correlacionar la red protegida. SafeMail desmantela todas estas cabeceras cuando procesa una nota; configure el servidor SMTP para que haga lo mismo. Además, SafeMail vuelve a grabar todos los nombres de sistemas principales de la ubicación privada en el nombre de dominio público. Con ello se elimina todavía más información que podría utilizarse para correlacionar la red.

Ejemplo de salida del registro para SafeMail

El siguiente es un ejemplo de la salida del registro para SafeMail.

```
Feb 03 13:46:11 1998 mr16n18: ICA2163i: Iniciado safemaild.

Feb 03 13:41:14 1998 mr16n18: ICA2177i: Conexión SafeMail 0xd71e7a19
recibida de RACK3BD.
Feb 03 13:41:21 1998 mr16n18: ICA2179i: SafeMail ha reenviado 215575
bytes para la conexión 0xd71e6118 de 9.67.144.52 a 9.67.131.250.
Feb 03 13:41:21 1998 mr16n18: ICA2178i: La sesión SafeMail 0xd71e7a19
se ha establecido desde 9.67.144.52 a 9.67.131.250.
Feb 03 13:41:23 1998 mr16n18: ICA2177i: Conexión SafeMail 0xd71e831a
recibida de RACK3BD.
Feb 03 13:41:36 1998 mr16n18: ICA2177i: Conexión de SafeMail 0xd71e901b
recibida de RACK3BD.
Feb 03 13:41:56 1998 mr16n18: ICA2179i: SafeMail ha reenviado 215567
bytes para la conexión 0xd71e7a19 de 9.67.144.52 a 9.67.131.250.
Feb 03 13:41:56 1998 mr16n18: ICA2178i: La sesión SafeMail 0xd71e831a
se ha establecido desde 9.67.144.52 a 9.67.131.250.
Feb 03 13:41:56 1998 mr16n18: ICA2178i: La sesión SafeMail 0xd71e901b
se ha establecido desde 9.67.144.52 a 9.67.131.250.
Feb 03 13:41:57 1998 mr16n18: ICA2179i: SafeMail ha reenviado 346
bytes para la conexión 0xd71e901b de 9.67.144.52 a 9.67.131.250.
Feb 03 13:41:57 1998 mr16n18: ICA2179i: SafeMail ha reenviado 358
bytes para la conexión 0xd71e831a de 9.67.144.52 a 9.67.131.250.
```

Los mensajes de registro indican lo siguiente:

- ICA2177 - indica el inicio de una nueva conexión.
- ICA2179 - indica una terminación satisfactoria.
- ICA2178 - indica que se ha establecido contacto con el servidor SMTP receptor.
- ICA2181 - indica que SafeMail ha rechazado la sesión. Consulte en el manual *IBM eNetwork Firewall - Manual de consulta* los códigos de causas.
- ICA2180 - indica el final de la sesión.
- ICA2182 - indica que la salida de usuario ha decidido que la sesión debe rechazarse.

Capítulo 8. Control del tráfico a través del cortafuegos

En este capítulo se explica cómo utilizar el cliente de configuración para controlar el tráfico de la red a través del cortafuegos. Mediante la utilización de filtros especiales, el cortafuegos filtra los paquetes a nivel de sesión basándose en varios criterios, como la hora, la dirección IP y la subred. El filtro actúa entre las interfaces de red protegida y no protegida. No influyen en las tablas de direccionamiento del cortafuegos.

Como valor por omisión, el cortafuegos no permite que fluya ningún tráfico entre la red protegida y la red no protegida. Para que tipos específicos de tráfico puedan fluir entre las redes protegidas y no protegidas deben crearse conexiones.

Utilización del cliente de configuración para crear conexiones

Debe utilizar los componentes del cliente de configuración que aparecen enFigura 14 en la página 46 para crear objetos de red, plantillas de normas, servicios y conexiones.

Conexiones Asocian los objetos de red a servicios y/o plantillas de socks para definir los tipos de comunicaciones permitidos entre puntos finales. Cada conexión define un tipo específico de tráfico IP permitido o denegado entre un objeto de red de origen y de destino.

Servicios Se componen de una o más plantillas de normas. Define el tipo de tráfico IP permitido o denegado entre un objeto de origen y de destino. Por ejemplo, puede crear un servicio para permitir Telnet o denegar Ping. (Uno de los servicios FTP se compone de ocho plantillas de normas). El IBM Firewall se entrega con un conjunto de servicios por omisión. No puede suprimir estos servicios por omisión previamente cargados, pero sí puede modificar determinados campos. Sin embargo, si estos servicios predefinidos no se ajustan a sus necesidades, puede realizar adiciones a los servicios utilizando las plantillas de normas para crear nuevas normas. Consulte el apartado “Definición de los servicios” en la página 65 para obtener más información.

Plantillas de normas Proporcionan instrucciones al cortafuegos para permitir o denegar paquetes IP basándose en sus diversos atributos.

Plantillas de socks Proporcionan instrucciones al daemon socks del cortafuegos basándose en sus diversos atributos.

Objetos de red Representan los diversos componentes, como los sistemas principales, usuarios y subredes, que interactúan con el cortafuegos. Se definen mediante una dirección IP y una máscara de dirección, por ello es posible que un objeto represente a todo un rango de direcciones de red. Los objetos de red pueden agruparse.

Grupos de objetos de red

Representan uno o más objetos de red. Se utilizan para facilitar la configuración de las conexiones y pueden eliminar el trabajo repetitivo. Un ejemplo sería agrupar varias direcciones en un grupo de objetos de red para representar un departamento. Este grupo de objetos de red puede utilizarse entonces como el origen o el destino de una conexión.

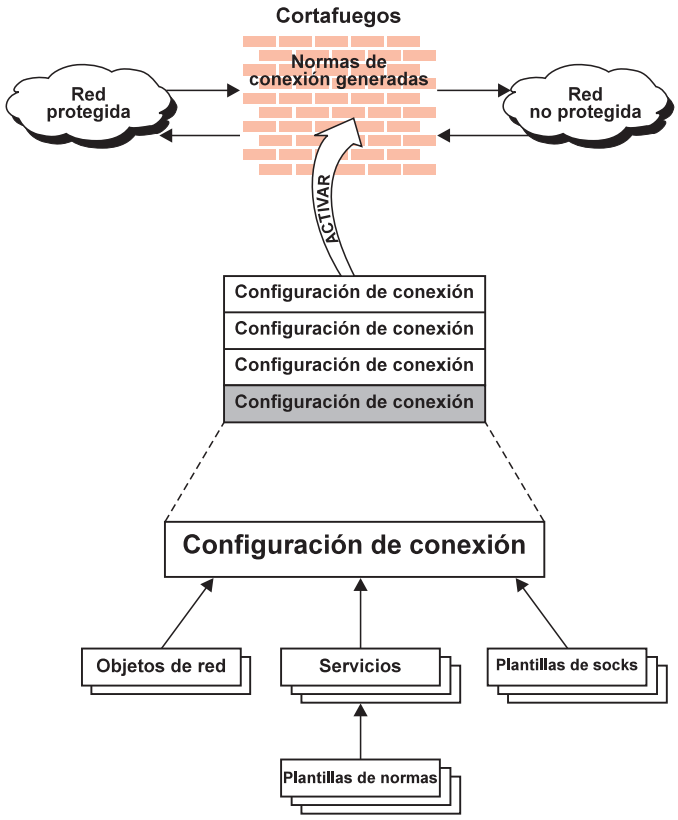

Figura 14. Creación de conexiones

Creación de conexiones utilizando los servicios predefinidos

Para permitir o denegar tipos específicos de comunicaciones entre dos objetos de red o grupos de objetos de red específicos que sirven como puntos finales, debe crear una conexión.

Tras haber definido los objetos de red, el paso siguiente es crear las conexiones. Seleccione el objeto de red o grupo que va a ser el origen y el objeto de red o grupo que va a ser el destino del flujo del tráfico a través del cortafuegos.

Para crear una conexión, seleccione Control del tráfico en el árbol de navegación del cliente de configuración y efectúe una doble pulsación en el icono de la carpeta de archivos para ampliar la vista. Seleccione **Configuración de la conexión**. Aparecerá el cuadro de diálogo **Lista de conexiones**. Seleccione **NUEVA** y pulse en **Abrir**. Aparecerá el cuadro de diálogo **Añadir una conexión**, como se muestra en la Figura 15 en la página 47.

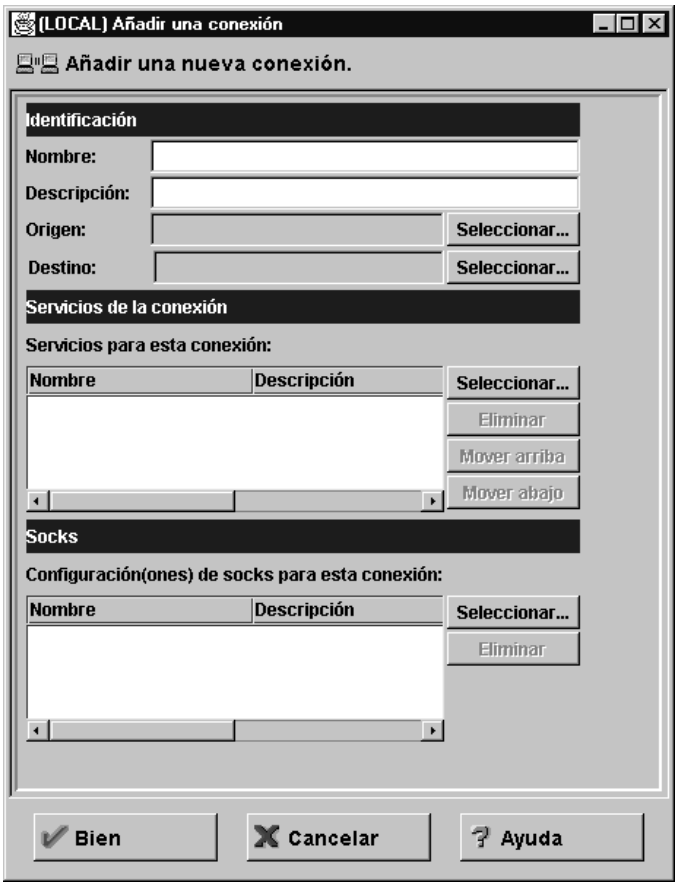

Figura 15. Añadir una conexión

1. Especifique un nombre para la conexión.
2. Escriba una descripción de la conexión.
3. Para el campo de origen, pulse en **Seleccionar** y elija un objeto de red de la lista del diálogo **Objeto de red**.
4. Para el campo de destino, pulse en **Seleccionar** y elija un objeto de red de la lista del diálogo **Objeto de red**.
5. Para elegir los servicios para esta conexión, pulse en **Seleccionar** y elija el tipo de tráfico que desea controlar entre los puntos finales.
6. Elija uno o más servicios de la lista para añadir el servicio a la Conexión.
7. Puede reordenar la lista seleccionando un servicio y pulsando en **Mover arriba** o **Mover abajo**. Consulte “Orden de las conexiones” en la página 48.
8. Puede eliminar un servicio seleccionándolo y pulsando en **Eliminar**.
9. Utilice **Configuración de socks para esta conexión**. Siga los pasos 5 a 7 para realizar las conexiones para Socks.
10. Tras haber completado las definiciones, pulse en **Bien**.
11. Active todas las conexiones. Consulte “Activación de la conexión” en la página 48.

Orden de las conexiones

La mayoría de los usuarios del IBM Firewall tienen menos de 1000 normas. Cuantas más normas se tengan, mayor será el impacto en el rendimiento.

Cuando se recibe un paquete en una interfaz de red, tanto si procede como si se dirige al sistema principal del cortafuegos, se aplican las normas, empezando desde el principio de las normas de conexión generadas. Cuando la información del paquete coincide exactamente con la información de una norma, se realiza la acción (permitir o denegar). Si se busca en la totalidad del archivo y no se encuentra ninguna coincidencia, la petición se deniega.

Sugerencia: Coloque las conexiones más específicas hacia el principio y las conexiones menos específicas hacia del final. Por ejemplo, podría tener un Departamento ABC, con una dirección de (1.1.10.X) y una máquina que se utiliza como servidor dentro del Departamento ABC, con una dirección de (1.1.10.7). Si desea excluir la máquina 1.1.10.7 porque es un servidor que no debe utilizarse para el tráfico telnet, debe colocar la conexión `Denegar telnet para servidor de Dept ABC` antes que las conexiones `Permitir telnet para Dept ABC`. Si invierte el orden de las conexiones, la conexión de tipo denegar nunca se encontrará.

Activación de la conexión

Nota: **Antes de activar las conexiones, asegúrese de que la interfaz protegida se haya definido**.

Seleccione **Activación de la conexión** en el árbol de navegación del cliente de configuración para realizar cualquiera de las acciones siguientes:

Regenerar y activar normas de conexión El cortafuegos crea las normas de conexión generadas a partir de la configuración de la conexión y activa ese conjunto de normas.

Desactivar normas de conexión El cortafuegos ahora está protegido por las normas por omisión.

Listar normas actuales de la conexión Verá el conjunto más reciente de las normas de conexión generadas. Si anteriormente ha desactivado normas, no estarán utilizándose.

Validar generación de norma Las normas que ha creado son válidas o no válidas.

Habilitar registros de normas de conexión El cortafuegos registra el tráfico seleccionado en el recurso `registro del cortafuegos`.

Inhabilitar registro de normas de conexión Detiene el registro del cortafuegos.

Aparecerá el cuadro de diálogo**Activación de la conexión** como se muestra en la Figura 16 en la página 49.

Figura 16. Activación de la conexión

Tras realizar una selección, pulse en **Ejecutar**.

Ejemplo de salida del registro cuando se regeneran y activan normas de conexión

El siguiente es un ejemplo de la salida del registro cuando se regeneran y activan normas de conexión.

```
Feb 03 13:46:53 1998 mr16n18: ICA9037i: Las interfaces del
cortafuegos están actualizándose
automáticamente el jueves 3 Feb  13:46:53 1998.

Feb 03 13:46:55 1998 mr16n18: ICA1032i: Las normas de filtros se
han actualizado a las
13:46:55 del 03 de Feb de 1998

Feb 03 13:46:55 1998 mr16n18: ICA1037i: #:1 permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
udp eq  53 eq 53 both local both l=n f=y t=0 e=none a=none
Feb 03 13:46:55 1998 mr16n18: ICA1037i: #:2 permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
udp gt  1023 eq 53 both local both l=n f=y t=0 e=none a=none
Feb 03 13:46:55 1998 mr16n18: ICA1037i: #:3 permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
udp eq  53 gt  1023 both local both l=n f=y t=0 e=none a=none
Feb 03 13:46:55 1998 mr16n18: ICA1037i: #:4 permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
tcp     gt  1023 eq 25 both local both l=y f=y t=0 e=none a=none
Feb 03 13:46:55 1998 mr16n18: ICA1037i: #:5 permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
tcp/ack eq  25 gt 1023 both local both l=y f=y t=0 e=none a=none
Feb 03 13:46:55 1998 mr16n18: ICA1037i: #:6 permit 9.67.144.49 255.255.255.240
9.67.130.154 255.255.248.0 all any 0 any 0 both both both l=y f=y t=0 e=none a=none
Feb 03 13:46:55 1998 mr16n18: ICA1037i: #:7 permit 9.67.130.154 255.255.248.
0 9.67.144.49 255.255.255.240 all any 0 any 0 both both both l=y f=y t=0 e=none a=none
Feb 03 13:46:55 1998 mr16n18: ICA1037i: #:8 permit 9.67.144.49 255.255.255.240
9.67.131.250 255.255.255.255 tcp     gt  1023 eq  21 secure local inbound
l=n f=y t=0 e=none a=none
Feb 03 13:46:55 1998 mr16n18: ICA1037i: #:9 permit 9.67.131.250 255.255.255.255
9.67.144.49 255.255.255.240 tcp/ack eq  21 gt  1023 secure local outbound
l=n f=y t=0 e=none a=none
Feb 03 13:46:55 1998 mr16n18: ICA1037i: #:10 permit 9.67.131.250 255.255.255.
255 9.67.144.49 255.255.255.240 tcp     eq  20 gt  1023 secure local outbound
l=n f=y t=0 e=none a=none
Feb 03 13:46:55 1998 mr16n18: ICA1037i: #:11 permit 9.67.144.49 255.255.255.
240 9.67.131.250 255.255.255.255 tcp/ack gt  1023 eq  20 secure local inbound
l=n f=y t=0 e=none a=none
Feb 03 13:46:55 1998 mr16n18: ICA1037i: #:12 permit 9.67.144.49 255.255.255.
240 9.67.131.250 255.255.255.255 tcp     gt  1023 gt  1023 secure local inbound
l=n f=y t=0 e=none a=none
.
.
.
Feb 03 13:46:58 1998 mr16n18: ICA1037i: #:100 deny 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
all any 0 any 0 both both both l=y f=y t=0 e=none a=none
```

Determinación de los estados de las normas

Las normas de IBM Firewall pueden tener uno de los estados siguientes:

1. La configuración no está activa.

   Todavía no ha utilizado el cliente de configuración para activar la configuración o bien ha desactivado la configuración. Éste es el estado que tiene la configuración cuando instala por primera vez el IBM Firewall y arranca el sistema o desactiva normas de filtros. Cuando instala el cortafuegos por primera vez, los filtros por omisión protegen la red de intrusos.

   Acceso al cortafuegos:

- La configuración del filtro por omisión permite todo el tráfico de entrada local y permite todo el tráfico de salida.

2. La configuración está activa, pero tiene errores.

   Ha activado la configuración. En la configuración existen errores (normas no válidas) o bien no se ha realizado ninguna configuración. En la ventana de salida Activación se visualizan los errores y los avisos.

   Acceso al cortafuegos:

   - Permitir todo el tráfico de entrada.
   - Permitir todo el tráfico de salida.

3. La configuración está activa y es válida. Tenga en cuenta que pueden existir avisos, muy señalados, de normas de filtros duplicadas.

   Ha activado la configuración que ha definido utilizando la sección de control de tráfico del cliente de configuración.

   Nota: El archivo de configuración puede ser válido y no contener ninguna norma. En este caso, existe una norma “denegar todo el acceso” en vigor.

   Acceso al cortafuegos:

   - El acceso lo determina el archivo de configuración.

     Cada paquete que recibe, o va a enviar, cualquier interfaz de red se examina, y su contenido se compara con cada una de las normas de conexión generadas. Cuando se encuentra una coincidencia, se realiza la acción (permitir o denegar) de esa norma.

   - Si ninguna norma coincide con el paquete, existe una norma implícita “denegar todo” que deniega el acceso.

Capítulo 9. Ejemplos de servicios

En este capítulo se describe cómo configurar el cortafuegos para realizar determinadas tareas comunes. Las tareas que se listan son sólo ejemplos pero, después de haberlas entendido, podrá configurar el cortafuegos para utilizar cualquiera de los servicios que se facilitan.

Consideraciones para la planificación

El control del tráfico del cortafuegos se organiza en términos de conexiones que definen los tipos de comunicaciones permitidos o prohibidos entre pares de puntos finales. Por lo tanto, es muy importante planificar las conexiones teniendo en cuenta los puntos finales.

Como se describía en el Capítulo 8, “Control del tráfico a través del cortafuegos” en la página 45, los puntos finales se representan ante el cortafuegos mediante objetos de red. Si todavía no lo ha hecho, debe completar la hoja de trabajo de planificación de la red del Capítulo 2, “Planificación” en la página 7 y crear los objetos de red necesarios para representar su red.

Los ejemplos de este capítulo utilizan los objetos de red siguientes:

Interfaz protegida La interfaz protegida del cortafuegos.

Interfaz no protegida
La interfaz no protegida del cortafuegos.

Red protegida
El rango de direcciones a las que puede accederse a través de la interfaz protegida del cortafuegos. Puede ser un grupo de objetos de red que contenga varios dominios diferenciados, cada uno de ellos representado mediante su propio objeto de red.

Mundo La red no protegida.

Cada tipo de comunicación deseado debe considerarse bajo el punto de vista de la comunicación punto final a punto final implicada. En esta fase, considere si el cortafuegos proporcionará estas comunicaciones mediante el proxy o si el cortafuegos direccionará estas comunicaciones.

Si el cortafuegos actúa de proxy, el cortafuegos realizará el trabajo necesario en lugar de hacerlo el usuario protegido y el sistema o sistemas principales no protegidos nunca sabrán que existe el sistema principal protegido. Si el cortafuegos va a direccionar el tráfico, el sistema principal protegido y el sistema principal no protegido se comunicarán directamente.

Si va a utilizar el cortafuegos como proxy, los puntos finales de la comunicación incluirán el cortafuegos, como se muestra en la Figura 17 en la página 54.

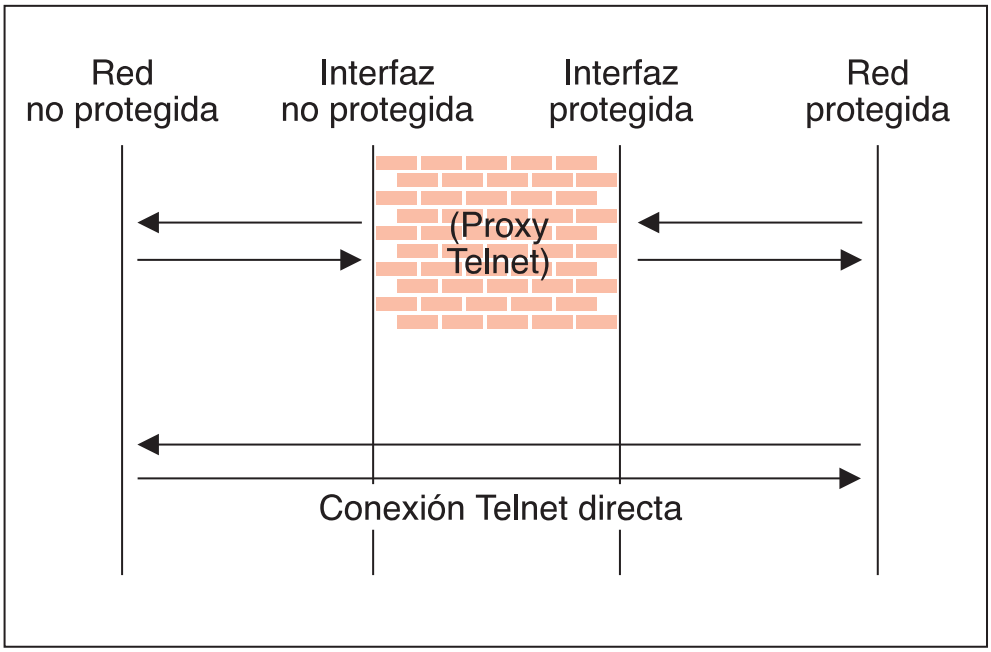

Figura 17. Proxy Telnet y conexión de Telnet directo

Ejemplo de Proxy Telnet

Este primer ejemplo corresponde a una conexión de proxy telnet de salida simple. En este ejemplo, los usuarios de la red protegida podrán utilizar el Proxy Telnet del cortafuegos para acceder a los servicios telnet de los sistemas principales de la red no protegida.

Como se describe en la Figura 17, tienen lugar dos conexiones:

1. El cliente del interior de la red protegida se conecta al Proxy Telnet del cortafuegos.
2. El Proxy Telnet del cortafuegos, en nombre del usuario protegido, se conecta al sistema principal de la red no protegida.

Para configurar el control del tráfico del cortafuegos para esta comunicación, necesitamos establecer dos conexiones:

Tabla 1. Proxy Telnet

Objeto de origen	**Objeto de destino**	**Servicios necesarios**
Red protegida	Interfaz protegida	Proxy Telnet para 1/2
Interfaz no protegida	Mundo	Proxy Telnet para 2/2

Ejemplo de Telnet con filtro

Compare el ejemplo anterior con una conexión telnet de con filtro simple. En este caso, el cliente del lado protegido se conectará directamente con el sistema principal del lado no protegido.

Tabla 2. Telnet con filtro

Objeto de origen	Objeto de destino	Servicios necesarios
Red protegida	Mundo	Telnet directamente

Como ya se ha explicado, esta configuración expondrá las direcciones de los clientes protegidos cuando se conecten a sistemas principales no protegidos.

Ejemplo de proxy HTTP

La mayoría de las instalaciones desearán que, como mínimo, algunos de los clientes protegidos puedan navegar por la Web. El IBM Firewall proporciona un servicio directo de salida HTTP predefinido para admitir el HTTP direccionado, que funciona exactamente igual que el ejemplo de Telnet con filtro. Además, el cortafuegos proporciona un proxy HTTP.

El protocolo HTTP difiere de Telnet en que puede encapsular otros protocolos. Incluso para la navegación más sencilla, la mayoría de usuarios no sólo necesitarán HTTP, sino también los servicios FTP. Para beneficiarse de toda la selección de funciones HTTP, también deben admitirse Gopher y WAIS, aunque se utilicen con menos frecuencia.

Sin embargo, tenga en cuenta que cuando se utilizan estos protocolos adicionales, se acomodan en el HTTP, entre el cliente y el proxy. Por lo tanto, la comunicación sería similar a la del diagrama de la Figura 18.

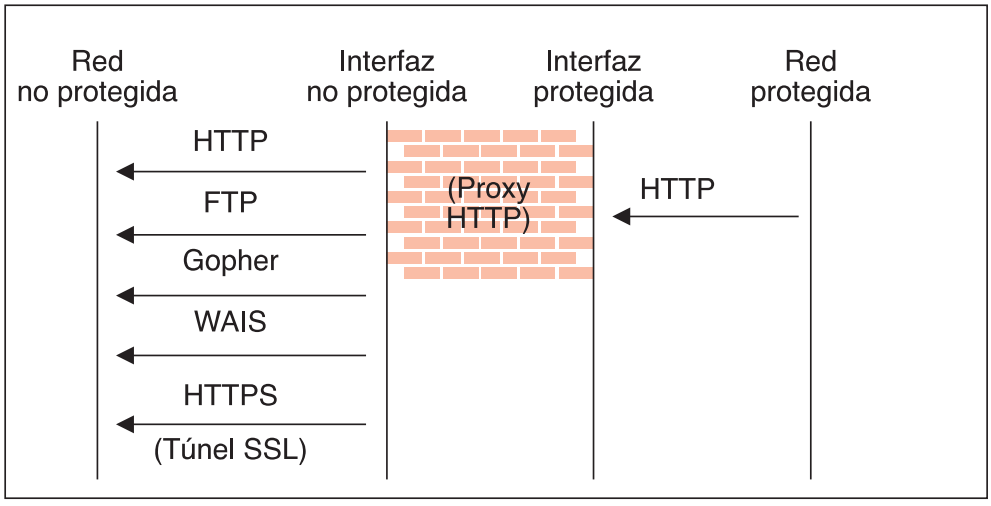

Figura 18. Proxy HTTP

Puesto que disponemos de dos pares de puntos finales, debemos codificar las dos conexiones.

Tabla 3. Proxy HTTP		
Objeto de origen	**Objeto de destino**	**Servicios necesarios**
Red protegida	Interfaz protegida	Proxy HTTP para salida 1/2
Interfaz no protegida	Mundo	Seleccionar... • Proxy HTTP para 2/2 • Proxy FTP para 2/2 • Proxy Gopher para 2/2 • Proxy WAIS para 2/2 • Proxy HTTPS para 2/2

Para obtener más información acerca del Proxy HTTP, consulte el Capítulo 13, “Configuración de servidores proxy” en la página 89.

Ejemplo de socks

Socks presenta un reto similar al que presenta el proxy HTTP en tanto que el daemon del socks maneja muchos protocolos distintos y los encapsula en una única corriente de datos entre el cortafuegos y el cliente. Socks es más flexible que el proxy HTTP, pues puede acomodar cualquier protocolo orientado a TCP o UDP y el cortafuegos puede configurarse independientemente de los filtros para ejercer un mayor control sobre las comunicaciones.

Debido a esta flexibilidad adicional, la configuración de socks requiere una tercera conexión además de las que se han mostrado con el proxy HTTP. Las dos conexiones básicas permitirán el flujo de paquetes en el cortafuegos en ambos sentidos; la tercera conexión se necesita para indicar al daemon del socks que adquiera las peticiones cuando reciba los paquetes.

Tabla 4. Socks		
Objeto de origen	**Objeto de destino**	**Servicios necesarios**
Red protegida	Interfaz protegida	Socks 1/2
Interfaz no protegida	Mundo	Seleccionar... • Proxy HTTP para 2/2 • Proxy FTP para 2/2 • Proxy Telnet de 2/2 (Cualquier servicio de proxy para la segunda mitad al que desee proporcionar soporte)
Red protegida	Mundo	En la ventana Configuración de socks, seleccione... • permitir HTTP socks • permitir FTP socks • permitir Telnet socks

Por supuesto, los clientes que se encuentran en el interior de la red protegida deben ser de tipo socks y deben configurarse para utilizar el cortafuegos como su servidor socks.

Para obtener más información acerca de Socks, consulte el Capítulo 11, “Configuración del servidor Socks” en la página 69.

Sugerencias para DNS

Si no proporciona una resolución DNS, el grado de comunicaciones eficaces será muy bajo. Consulte Capítulo 6, “Gestión del Servicio de denominación de nombres” en la página 31 para obtener detalles acerca de la configuración del DNS. No olvide habilitar "Permitir consultas DNS" en la Política de seguridad.

Sugerencias para clientes socks no protegidos

El panel Política de seguridad contiene un cuadro de selección para **Denegar socks a interfaz no protegida**. Este servicio rechazará cualquier paquete que se dirija al daemon del socks desde cualquier interfaz no protegida y hará que su cortafuegos sea mucho más seguro.

Si quiere permitir a los clientes que entren en su red desde una red no protegida, *no debe* seleccionar esta casilla.

Capítulo 10. Personalización del control del tráfico

Este capítulo le ayuda a definir las normas para los filtros y los servicios. Los servicios son una colección de normas o un conjunto de instrucciones que permiten o deniegan un tipo determinado de tráfico a través del cortafuegos; por ejemplo, una sesión telnet. Puede realizar adiciones a los servicios utilizando las plantillas de normas para crear nuevas normas. También puede suprimir servicios. Los servicios socks se aplican a las conexiones socks.

El IBM Firewall se entrega con un conjunto de servicios por omisión previamente cargado. Puede adaptar cualquier servicio definido previamente en función de sus necesidades o crear nuevos servicios.

Utilización del cliente de configuración para crear plantillas de normas

Para añadir una nueva norma a la lista de plantillas de normas disponibles, siga este procedimiento.

1. En el árbol de navegación del cliente de configuración, seleccione Control del tráfico y efectúe una doble pulsación en el icono de la carpeta de archivos. Seleccione **Plantillas de conexión** y, a continuación, seleccione **Normas**.
2. En el cuadro de diálogo **Lista de normas**, efectúe una doble pulsación en **NUEVO**.

   El IBM Firewall visualizará un cuadro de diálogo **Añadir norma IP**, como se muestra en la Figura 19, para que pueda definir una norma.

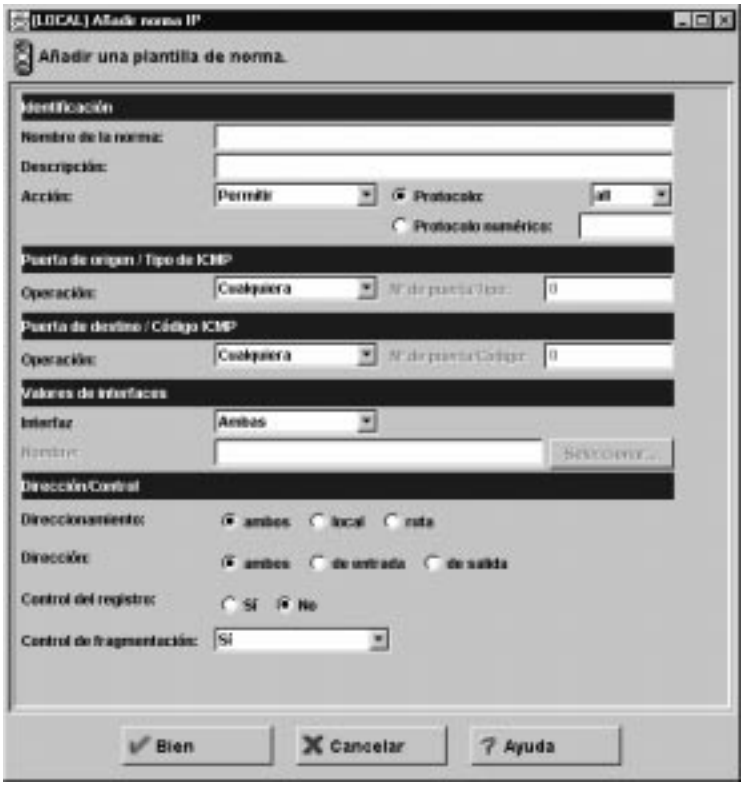

Figura 19. Añadir norma IP

3. Escriba el Nombre de la norma.
4. Escriba la Descripción de la norma. Este campo es opcional.
5. Pulse en la flecha de acción y elija permitir o denegar el acceso al cortafuegos.
6. Pulse en la flecha de protocolo y realice su selección utilizando la lista siguiente:

   todos Cualquier protocolo podrá coincidir con esta norma.

   tcp Para coincidir con esta norma, el protocolo del paquete debe ser el protocolo de control de transmisión (TCP).

   tcp/ack Para coincidir con esta norma, el protocolo del paquete debe ser TCP con acuse de recibo.

   udp Para coincidir con esta norma, el protocolo del paquete debe ser el protocolo de paquete de usuario (UDP).

   icmp Para coincidir con esta norma, el protocolo del paquete debe ser el protocolo de mensajes de control de Internet (ICMP).

   ospf Para coincidir con esta norma, el protocolo del paquete debe ser el protocolo Abrir primera vía de acceso más corta (ospf). Cuando se especifica ospf como protocolo, el valor de la puerta de origen y de la operación de la puerta de origen se utilizan para el valor de tipo de registro ospf. En el tipo ospf también puede realizarse el filtrado. Puede especificarse un valor de tipo **cualquiera**, y en los campos de la puerta de destino debe especificarse **cualquiera 0**. Todo lo demás se pasa por alto.

   ipip Para coincidir con esta norma, el protocolo del paquete debe ser el protocolo IP en IP (IPIP). Cuando se especifica IPIP, en los campos de puerta debe especificarse **cualquiera 0**.

   esp Para coincidir con esta norma, el protocolo del paquete debe ser el protocolo de seguridad de encapsulado que utiliza la red privada virtual para enviar paquetes IP encapsulados.

   ah El protocolo de cabecera de autentificación es el protocolo de paquete que utiliza la red privada virtual para enviar paquetes IP a los que se asocia un símbolo de autentificación.
7. El protocolo numérico le permite especificar un protocolo utilizando su valor decimal (de acuerdo con la RFC-1700). Los valores válidos van del 1 al 252. Tenga en cuenta que, al utiliza esta opción, en los campos de puerta para esta norma debe especificarse 0 (que significa cualquier puerta). Consulte la RFC-1700 para obtener una lista de todos los protocolos. O puede acceder a la Autorización de números asignados de Internet (Internet Assigned Numbers Authority, IANA) directamente con un navegador.
8. Los operandos de número de puerta y operación se utilizan conjuntamente. Las operaciones de origen y lógica indican una relación entre el número de puerta (destino u origen) del paquete y los operandos del n de puerta de origen y n de puerta de destino. Por ejemplo, si la puerta de destino del paquete es la puerta 20 y la operación de destino y el n de puerta de destino son “ge 15”, el paquete coincide. (20 es mayor o igual a 15).

   Si utiliza una operación de origen o de destino con el valor **cualquiera**, el filtro no comprobará el número de puerta; coincidirá cualquier puerta. En este caso, el número de puerta no puede cambiarse.

Para el protocolo ICMP, en lugar de especificar una puerta de origen, especifique un tipo ICMP y, en lugar de una puerta de destino, especifique un código ICMP. El operador lógico especificado se aplica al tipo o al código y, como con las puertas, un operador con un valor de cualquiera significa que cualquier valor de tipo y/o código coincidirá con la norma. En este caso, el número de puerta no puede cambiarse.

Los valores para la operación son:

- Cualquiera
- Igual a
- No igual a
- Menor que
- Mayor que
- Menor que o igual a
- Mayor que o igual a

Éstas son algunas de las puertas más importantes que han de protegerse. Los valores de los números de las puertas deben encontrarse en el rango 1 a 65535:

Puerta	**Utilización**
20	Datos FTP
21	Control FTP
23	Telnet
25	Correo
53	Servidor de denominación de dominios
70	Gopher
80	HTTP
111	RPC
161	SNMP
1080	socks

Éstos son algunos de los tipos y códigos ICMP:

Tipo	**Código y descripción**
0	0 - Respuesta ping
8	0 - Petición ping
3	1 - Sistema principal no accesible
3	3 - Puerta no accesible
5	1 - Redirigir para el sistema principal

9. Pulse en la flecha **Interfaz** para seleccionar el tipo de interfaz (adaptador).

   ambas Para los paquetes que proceden de o se dirigen a la interfaz protegida o no protegida

   protegida Para los paquetes que proceden de o se dirigen a la interfaz protegida

   no protegida Para los paquetes que proceden de o se dirigen a la interfaz no protegida

específica A utilizar con el campo de nombre de interfaz cuando se selecciona una interfaz, si se ha asignado un nombre a la interfaz.

10. Si elige específica como tipo de interfaz, el nombre de la interfaz específica aparecerá en el campo Nombre.
11. Efectúe una pulsación en el direccionamiento deseado:

    ambas Se aplica a todo el tráfico.

    local Implica que el paquete es local respecto al sistema principal del cortafuegos. Esto quiere decir que:

    - Los paquetes locales de entrada son paquetes que la interfaz recibe y que se destinan a este sistema principal del cortafuegos; no se direccionarán a otro sistema principal. Su destino es local.
    - Los paquetes de salida se transmiten desde la interfaz, pero se originan en el sistema principal del cortafuegos. Su origen es local.

    direccionado Implica que el sistema principal del cortafuegos direcciona el paquete. Esto quiere decir que:

    - Los paquetes locales de entrada son paquetes que la interfaz recibe y que se destinan a otro sistema principal; no permanecerán en el cortafuegos. Su destino es remoto.
    - Los paquetes de salida se transmiten desde la interfaz y se originan en otro sistema principal. Su origen es remoto.
12. Efectúe una pulsación en la dirección deseada:

    ambas Para los paquetes que proceden de o se dirigen a la interfaz seleccionada

    de entrada Para los paquetes que se dirigen a la interfaz seleccionada desde la red

    de salida Para los paquetes que proceden de la interfaz seleccionada y se dirigen a la red
13. Si elige Sí en el campo Control del registro, cada paquete que coincida con esa norma se grabará en el `registro del cortafuegos` con el nivel de prioridad `Error`. Si no se especifica este parámetro, el valor por omisión es no.
14. Pulse en la flecha **Control de fragmentación** para elegir el control de fragmentación deseado. Para que la información del paquete IP coincida con una especificación de control de fragmentación de la norma, el control se interpreta de la forma siguiente:

    Sí La norma coincidirá con las cabeceras de fragmento, fragmentos y no fragmentos. Para los fragmentos, la información de la puerta se pasará por alto y se dará por supuesta la coincidencia.

    Sólo Sólo podrán coincidir los fragmentos y las cabeceras de fragmento. Para las cabeceras de fragmento, la información de la puerta deberá coincidir. Para los fragmentos, la información de la puerta se pasará por alto.

No Sólo pueden coincidir los no fragmentos. Este parámetro excluye las cabeceras de fragmento y los fragmentos.

Cabeceras Sólo podrán coincidir los no fragmentos y las cabeceras de fragmento. Este parámetro excluye los fragmentos.

Si no se especifica este parámetro, el valor por omisión para "permitir" y "denegar" normas es Sí.

Nota: Con independencia del valor de este control, los fragmentos IP con un desplazamiento de uno (1) se descartan. Esta acción elimina el conocido ataque de utilizar fragmentos de paquete para recubrir los distintivos de cabecera TCP.

Para que una cabecera de paquete coincida con una norma IP definida, la información del paquete debe coincidir con todos los parámetros especificados en la norma codificada. Para los fragmentos de paquete, todos los parámetros, a excepción de la información de la puerta, se utilizan para determinar la coincidencia.

Si una norma anterior, con el código Sí o Sólo, no ha permitido los fragmentos, la norma final que siempre se añade al final del archivo denegará los fragmentos del paquete.

Cambio de una entrada de configuración de una norma IP

Para modificar una norma IP que ha creado:

1. Efectúe una doble pulsación en una norma existente en la **Lista de normas**. Aparecerá el cuadro de diálogo **Modificar configuración de norma IP**.
2. Modifique los campos correspondientes, tal como se describe en el Capítulo 10, “Personalización del control del tráfico” en la página 59, y pulse en **Bien** para aplicar los cambios.

Supresión de una entrada de configuración de una norma

Para suprimir una norma, seleccione una norma en **Lista de normas** y pulse en **Suprimir**.

Servicios predefinidos

El IBM Firewall se entrega con un conjunto de servicios por omisión previamente cargado. Los servicios son una colección de normas o un conjunto de instrucciones que permiten o deniegan un tipo determinado de tráfico a través del cortafuegos; por ejemplo, una sesión telnet. Puede realizar adiciones a los servicios utilizando las plantillas de normas para crear nuevas normas.

Los servicios por omisión cargados previamente son:

Todo en no protegida Denegar todo el tráfico a través de la interfaz no protegida

Todo permitido Permitir todo el tráfico (sólo para la depuración)

Permitir todo, en una dirección Permitir todo el tráfico (sólo para la depuración)

Todo en protegida Denegar todo el tráfico a través de la interfaz protegida (en caso de producirse una violación de la seguridad)

Todo concluir Denegar todos los paquetes (concluir o depurar)

Antifraudes Denegar paquetes no protegidos de entrada con dirección de origen protegida

Difusiones generales Denegar mensajes de difusión general a la interfaz no protegida

Cliente de configuración desde no protegida Permitir la utilización del cliente de configuración desde la red no protegida

Cliente de configuración desde protegida Permitir la utilización del cliente de configuración desde la red protegida

CU-SeeMe Vídeo CU-SeeMe en puertas por omisión 7649 y 7648

Consultas DNS (POLÍTICA DE SEGURIDAD) Permitir consultas DNS

Transferencias DNS Permitir transferencias de zona DNS (para los servidores de nombres secundarios)

Autentificación de controlador de dominio Permitir la utilización del Controlador de dominio para la autentificación del usuario

Proxy FTP para 1/2 Permitir FTP de entrada desde la red no protegida al cortafuegos

Proxy FTP para 2/2 Permitir FTP de entrada desde el cortafuegos a la red protegida

Proxy FTP de 1/2 Permitir FTP de salida desde la red protegida al cortafuegos

Proxy FTP de 2/2 Permitir FTP de salida desde el cortafuegos a la red no protegida

Proxy Gopher para 2/2 Permitir gopher desde el cortafuegos a la red protegida

Proxy Gopher de 2/2 Permitir gopher desde el cortafuegos a la red no protegida

Denegar HTTP a no protegidas Denegar HTTP a las interfaces no protegidas

HTTP directamente Permitir HTTP desde la red protegida directamente a la red no protegida

Proxy HTTP para 2/2 Permitir HTTP desde el cortafuegos a la red protegida

Proxy HTTP de 1/2 Permitir HTTP (puerta 8080) desde la red protegida al cortafuegos

Proxy HTTP de 2/2 Permitir HTTP desde el cortafuegos a la red no protegida

HTTPS directamente Permitir HTTPS (SSL) desde la red protegida a la red no protegida

Proxy HTTPS de 2/2 Permitir HTTPS (túnel SSL) desde el cortafuegos a la red no protegida

IDENTD Permitir identificación de usuario con protocolos Socks

Correo (POLÍTICA DE SEGURIDAD) Permitir el tráfico del Correo a través del cortafuegos

Difusiones generales de los servicios de nombres NetBT Permitir difusiones generales de los servicios de nombres NetBIOS sobre TCP/IP

Ping Permitir Ping de red protegida de salida a cualquier punto

Autentificación SDI Permitir conexión al servidor SecurID ACE en la red protegida

Socks 1/2 Permitir la utilización de Socks desde la red protegida al cortafuegos

Denegar Socks de no protegidos Denegar Socks desde los adaptadores no protegidos

Socks para 1/2 Permitir la utilización de Socks desde la red no protegida al cortafuegos

Telnet directamente Permitir Telnet de salida desde la red protegida a la red no protegida

Proxy Telnet para 1/2 Permitir Telnet de entrada desde la red no protegida al cortafuegos

Proxy Telnet para 2/2 Permitir Telnet de entrada desde el cortafuegos a la red protegida

Proxy Telnet de 1/2 Permitir Telnet de salida desde la red protegida al cortafuegos

Proxy Telnet de 2/2 Permitir Telnet de salida desde el cortafuegos a la red no protegida

Entrada directa VDOLIVE Permitir cliente no protegido al servidor protegido

Tenga en cuenta que los usuarios deben configurar propiedades de reproducción individuales para utilizar sólo la puerta UDP 7001.

Salida directa VDOLIVE Permitir cliente protegido al servidor protegido

Proxy WAIS para 2/2 Permitir WAIS (z39.50) desde el cortafuegos a la red protegida

Proxy WAIS para 2/2 Permitir WAIS (z39.50) desde el cortafuegos a la red no protegida

Definición de los servicios

Tras haber definido una norma o normas, será necesario añadir la norma o normas a un servicio. Seleccione Control del tráfico en el árbol de navegación del cliente de configuración y efectúe una doble pulsación en Plantillas de conexión y, a continuación, seleccione Servicios. Aparecerá el cuadro de diálogo Lista de servicios. Efectúe una doble pulsación en NUEVO para que se visualice el cuadro de diálogo Añadir servicio, como se muestra en la Figura 20 en la página 66.

Figura 20. Añadir un servicio

Utilización del cliente de configuración para crear servicios

1. Escriba el nombre del servicio.
2. Escriba una descripción.
3. El campo **Alterar temporalmente control de registro** proporciona un medio de alterar temporalmente el valor del control de registro de las plantillas de normas que se han seleccionado para este servicio. Por ejemplo, si incluye un conjunto de plantillas de normas cuyo control generalmente está establecido en no, puede alterar temporalmente este valor para que sea sí para este servicio. El valor de la alteración temporal se aplicará a todas las normas de este servicio. En el campo **Alterar temporalmente control de registro**, especifique una de las opciones siguientes:
   - sin alteración temporal - la alteración temporal está desactivada, seguirán aplicándose los valores de las normas
   - sí - grabar un registro de anotaciones cuando se detecte una coincidencia con cualquier norma de este servicio
   - no - no grabar ningún registro de anotaciones cuando se detecte una coincidencia con cualquier norma de este servicio

   Cuando se graba un registro de anotaciones para una norma de filtro, los valores que se muestran en el registro de anotaciones son los valores reales del paquete IP. El registro que coincide con las normas de filtros puede proporcionar valiosa información acerca del contenido de los paquetes IP que ha detectado el cortafuegos; por ejemplo, el protocolo real y los números de puertas.
4. El campo **Alterar temporalmente control de fragmentación** proporciona un medio de alterar temporalmente el valor del Control de fragmentación de las plantillas de normas que se han seleccionado para este servicio. Por ejemplo,

si incluye un conjunto de plantillas de normas cuyo Control de fragmentación generalmente está establecido en no, puede alterar temporalmente este valor para que sea sí para este servicio. El valor de la alteración temporal se aplicará a todas las normas de este servicio. El campo Alterar temporalmente control de fragmentación, especifique una de las opciones siguientes:

- sin alteración temporal - la alteración temporal está desactivada, seguirán aplicándose los valores de las normas
- sí - buscar coincidencia con cualquier paquete IP; por ejemplo, no fragmentos, cabeceras de fragmento y fragmentos sin cabeceras
- no - buscar coincidencia sólo con paquetes de no fragmento, no buscar coincidencia con las cabeceras de fragmento o fragmentos sin cabeceras
- sólo - buscar coincidencia sólo con cabeceras de fragmento y fragmentos sin cabecera, no buscar coincidencia con no fragmentos
- cabeceras - buscar coincidencia sólo con no fragmentos y cabeceras de fragmento, no buscar coincidencia con fragmentos sin cabeceras

5. Los controles para los períodos de tiempo le permiten asociar un rango de horas a cada servicio. Por lo tanto, este servicio sólo tendrá validez durante el período de tiempo especificado. Si no existe ninguna especificación horaria para un servicio, el servicio será válido todo el tiempo.

   Control por horas Seleccione si desea que este servicio se active o desactive a lo largo del día en función de las horas de inicio y finalización especificadas. Utilice un formato de 24 horas. Si este campo no está habilitado, los campos Horas estarán en vigor las 24 horas del día.

   Control por días Seleccione si desea que este servicio se active o desactive en función de una planificación basada en días de la semana o en fechas de calendario. Tenga en cuenta que la activación o desactivación de un servicio depende del valor del campo Acción del control horario.

   Acción del control horario Elija **Activar servicio durante las horas especificadas** si desea que este servicio se active durante las horas especificadas. Este servicio quedará desactivado durante las horas no incluidas entre las especificadas.

   Elija **Desactivar servicio durante las horas especificadas** si desea que este servicio se desactive durante las horas especificadas. Este servicio se activará durante las horas no incluidas entre las especificadas.

6. Pulse en **Seleccionar** para elegir las normas que componen este servicio.
7. Utilice el conmutador Flujo para determinar la forma en que los valores Origen y Destino de la Conexión deben asignarse a los filtros a medida que se graban en el archivo Norma base.

   ```
   ---> Izquierda a derecha indica que el Origen y el Destino de la
        Conexión se graban directamente en la norma a medida que se graban
        en el archivo Norma base.

   <--- Derecha a izquierda indica que el Origen y el destino de la
        Conexión se graban en sentido inverso cuando se graban en el archivo
        Norma Base.
   ```

8. Cuando se recibe un paquete, el IBM Firewall compara la información del paquete con las normas del archivo de configuración de normas, empezando desde el inicio del archivo. Detiene la comparación cuando se detecta la primera coincidencia y realiza la acción que la norma contiene.

   Cuando se ha añadido una serie de normas al servicio, puede cambiarse su orden. Seleccione una norma de la lista **Objetos del servicio** y pulse en los botones **Mover arriba** o **Mover abajo** para cambiar la posición de la norma. O también puede eliminar una norma pulsando en **Eliminar**. El cliente de configuración visualizará una lista de normas renovada. Pulse en **Bien** para guardar los cambios.

Capítulo 11. Configuración del servidor Socks

Socks es un estándar de Internet para las pasarelas a nivel de circuito. El servidor Socks se utiliza para la conversión de las direcciones si la aplicación utiliza TCP, como los navegadores de la Web, FTP o las aplicaciones Telnet. Socks puede ayudarle a acceder a Internet, a la vez que su dirección IP interna queda oculta.

Para las peticiones de salida, desde un cliente protegido a un servidor no protegido, el servidor Socks tiene los mismos objetivos que un servidor proxy: interrumpir la sesión en el cortafuegos y proporcionar una puerta segura en la que puede permitirse a los usuarios acceder a la red no protegida externa a la vez que se protege la dirección y la estructura de la red interna. Para el usuario, la ventaja del servidor Socks es su simplicidad, con poco trabajo administrativo adicional.

El servidor Socks puede interceptar todas las peticiones TCP/IP de salida que fluyan entre su red e Internet. El servidor Socks ofrece una interfaz de programación de aplicaciones remota para que las funciones que ejecutan los programas de cliente en los dominios protegidos fluyan a través de los servidores protegidos en las estaciones de trabajo del cortafuegos, ocultando la dirección IP del cliente. El acceso lo controlan los filtros que se asocian a las normas de Socks.

El servidor Socks es similar al servidor proxy. Pero, mientras que el servidor proxy realmente lleva a cabo la función TCP/IP en el cortafuegos, el servidor Socks sólo identifica al usuario y redirige la función a través del cortafuegos. La función TCP/IP se realiza realmente en la estación de trabajo del cliente, no en el cortafuegos. Esto ahorra proceso en el cortafuegos. Los usuarios de la red protegida pueden utilizar los numerosos productos TCP/IP que dan soporte al estándar socks. La Figura 21 muestra cómo el servidor Socks intercepta una petición HTTP de un cliente dentro de la red protegida.

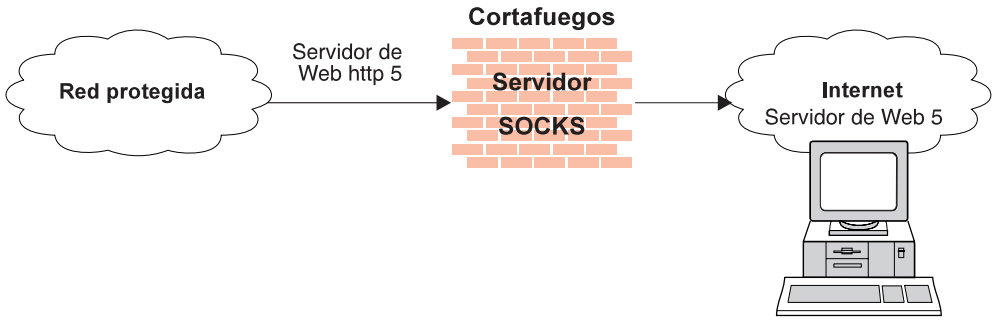

Figura 21. Servidor Socks

El servidor Socks oculta con eficacia las direcciones IP internas al exterior.

El IBM Firewall proporciona el protocolo Socks versión %, que permite a los clientes de la red protegida pasar una fase de autentificación antes de acceder a aplicaciones de la red no protegida. También proporciona un proxy genérico autentificado y el proxy de algunos protocolos de audio y vídeo en modalidad continua.

El daemon de Socks se ejecuta como un Servicio de Windows NT, que se inicia automáticamente al arrancarse el sistema. Además, se proporciona un Watch Agent (Agente de observación) para permitir la supervisión del servidor. Puede iniciar el Watch Agent manualmente.

El IBM Firewall ofrece un método de migración gradual en forma de tres perfiles de autentificación para que los usuarios puedan utilizar el protocolo Socks versión 4 instalado a medida que introducen clientes de protocolo Socks versión 5.

1. El perfil más permisivo no permite la autentificación de salida y permite a cualquier usuario, tanto si utiliza un cliente de protocolo Socks versión 4 o protocolo Socks versión 5, conectarse. En esta situación, se deniegan las conexiones de entrada.
2. El perfil de migración permite a los usuarios del protocolo Socks versión 4 pasar sin autentificación, pero solicita a los usuarios del protocolo Socks versión 5 que se autentifique. Se deniegan las conexiones del protocolo Socks versión 4 y las conexiones del protocolo Socks versión 5 de entrada son necesarias para la autentificación. Es el perfil por omisión.
3. El perfil más seguro necesita que todos los usuarios utilicen clientes de protocolo Socks versión 5 y que proporcionen autentificaciones válidas.

Cuando se instala el cortafuegos, el servidor Socks está habilitado, pero el archivo de configuración del socks no contiene ninguna norma. Para que los clientes socks puedan utilizar el servidor Socks, debe configurar el socks utilizando el cliente de configuración. Consulte el apartado “Ejemplo de socks” en la página 56, para ver un ejemplo de cómo configurar un servicio socks.

Protocolos a los que da soporte el Servidor de protocolo Socks versión 5

El servidor de protocolo Socks versión 5 da soporte a los protocolos TCP y UDP siguientes y a muchos más:

- Archie
- Finger
- FTP
- Gopher
- HTTP
- Proxy HTTP
- News
- SNMP
- Telnet
- TFTP
- RealAudio
- RealPlayer
- Whois
- X-Windows

Además, también reciben soporte la mayoría de clientes de correo electrónico. El soporte de estos protocolos depende de su implementación real.

Configuración del servidor Socks utilizando el cliente de configuración

Las plantillas de Socks son normas que controlan la seguridad del servidor Socks. Las plantillas de socks le permiten personalizar, añadir, copiar o suprimir plantillas de socks existentes. A su vez, estas plantillas de socks pueden utilizarse en las definiciones de las conexiones del cortafuegos de la misma forma que se utilizan las plantillas de normas.

Adición de una nueva norma de socks

Para añadir una norma al archivo de configuración del socks utilizando una plantilla de socks que proporcione el cliente de configuración, seleccione Control del tráfico en el árbol de navegación del cliente de configuración. Efectúe una doble pulsación en el icono de la carpeta de archivos para ampliar la vista. Seleccione Plantillas de conexión. Efectúe una doble pulsación en el icono de la carpeta de archivos para ampliar la vista. Seleccione **Socks**. Aparecerá el cuadro de diálogo **Socks**.

1. Para añadir una nueva plantilla de socks, efectúe una doble pulsación en **NUEVA**.

   Aparecerá el cuadro de diálogo **Añadir una norma socks**, como se muestra en la Figura 22.

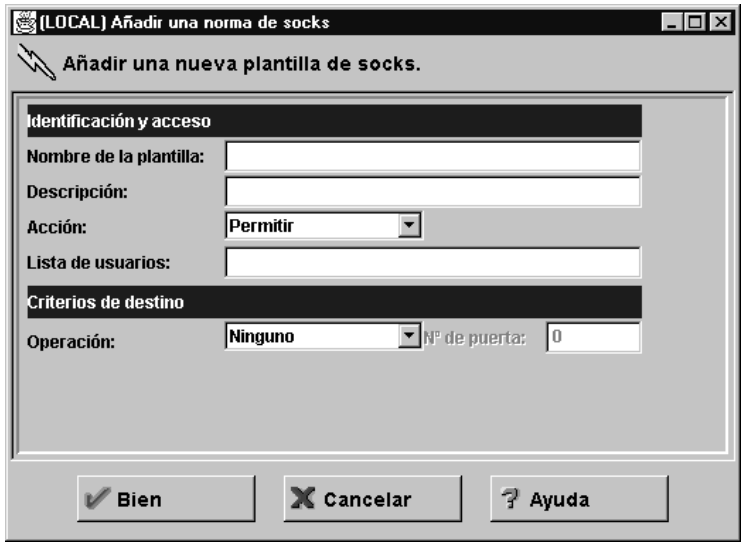

Figura 22. Añadir una norma de socks

2. En el campo **Nombre de la plantilla**, especifique el nombre de la entrada del socks. Este nombre debe ser exclusivo y no debe contener el símbolo de la barra vertical (|), el carácter de la comilla simple (o apóstrofo) (') o el carácter de comillas ("), pues estos símbolos se utilizan como delimitadores de archivos. La utilización de estos caracteres dará lugar a que los datos no sean fiables.
3. Escriba una descripción.
4. Efectúe una pulsación en la flecha Acción y elija permitir o denegar el acceso desde un origen a un destino.

   Cuando un datagrama llega al servidor Socks, el servidor compara las especificaciones del datagrama con cada una de las normas del archivo de configuración, empezando por la primera norma, y hasta encontrar una norma que

coincide exactamente. Entonces, detiene la búsqueda y realiza la acción relevante (permitir o denegar el acceso) de esa norma. Si no se encuentra ninguna coincidencia, el acceso se deniega automáticamente.

5. En el campo **Lista de usuarios**, puede especificar un ID de usuario o una lista de ID de usuarios. Si especifica una lista, separe las entradas con comas. No utilice espacios, tabulaciones, el símbolo de la barra vertical (|) ni las comillas (") en la lista de usuarios.
   - La lista de usuarios tiene un límite de 396 caracteres.
   - Los ID de usuarios deben ser ID de usuarios del sistema principal peticionario, no los que se encuentran en el sistema principal de destino ni los del sistema principal del servidor Socks.
   - Un ID de usuario puede contener de 1 a 8 caracteres, incluyendo:
     – a a z
     – A a Z
     – 0 a 9
     – _ (subrayado)
6. Un ID de usuario no debe contener caracteres de símbolo de barra vertical (|) ni comillas (").
7. Si se utilizan nombres de archivos, deben calificarse al completo (con la "/" inicial para evitar que se interpreten como ID de usuarios). Cada archivo puede contener una lista de ID de usuarios, uno o más por línea, separados por comas, incluyendo opcionalmente un comentario que se delimitará con el carácter #. Las líneas de comentarios completas -las que empiezan con el carácter #- también reciben soporte. Cada línea del archivo puede tener una longitud de hasta 1023 caracteres y debe finalizar con un carácter de "nueva línea".
8. En el campo **Operación**, especifique la operación lógica que ha de realizarse en el número de puerta:

eq	Igual a
neq	No igual a
lt	Menor que
gt	Mayor que
le	Menor que o igual a
ge	Mayor que o igual a

   Cuando se utiliza con el Número de puerta, la operación lógica establece una relación que debe satisfacerse. Por ejemplo, si especifica la Operación gt y el Número de puerta 23, el número de puerta deberá ser mayor que 23 para que se invoque la norma.
9. En el campo **N de puerta**, especifique el número de una puerta. El Número de puerta se utiliza con el campo Operación para establecer una relación que debe satisfacerse. Por ejemplo, si especifica la Operación gt y el Número de puerta 23, el número de puerta deberá ser mayor que 23 para que se invoque la norma. Si se omiten la operación y el número de puerta, la norma se aplica a todos los números de puertas de destino.

Utilice este cuadro de diálogo **Añadir una norma de socks** para permitir o denegar el acceso al cortafuegos a los sistemas principales de la red basándose en la dirección IP.

Modificación de una norma de socks

1. Efectúe una doble pulsación en una entrada del cuadro de diálogo **Socks**.

   Aparecerá el cuadro de diálogo **Modificar una norma de socks**.

2. Cambie los campos correspondientes tal como se describe en el apartado “Adición de una nueva norma de socks” en la página 71, y pulse en **Bien**.

Supresión de una norma de socks

Seleccione una entrada del cuadro de diálogo **Socks** y pulse en **Suprimir**. Se le preguntará si está seguro de que desea suprimir esta norma de socks. Pulse en **Bien** para suprimir la norma.

Activación de las normas de conexión

Como sucedía con las normas de filtros, también es necesario activar las normas de socks. Pulse en **Activación de la conexión** en el árbol de navegación del cliente de configuración, seleccione **Regenerar normas de conexión y activar** y, a continuación, pulse en **Ejecutar**.

El cortafuegos copia las normas del archivo de configuración del socks en las normas del cortafuegos y activa las normas. Cuando se activan normas, las nuevas normas se registran en el archivo de registro del cortafuegos.

Ejemplo de salida del registro para Socks

El siguiente es un ejemplo de la salida del registro para Socks.

```
Feb 03 13:46:20 1998 mr16n18: ICA3123i: Iniciando el servidor Sockd
Feb 03 13:47:31 1998 mr16n18: ICA3010i: Inicio de sesión
Feb 03 13:47:31 1998 mr16n18: ICA3011i: Inicio d sesión
Feb 03 13:49:15 1998 mr16n18: ICA3007i: Demasiadas hebras
Feb 03 13:58:31 1998 mr16n18: ICA3015i: Finalización de la sesión
```

Consideraciones del cliente para la utilización del servidor Socks

La mayoría de visualizadores de la Web son de tipo socks y pueden obtenerse pilas socks para la mayoría de plataformas. Los clientes socks para otras aplicaciones TCP/IP puede obtenerse de muchas fuentes. Para conocer un cliente específico que socks implementa, consulte la documentación de ese cliente. Para obtener información adicional, consulte:

http://www.raleigh.ibm.com/sng/sng-socks.html
http://www.socks.nec.com

Encadenado del servidor Socks

El encadenado del servidor Socks es una función por la cual un servidor Socks puede residir detrás de otro servidor Socks, pero permite acceso a la red más allá del servidor Socks más externo. (Se puede considerar una socksificación de un servidor Socks). Es un escenario de internet muy útil.

Para configurar el encadenamiento con el servidor Socks, edite el archivo `socks5.header.cfg`. Este archivo se encuentra en el subdirectorio `config` del cortafuegos. Añada lo siguiente:

- Una directiva *no proxy* para indicar la(s) subred(es) a la(s) que el cortafuegos tiene acceso directo
- Una directiva *socks4* para indicar la(s) subred(es) a la(s) que se puede acceder mediante el servidor de protocolo SOCKS versión 4
- Una directiva *socks5* para indicar la(s) subred(es) a la(s) que se puede acceder mediante un servidor de protocolo Socks versión 5

Por ejemplo, estudie la siguiente red. El departamento de investigación tiene una pequeña red privada, *q.private.com*, detrás de su propio cortafuegos. La subred del departamento de investigación es 10.007.007.0/255.255.255.0. La red privada de la empresa, *private.com*, cotiene toda la red 10.0.0.0/255.0.0.0. El servidor de protocolo SOCKS versión 4, *socks.private.com*, proporciona acceso a Internet.

En el servidor Socks de Investigación, *socks.q.private.com*, añada las dos siguientes líneas a `socks5.header.cfg`.

```
no proxy 10.0.0.0/255.0.0.0 - - -
socks4      0/0   - socks.private.com 1080
```

Por último, añada una conexión de control de tráfico para permitir que *socks.q.private.com* se comunique con *socks.private.com*. Esto podría haberse realizado mediante un servicio más general. Añada una conexión cuyo origen es la interfaz no protegida del cortafuegos *q.private.com* y cuyo destino es *socks.private.com* e incluya el servicio *Encadenado del proxy de Socks*. A continuación vuelva a activar su control de tráfico.

Capítulo 12. Administración de los usuarios en el cortafuegos

En este capítulo se describe cómo realizar las tareas administrativas cotidianas con el IBM Firewall, incluyendo:

- Adición de usuarios al IBM Firewall para que puedan acceder a los sistemas principales que se encuentran fuera de la red protegida
- Cambio de los atributos de los usuarios que acceden al cortafuegos
- Supresión de usuarios que ya no necesitan acceso al exterior de la red

No edite los archivos de configuración directamente; si lo hace, los atributos de usuario del IBM Firewall no se configurarán correctamente. Realice toda la administración del IBM Firewall utilizando la línea de mandatos o los diálogos del cliente de configuración.

Adición de un usuario al IBM Firewall

El IBM Firewall define tres tipos de usuarios y almacena su información en dos bases de datos de usuarios distintas.

Tipos de usuarios

El IBM Firewall divide a los usuarios en tres categorías:

Usuarios del proxy Utilice los servicios del cortafuegos, como el servicio del proxy HTTP para acceder a sitios Web de Internet desde el interior de una red corporativa. Los usuarios del proxy pueden utilizar servicios a través del cortafuegos, pero no tienen acceso a la máquina del cortafuegos y no pueden realizar conexiones lógicas a la máquina del cortafuegos.

Administradores del cortafuegos Pueden utilizar los servicios del proxy del cortafuegos y también pueden configurar el cortafuegos utilizando el cliente de configuración y conectándose al cortafuegos desde un sistema principal remoto. Como los usuarios del proxy, los administradores del cortafuegos no pueden realizar conexiones locales a la máquina del cortafuegos.

Los administradores del cortafuegos pueden crear y modificar las definiciones de los usuarios del proxy, pero no pueden crear ni modificar las definiciones de otros administradores del cortafuegos.

Administradores principales del cortafuegos Tienen la misma capacidad que los administradores del cortafuegos. También pueden realizar conexiones lógicas a la máquina del cortafuegos. Los administradores principales del cortafuegos pueden crear y modificar las definiciones de los otros administradores del cortafuegos.

Tipos de bases de datos

Existen dos tipos de bases de datos de usuarios.

Base de datos de usuarios del cortafuegos Contiene los atributos relacionados con el cortafuegos de cada usuario del proxy y administrador. Incluye atributos tales como la contraseña del cortafuegos del usuario y las normas de contraseñas y qué método de autentificación debe utilizarse para autentificar al usuario para cada servicio.

Si el usuario del proxy no se ha definido en la base de datos de usuarios del cortafuegos y el usuario intenta utilizar los servicios del proxy del cortafuegos, se utilizará el registro de usuario por omisión, `fwdfusr`, para definir los atributos y esquemas de autentificación que se utilizan para validar al usuario.

Los administradores principales del cortafuegos no pueden definirse en la base de datos de usuarios del cortafuegos. Para asignar atributos a los administradores, utilice el registro de administrador del cortafuegos por omisión, `fwdfadm`.

Como los usuarios del proxy, si los administradores del cortafuegos también se definen en la base de datos de usuarios de Windows NT, su contraseña de conexión NT se utilizará cuando el usuario solicite servicios que deben autentificarse utilizando las contraseñas de conexión NT.

Base de datos de usuarios del Windows NT Contiene las contraseñas de conexión NT de los usuarios. En general, los usuarios del proxy no tienen que definirse en la base de datos de NT a no ser que vayan a autentificarse utilizando su contraseña de conexión de NT.

Si van a utilizarse otros métodos de autentificación para autentificar a los usuarios del proxy, éstos no tienen que definirse en la base de datos de usuarios de Windows NT.

Los administradores principales del cortafuegos son lo mismo que los usuarios de Windows NT que son miembros del grupo de administradores NT y deben definirse en la base de datos de usuarios de Windows NT.

Utilización del cliente de configuración para añadir un usuario

La adición de un usuario al IBM Firewall le proporciona acceso a la red externa.

1. En el árbol de navegación del cliente de configuración, seleccione Usuarios. Aparecerá el cuadro de diálogo **Administración de usuarios**.
2. Seleccione **Nuevo** en el cuadro de diálogo **Administración de usuarios** y pulse en **Abrir**. Aparecerá el cuadro de diálogo **Añadir usuario**, como se muestra en la Figura 23 en la página 77.

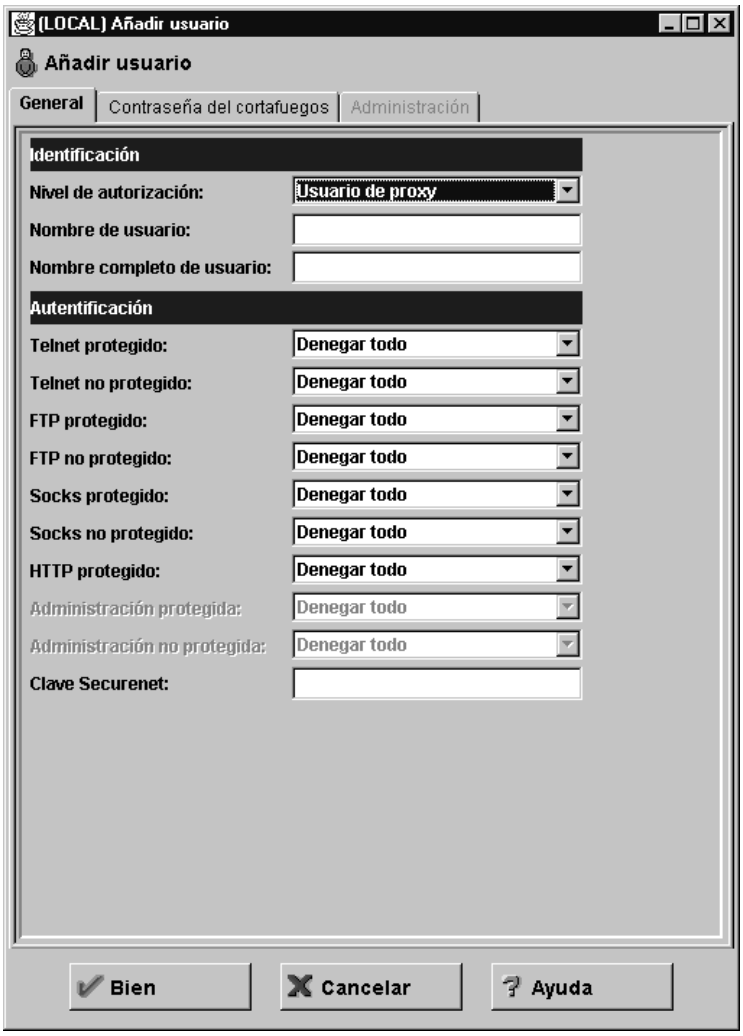

Figura 23. Añadir usuario

3. Proporcione esta información:

Nivel de autorización

Especifica el nivel de autorización de este usuario. Pulse en la flecha **Nivel de autorización** para seleccionar el tipo de usuario.

Usuario del socks/proxy

El usuario se define para el acceso al servidor Socks y para el acceso al proxy. El usuario no tiene ninguna autorización administrativa. Es el valor por omisión.

Administrador del cortafuegos

Tiene todos los atributos de un usuario, pero un administrador también puede conectarse al cortafuegos y realizar tareas administrativas. Un administrador dispone de atributos adicionales que definen las funciones adminis-

trativas que puede realizar. Un administrador del cortafuegos puede crear usuarios del cortafuegos, pero no puede crear otros administradores del cortafuegos. Los administradores del cortafuegos no pueden conectarse localmente a la máquina del cortafuegos. Deben acceder al servidor de configuración desde una máquina remota.

Administrador principal del cortafuegos
El administrador principal del cortafuegos puede conectarse localmente a la máquina del cortafuegos. Dispone de total acceso a las funciones administrativas. También puede crear otros administradores del cortafuegos, a excepción de administradores principales del cortafuegos.

El administrador principal del cortafuegos se define creando un usuario en la base de datos NT y haciendo que el usuario sea miembro del grupo de administradores NT. Para definir los atributos del administrador principal del cortafuegos, modifique el registro `fwdfadm`.

Nombre de usuario Especifica el nombre de este usuario. Es el nombre de usuario que este usuario utilizará para conectarse al servidor FTP o telnet en el IBM Firewall. No tiene que ser necesariamente el nombre del sistema principal o el nombre de usuario TCP/IP del usuario, pero pueden ser iguales.

Un nombre de usuario se compone de 1 a 20 caracteres, incluidos:

a a z
A a Z
0 a 9
_ (el signo de subrayado)

Los nombres de los usuarios no son sensibles a las mayúsculas y minúsculas.

El cortafuegos se entrega con dos usuarios previamente instalados:

a. Usuario por omisión o `fwdfuser`. Si un usuario no se define en la base de datos del cortafuegos, `fwdfuser` se utiliza para determinar los atributos del cortafuegos del usuario como, por ejemplo, qué métodos de autentificación han de utilizarse para autentificar al usuario.

   Durante la instalación, cuando se crea `fwdfuser`, todos los métodos de autentificación se establecen en denegar todo. El permiso de `fwdfuser` controla la forma en que el cortafuegos procesa los nombres de usuario no definidos.

   El administrador puede ver el `fwdfuser` o cambiar el método de autentificación asignado utilizando el cliente de configuración o la línea de mandatos. Sin embargo, `fwdfuser` no puede suprimirse y siempre debe existir en el cortafuegos. Además, la contraseña del cortafuegos y SNK no son tipos de autentificación válidos para `fwdfuser`. Para obtener más información, consulte el manual *IBM eNetwork Firewall - Manual de consulta.*

b. El administrador principal del cortafuegos por omisión, `fwdfadm`, define los atributos de cortafuegos de todos los administradores principales del cortafuegos. Puesto que los administradores principales del cortafuegos no tienen registros de usuario propios en la base de datos del cortafuegos, este registro se utiliza para definir los métodos de autentificación que se utilizan para autentificar a los administradores principales del cortafuegos.

   Durante la instalación, todos los métodos de autentificación de `fwdfadm` se establecen en *denegar todo*, excepto los métodos de autentificación de administración protegida y no protegida, que se establecen en contraseña de conexión NT. Los administradores principales del cortafuegos puede ver y modificar este registro, pero no pueden suprimirlo. Además, la contraseña del cortafuegos y SNK no son tipos de autentificación válidos para `fwdfadm`.

Nombre completo de usuario
Especifica una descripción del usuario.

Los campos siguientes corresponden a los métodos de autentificación. Pulse en las flechas para realizar su selección utilizando la lista de métodos de autentificación. Las opciones se explican en el apartado “Métodos de autentificación de usuario” en la página 81.

Telnet protegido Indica si la identidad de este usuario, cuando se conecta desde la red protegida, debe autentificarse de algún modo.

Telnet no protegido Indica si la identidad de este usuario, cuando se conecta desde la red no protegida, debe autentificarse de algún modo.

FTP protegido Especifica el nivel de autentificación que este usuario necesita para utilizar FTP para acceder al cortafuegos desde la red protegida.

FTP no protegido Especifica el nivel de autentificación que este usuario necesita para utilizar FTP para acceder al cortafuegos desde la red no protegida.

Socks protegido Especifica el método de autentificación Socks V5 para las conexiones del cliente Socks que proceden de la ubicación protegida del cortafuegos. Pulse en la flecha para realizar su selección utilizando la lista de opciones. Las opciones se explican en el apartado “Métodos de autentificación de usuario” en la página 81.

Socks no protegido Especifica el método de autentificación Socks V5 para las conexiones del cliente Socks que proceden de la ubicación no protegida del cortafuegos. Pulse en la flecha para realizar su selección utilizando la lista de opciones. Las opciones se explican en el apartado “Métodos de autentificación de usuario” en la página 81.

HTTP protegido Especifica un tipo de autentificación de ID de usuario/contraseña en las peticiones del proxy HTTP de salida. Pulse en la flecha para realizar su selección utilizando la lista de opciones. Las opciones se explican en el apartado “Métodos de autentificación de usuario” en la página 81.

El navegador solicita un ID de usuario y contraseña, por ello, si está utilizando SDI, especifique un passcode en la solicitud de contraseña.

Suministrada por el usuario debe reconocer que Socks/contraseña no puede dar soporte a diálogos interactivos y comportarse conforme a ello.

Administración protegida
Especifica el método de autentificación utilizado para conectarse desde el cliente de configuración a través de una interfaz protegida. Tenga en cuenta que, cuando se conecta localmente (seleccionando local en el panel de conexión), siempre se encuentra en un entorno protegido y, por lo tanto, éste es el método de autentificación que debe utilizar.

Administración no protegida
Especifica el método de autentificación utilizado para conectarse desde el cliente de configuración a través de una interfaz no protegida.

Clave SecureNet Especifica la secuencia de caracteres que ha de especificar un usuario remoto que disponga de una tarjeta de Claves SecureNet de AssureNet Pathways. Especifique el código de clave con el que también preparará la tarjeta de claves. Consulte la información de la clave SecureNet para obtener instrucciones acerca de la selección e instalación de un código de clave.

Notas:

a. Este campo no se utiliza para la tarjeta SecurID.

b. Debe crear una clave aleatoria exclusiva para cada usuario.

c. Cuando instale la clave en la tarjeta de claves SecureNet, utilice el procedimiento de instalación AssureNet Pathways y seleccione **Modalidad 5**.

Consulte el “Métodos de autentificación” en la página 85 para obtener más información.

Métodos de autentificación de usuario

Las opciones para la autentificación de usuario son:

Denegar todo El usuario tiene el acceso denegado.

Permitir todo No se necesita ninguna autentificación.

Contraseña de conexión NT

La contraseña de conexión NT es menos segura que la contraseña del cortafuegos. Sin embargo, si los usuarios ya se han definido en un dominio de Windows NT, puede utilizar la contraseña de conexión de Windows NT para que el usuario no necesite varias contraseñas.

Si elige este método de autentificación, el ID de usuario y la contraseña se validarán utilizando la base de datos de usuarios de Windows NT local. Si el cortafuegos se ha configurado para confiar en otros servidores de Windows NT, las definiciones de usuario se buscarán en estos servidores fiables.

Para que pueda establecerse una relación de fiabilidad entre el cortafuegos de Windows NT y los servidores de Windows NT fiables, debe definirse una conexión para permitir el tráfico de las comunicaciones TCP/IP entre las dos máquinas.

Defina esta conexión utilizando los servicios predefinidos siguientes:

1. Autentificación de controlador de dominio - que permite la utilización del Controlador de dominio para la autentificación del usuario
2. Difusiones generales de los Servicios de nombres NetBT - que permiten difusiones generales de los Servicios de nombres NetBIOS sobre TCP/IP

Utilice los programas de utilidad de configuración de Windows NT para definir las relaciones de fiabilidad.

Clave SecureNet La autentificación se realiza utilizando una clave AssureNet Pathways SecureNet.

En el campo Clave SecureNet, especifique el código de clave con el que también preparará la tarjeta de claves SecureNet.

Notas:

1. Debe crear una clave aleatoria exclusiva para cada usuario.
2. La clave aleatoria debe encontrarse entre el rango 1 a 377 para cada 8 valores octales
3. Cuando instale la clave en la tarjeta de claves SecureNet, utilice el procedimiento de instalación AssureNet Pathways y seleccione **Modalidad 5**.

Consulte el “Métodos de autentificación” en la página 85 para obtener más información.

Tarjeta SecurID La autentificación se realiza utilizando una tarjeta de seguridad Security Dynamics SecurID o tarjeta de área de PIN. *No* utilice el campo Clave SecureNet. El PIN debe definirse antes de utilizar este método de identificación con el IBM Firewall.

Para el FTP, la nueva modalidad PIN de SDI y siguiente modalidad de símbolos no reciben soporte.

Consulte el “Métodos de autentificación” en la página 85 para obtener más información.

Autentificación suministrada por el usuario 1, 2 y 3
La autentificación la suministra el usuario. En el cortafuegos, puede instalar hasta tres métodos de autentificación suministrada por el usuario. Para obtener información acerca de cómo crear y compilar una subrutina para la autentificación suministrada por el usuario, consulte el manual *IBM eNetwork Firewall - Manual de consulta*.

Contraseña del cortafuegos
Debe solicitarse una contraseña válida al usuario, que debe especificarla. Cuando se ha completado este panel, el IBM Firewall le solicita que especifique una contraseña para este nuevo usuario.

La contraseña del cortafuegos admite más contraseñas protegidas y normas de contraseñas que la contraseña de conexión de Windows NT, por lo tanto, es la opción que se recomienda para las contraseñas.

Solicitar cambio al usuario Pulse en Sí o No para indicar si el usuario debe cambiar su contraseña la próxima vez que se autentifique.

Bloquear contraseña Pulse en Sí o No para indicar si la contraseña está bloqueada. Se establece en Sí cuando se excede el número máximo de conexiones anómalas o cuando la contraseña no se ha utilizado durante el número de semanas que se especifique en Tiempo máximo antes del bloqueo.

El administrador puede establecer este campo en sí para que un usuario no pueda utilizar la autentificación de contraseña.

Notas:

1. Las contraseñas son sensibles a las mayúsculas y minúsculas. Si especifica una contraseña de usuario utilizando mayúsculas y minúsculas mezcladas, el usuario deberá especificar la contraseña de forma idéntica. Si tiene estaciones de trabajo que sólo funcionan con mayúsculas, especifique las contraseñas de esos usuarios en mayúsculas.
2. El sistema operativo le permite definir normas de contraseñas. Estas normas de contraseñas se aplican cuando un usuario cambia su contraseña, pero no cuando un administrador se encarga de realizar los cambios de las contraseñas. Las normas para las contraseñas son las siguientes:

   Días para advertencia antes de la caducidad (días) Número de días previos a la caducidad de la contraseña y durante los cuales el cortafuegos ofrecerá al usuario la opción de cambiar la contraseña.

   Semanas máximas antes de la caducidad Número de semanas que han de transcurrir antes de que se solicite al usuario que cambie la contraseña.

   Semanas máximas antes del bloqueo Número de semanas durante las que no se utiliza la contraseña antes de que se bloquee.

   Reintentos de conexión máximos permitidos Número máximo de intentos de conexión no satisfactorios antes de que se bloquee la contraseña.

   Contraseñas antes de la reutilización Número de contraseñas almacenadas en la lista del historial de contraseñas. La contraseña no puede cambiarse por ninguna contraseña que esté actualmente en la lista del historial. Este parámetros sólo es válido si Semanas antes de la reutilización de la contraseña es cero.

   Semanas antes de la reutilización de la contraseña Número de semanas que las contraseñas se conservan en la lista del historial de contraseñas. La contraseña no puede cambiarse por ninguna contraseña que esté actualmente en la lista del historial.

   Longitud mínima Número mínimo de caracteres de una contraseña.

   Caracteres alfabéticos mínimos Número mínimo de caracteres alfabéticos de una contraseña.

   Mínimo de otros caracteres Número mínimo de caracteres no alfabéticos de una contraseña.

Caracteres repetidos máximos Número máximo de veces que puede repetirse un carácter en la contraseña.

Caracteres distintos mínimos Número mínimo de caracteres distintos de la contraseña.

Pulse en la pestaña **Contraseña del cortafuegos** para personalizar estos valores para cada usuario, como se muestra en la Figura 24.

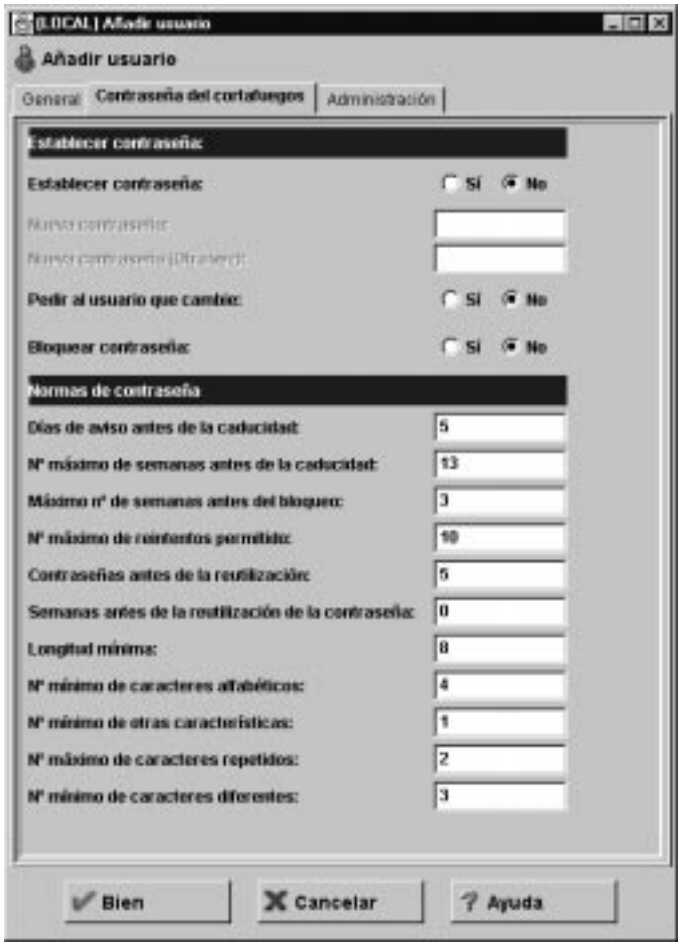

Figura 24. Pestaña Contraseña del cortafuegos

Cambio del acceso de un usuario

Tras añadir un usuario al cortafuegos, puede cambiar los atributos de seguridad de ese usuario en el cuadro de diálogo **Modificar usuario**.

1. Seleccione el usuario que desea cambiar en el cuadro de diálogo **Usuarios** y pulse en **Abrir**.
2. Cuando aparezca el cuadro de diálogo **Modificar usuario**, cambie los campos correspondientes. Consulte el apartado “Adición de un usuario al IBM Firewall” en la página 75 para conocer la lista de los atributos de usuario que puede cambiar.

3. Cuando haya completado los cambios, pulse en **Bien**.

Supresión de un usuario del IBM Firewall

Nota: No suprima los usuarios `fwdfuser` ni `fwdfadm`.

Para suprimir un usuario, pulse en **Suprimir** en el panel **Lista del usuario**.

Nivel de autorización del administrador por funciones

Sólo el *administrador principal del cortafuegos* puede crear y modificar administradores y determinar para qué funciones del cortafuegos tendrán autorización. Por ejemplo, puede limitar a un administrador en particular a tener sólo autorización para realizar las funciones Usuarios y Supervisor de registro.

En el cuadro de diálogo **Añadir usuario**, seleccione Administrador del cortafuegos para el campo **Nivel de autorización**. Consulte el apartado “Adición de un usuario al IBM Firewall” en la página 75 para obtener más detalles acerca de cómo cumplimentar el cuadro de diálogo **Añadir usuario**.

A continuación, seleccione la pestaña **Administrador** que se encuentra en la parte superior del cuadro de diálogo **Añadir usuario**. Seleccione las funciones que el administrador estará autorizado a utilizar.

Métodos de autentificación

A continuación se muestran diversos métodos de autentificación de usuario

Denegar todo

El IBM Firewall prohíbe el acceso al servidor.

Permitir todo

No es necesaria ninguna autentificación. El servidor no intenta autentificarle; en lugar de ello, continúa con un indicador de mandatos para permitirle acceder a un sistema principal externo.

Contraseña del cortafuegos

El servidor le solicita la contraseña del cortafuegos (que no se visualizará) antes de permitirle continuar.

```
Password:
```

Escriba su contraseña del cortafuegos. Se trata de la misma contraseña con la que se ha añadido el nombre de usuario al cortafuegos.

Autentificación de tarjeta SecurID

Utilice este método si tiene una tarjeta SecurID y su red utiliza Security Dynamics ACE/Server.

El servidor proxy le solicitará su PASSCODE (que no se visualizará) antes de permitirle continuar.

```
Enter PASSCODE:
```

En este punto, escriba su código PIN SecurID de 4 dígitos seguido de una coma y, a continuación, el código de la tarjeta SecurID. Por ejemplo, para conectarse como usuario NEWUSER con un PIN asignado de 1234, cuando la tarjeta SecurID muestre el código 179091, deberá escribir:

```
login: NEWUSER
Enter PASSCODE: 1234,179091
```

Si los usuarios utilizan inicialmente FTP, la autentificación de la tarjeta SecurID no será satisfactoria porque FTP no tiene una opción que permita un cambio de contraseña. Los usuarios deben utilizar telnet la primera vez que intenten realizar la autentificación de la tarjeta SecurID, mediante lo cual crearán un PIN. Los usuarios podrán seguir utilizando ese PIN para autentificaciones posteriores, como FTP, HTTP, etc.

Si la tarjeta SecurID está en la nueva modalidad de PIN, deberá definir el PIN antes de utilizar este método de autentificación con el IBM Firewall.

Autentificación de clave SecureNet

Utilice este método si tiene una tarjeta de Claves SecureNet de AssureNet Pathways. Cuando inicialice la tarjeta SNK, utilice lo siguiente:

- Formato de visualización (hexadecimal)
- Posibilidad ERASE (activación o desactivación)
- Posibilidad de solicitud de un solo dígito (desactivación)

El servidor proxy le solicitará la respuesta que le proporciona la tarjeta de claves SecureNet antes de permitirle continuar.

```
Use SNK for challenge
######## for user user_id
Ed:
```

La respuesta `########` es el número de 8 dígitos que ha entrado en la tarjeta de claves SecureNet.

1. Cuando reciba esta solicitud, active la tarjeta de claves SecureNet y escriba su código PIN. El código PIN se le facilitó con la tarjeta.
2. Escriba la respuesta tal como se la proporciona el servidor.

   Por ejemplo: se conecta al servidor; el servidor le solicita:

   ```
   Use SNK for challenge
      78987648 for user NEWUSER
   Ed:
   ```

   Escriba el valor 78987648 en la tarjeta de claves SecureNet. A continuación, la tarjeta visualiza la respuesta, que debe proporcionar al servidor proxy.
3. Escriba la respuesta en el servidor.

   Si la tarjeta de claves SecureNet ha visualizado `8AE222A9` como respuesta a su acción, escriba `8AE222A9` en el servidor:

   ```
   logon: NEWUSER
      Use SNK for challenge 78987648 for user NEWUSER
   Ed:8AE222A9
   ```

SecurNetKey (SNK) ahora se denomina Defender Handheld Token** (DHT) cambio realizado por AXENT** Technologies.

Contraseña de conexión NT

Si elige este método de autentificación, el ID de usuario y la contraseña se validarán utilizando la base de datos de usuarios de Windows NT local. Si el cortafuegos se ha configurado para confiar en otros servidores de Windows NT, las definiciones de usuario se buscarán en estos servidores fiables.

Autentificación suministrada por el usuario 1, 2 y 3

Puede utilizar la Autentificación suministrada por el usuario para FTP y telnet. Consulte el manual *IBM eNetwork Firewall - Manual de consulta* para obtener más información.

Capítulo 13. Configuración de servidores proxy

Este capítulo contiene información general acerca de cómo configurar y utilizar los servidores proxy desde las estaciones de trabajo tanto en el interior como en el exterior de la red protegida.

Proxy HTTP

proxy HTTP gestiona con eficacia las peticiones del navegador a través de IBM Firewall, eliminando la necesidad de un servidor socks para navegar por la Web. Los usuarios pueden acceder a la útil información de Internet sin comprometer la seguridad de sus redes internas y sin alterar su entorno de cliente para implementar el proxy HTTP.

El proxy HTTP no es un servidor. El usuario final no puede cargar archivos del proxy ni colocar archivos en el proxy. Además, no se trata de un proxy con colocación en memoria. En el cortafuegos no se almacena nada por parte de una petición HTTP.

Sesiones continuas

Las conexiones continuas permiten a un cliente y a un servidor señalar el cierre de una conexión TCP. Esta señalización utiliza un campo de cabecera de conexión.

El proxy del IBM Firewall da soporte a conexiones persistentes entre un cliente y el proxy. La condición de *peticiones continuas máximas* y la condición de *tiempo de espera de conexión continua* controlan la duración de esa conexión. Si se alcanza una de estas condiciones, la conexión del socket entre el proxy y el cliente se cerrará. Si no se satisfacen la condición de *peticiones continuas máximas* y la condición de *tiempo de espera de conexión continua*, la conexión permanecerá abierta y será responsabilidad del cliente determinar cuándo se ha completado una petición.

Si se determina de forma incorrecta, ello puede dar como resultado la visualización de una pantalla en la que se indique tráfico en la conexión cuando éste es inexistente. Un ejemplo de ello sería el icono con animación de un navegador que se ejecuta de forma continua incluso cuando ya se ha cargado por completo la página. Pulse en **Detener** para detener la animación. Consulte “Peticiones continuas máximas” en la página 92 y “Tiempo de espera de conexión continua” en la página 92 para obtener información acerca de estos parámetros.

Configuración del proxy HTTP utilizando el cliente de configuración

Para configurar el Proxy HTTP, realice lo siguiente:

1. Para que el funcionamiento del Proxy HTTP sera correcto, deberá permitir consultas DNS. Una sencilla forma de hacerlo es efectuando una pulsación en Política de seguridad desde la carpeta Administración del sistema del árbol de navegación del cliente y pulsando en Permitir consultas DNS.
2. Activar filtros

3. Añadir una conexión. Consulte el apartado “Ejemplo de proxy HTTP” en la página 55 para ver un ejemplo de cómo configurar una conexión en la ubicación no protegida de la red.
4. Para configurar el Proxy HTTP, seleccione HTTP en el árbol de navegación del cliente de configuración. El IBM Firewall visualiza el cuadro de diálogo **Proxy HTTP**, tal como se muestra en la Figura 25.

Figura 25. HTTP

5. Para detener el proxy, seleccione `mi pc/panel de control/servicios`. Elija el Proxy HTTP del IBM Firewall y pulse en *Detener*.

   El phttpd ejecutable es un servicio del sistema que se inicia automáticamente cuando se arranca el sistema.

Configure los parámetros en el cuadro de diálogo **Proxy HTTP**. Si cambia algún parámetro, el servicio del proxy del cortafuegos se detendrá y volverá a iniciarse. Las peticiones de los usuarios del proxy activo finalizarán hasta que el proxy vuelva a iniciarse (unos segundos).

Número de puerta del proxy

Utilice este parámetro para especificar el número de puerta cuyas peticiones debe atender el proxy. Si cambia el número de puerta, deberá configurar filtros para permitir o denegar el flujo a través de las puertas. Los números de puertas inferiores a 1024 se reservan para las aplicaciones TCP/IP. Las puertas que suelen utilizarse para los servidores proxy de la Web son 8080 y 8088.

Las normas de filtros por omisión se han establecido para no permitir el tráfico de entrada no protegido en la puerta 8080, pero sí permitir el tráfico protegido en esa misma puerta. El proxy sólo rechazará los requisitos del proxy no protegido. El valor por omisión es `8080`. Si lo cambia, el número de la puerta también deberá cambiarse en los Servicios que se han definido para esta configuración. Si cambia alguno de estos valores deberá rearrancar el proceso phttpd.

Longitud de almacenamiento intermedio de contenido máxima

Utilice este parámetro para establecer el tamaño del almacenamiento intermedio para los datos dinámicos que genera un servidor. Los datos dinámicos son la salida de los programas CGI, de la ubicación del servidor y de los programas de la API. Son datos que no proceden de un proxy.

Especifique el valor en kilobytes (K). El valor por omisión es `50K`.

Tamaño de agrupación de hebras

Utilice este parámetro para definir el número fijo de hebras que desea tener activas a la vez. El proxy retiene las nuevas peticiones hasta que finaliza otra petición y las hebras vuelven a estar disponibles. Por lo general, cuanto más posibilidades tenga una máquina, más alto deberá ser el valor para este parámetro. Si una máquina parece necesitar demasiado tiempo para la realización de tareas generales, como el intercambio de memoria, reduzca este valor. Especifique un número entero, como 60, por ejemplo. El valor por omisión es `200`.

Nivel de usuarios

Este parámetro indica al proxy qué nivel de usuarios debe autentificar. Especifique el valor como todos, nuevo o ninguno. El valor por omisión es ninguno. Los valores son:

todos A todos los navegadores se les enviará la respuesta de autentificación del proxy para indicar que el navegador debe solicitar al usuario un ID de usuario y una contraseña. Si el navegador no da soporte a la respuesta de autentificación del proxy, se visualizará la página de error que así lo indica. Si el navegador sí le da soporte, se visualizará el indicador de solicitud de ID de usuario y contraseña.

nuevo Se utiliza como ayuda para la migración. Sólo devolverá una respuesta de autentificación de proxy 407, para indicar al navegador que emita una identificación de solicitud de ID de usuario/contraseña, a un navegador del cliente que se identifique a sí mismo como navegador HTTP/1.1. Puede establecer un conmutador en el Internet Explorer 4.0 para que emita las peticiones con el identificador HTTP/1.1. Netscape y otros se identifican a sí mismos como peticiones HTTP/1.0.

ninguno No comprueba las peticiones del navegador. No solicita ningún ID de usuario/contraseña.

Tiempo de espera

Este parámetro indica al proxy el tiempo que debe esperar la respuesta de un cliente antes de solicitar al usuario que vuelva a autentificarse. Un usuario se autentifica a partir de la dirección IP e ID de usuario específicos proporcionados en el momento de la autentificación original para este período de tiempo de desocupación. Especifique el tiempo en minutos. El valor por omisión es de 60 minutos.

Mientras el usuario esté navegando activamente, esta ventana de tiempo no caducará.

Peticiones continuas máximas

Este parámetro indica el número máximo de peticiones que un proxy puede recibir en una conexión continua HTTP/1.1. Es una herramienta para el rendimiento que tiene un impacto directo sobre el tiempo de espera de la autentificación. Mientras se encuentra en una sesión continua, no se realiza ninguna prueba de la autentificación de un usuario hasta que finaliza la sesión continua. Especifique el valor como un número entero, por ejemplo, 25. El valor por omisión es 5.

Tiempo de espera de conexión continua

Este parámetro indica el tiempo en segundos que debe conservarse una conexión continua HTTP/1.1 con un navegador de cliente una vez que un navegador compatible con HTTP/1.1 inicia una sesión con el proxy. Es una herramienta para el rendimiento que tiene un impacto directo sobre el tiempo de espera de la autentificación. Mientras se encuentra en una sesión continua, no se realiza ninguna prueba de la autentificación de un usuario hasta que finaliza la sesión continua. Especifique el tiempo en segundos. El valor por omisión es de 60 minutos.

Gestión del registro HTTP

Este parámetro indica al proxy que registre el inicio/conclusión y todas las peticiones del proxy en el registro del cortafuegos. Utiliza el nivel de registro LOG_NOTICE. Actívelo si desea supervisar la actividad de las peticiones HTTP. Los sucesos se registran en el recurso del `registro del cortafuegos`.

Configuración del navegador

El navegador del cliente puede configurarse para conectarse a la puerta a la que el proxy HTTP atiende.

Si se utiliza HTTPS, apunte también al proxy HTTP del IBM Firewall para el proxy protegido.

Si quiere representar su navegador Internet Explorer como un navegador HTTP/1.1 al proxy, realice las siguientes acciones:

- Abra el menú desplegable *Ver*.
- Seleccione *Opciones*.
- Seleccione la pestaña *Avanzadas*.
- Desplácese abajo hasta los valores de HTTP1.1 y active los conmutadores.

Conexiones SSL

Se da soporte a los túneles SSL para la Conexión protegida HTTP con otros servidores. En este caso, IBM Firewall actúa como pasarela. El túnel parte del cliente, atraviesa el cortafuegos y llega al servidor. Utilice la puerta estándar 443 para la Conexión protegida HTTP, como se muestra en el ejemplo siguiente:

```
https://www.ibm.com:443
```

Utilice también el servicio predefinido `Proxy HTTPS de 2/2`.

Si se utiliza HTTPS, apunte también al proxy HTTP del IBM Firewall para el proxy protegido.

Para obtener más información, consulte el apartado “Ejemplo de proxy HTTP” en la página 55.

Métodos que reciben soporte

El proxy HTTP soporta los métodos siguientes, que constituyen formas distintas de consultar Internet:

- FTP
- Gopher
- HTTP
- HTTPS
- WAIS

Ejemplo de salida del registro para el Proxy HTTP

A continuación se muestra un ejemplo de salida de registro de peticiones get autentificadas del Proxy HTTP.

```
Mar 06 14:04:50 1998 fire3: ICA2140i: httpd --> Autentificación
del proxy HTTP NO SATISFACTORIA para el usuario <Desconocido>,
en 9.67.140.162, a través de la red protegida ... RC:30.
Mar 06 14:04:50 1998 fire3: ICA2099i: httpd --> Estado: 407 de cliente
9.67.140.162, que ha solicitado "GET http://9.67.128.69/ HTTP/1.1" de
0 bytes.
Mar 06 14:05:05 1998 fire3: ICA2024i: El usuario Pedro se ha
autentificado satisfactoriamente la autentificación de NT desde la
red protegida:9.67.140.162.
Mar 06 14:05:05 1998 fire3: ICA2169i: El usuario Pedro se ha
autentificado satisfactoriamente
para el servidor HTTP mediante NT desde la red protegida:9.67.140.162.
Mar 06 14:05:05 1998 fire3: ICA2140i: httpd --> Autentificación
del proxy HTTP SATISFACTORIA para el usuario (Pedro), en
9.67.140.162, a través de la red protegida ...RC:1.
Mar 06 14:05:05 1998 fire3: ICA2099i: httpd --> Estado: 200
del cliente 9.67.140.162, que ha solicitado "GET
http://9.67.128.69/HTTP/1.1" de 2693 bytes.
Mar 06 14:05:05 1998 fire3: ICA2140i: httpd --> Autentificación
del proxy HTTP SATISFACTORIA para el usuario (Pedro), en
9.67.140.162, a través de la red protegida ...RC:1.
Mar 06 14:05:06 1998 fire3: ICA2099i: httpd --> Estado: 200 del
cliente 9.67.140.162, que ha solicitado "GET
http://9.67.128.69/Admin/lgsplash.gif HTTP/1.1"
de 211 bytes.
Mar 06 14:05:10 1998 fire3: ICA2140i: httpd --> Autentificación
del proxy HTTP
SATISFACTORIA para el usuario Pedro en 9.67.140.162, a través de la
red protegida ...RC:1.
Mar 06 14:05:10 1998 fire3: ICA2099i: httpd --> Estado: 200 del
cliente 9.67.140.162, que ha solicitado "GET
http://9.67.128.69/Admin/lgmast.gif HTTP/1.1"
de 211 bytes.
```

La actividad del registro es la siguiente:

- ICA2099i - muestra el código de retorno 407 y significa que la autentificación ha resultado anómala para la petición get.

  A continuación el navegador solicita al usuario alguna autentificación. El navegador pide un id de usuario y una contraseña.

- ICA2140i - la autentificación ha resultado satisfactoria para el usuario Pedro.

La autentificación se produce en cada petición get para cada elemento de la página Web.

FTP

1. Utilice el proxy FTP para acceder al sistema principal del cortafuegos. (Utilizaremos `ftp_gw.domain.net.com` como nombre de sistema principal para el cortafuegos).

   ```
   ftp ftp_gw.domain.net.com
   ```

   El servidor proxy le preguntará su nombre de usuario:

   ```
   login:
   ```

2. Especifique su nombre de usuario con autorización para utilizar el cortafuegos:

   ```
   login: jane_doe
   ```

El servidor validará su identidad en función del esquema de autentificación que se seleccionó al añadirse su nombre de usuario al cortafuegos (consulte el apartado “Adición de un usuario al IBM Firewall” en la página 75). Consulte el apartado “Métodos de autentificación” en la página 85 para obtener información acerca de cómo los servidores proxy autentifican usuarios.

Tras la autentificación, el servidor proxy visualiza un indicador de mandatos FTP.

```
ftp>
```

Utilice los mandatos `quote` y `site` de FTP para conectarse al sistema principal externo:

```
ftp> quote site forhost.network.outside.com
```

Ahora, el sistema principal externo le solicitará un nombre de usuario y una contraseña para que pueda conectarse. Probablemente se trata de un nombre de usuario y contraseña distintos de los que utiliza para FTP para el cortafuegos.

El valor del tiempo de espera por omisión para la conexión es de 60 segundos y para el proxy desocupado es de 7200 segundos. Para cambiar los valores de tiempo de espera por omisión, consulte “Alteración temporal de los valores de tiempo de espera de los proxies FTP y Telnet” en la página 96.

FTP Transparente

Puede ejecutar ftp de forma transparente a través del cortafuegos. Los proxies transparentes no necesitan ninguna autentificación del cortafuegos, por lo que los usuarios de los proxies transparentes no tienen que definirse como usuarios de proxy de cortafuegos. Los proxies transparentes sólo están permitidos desde la ubicación protegida del cortafuegos a la ubicación no protegida del cortafuegos. Para que el proxy transparente funcione, deberá seleccionarlo en el panel del cliente de configuración Política de seguridad.

1. Utilice ftp para acceder al sistema principal del cortafuegos. (Utilizaremos `ftp_gw.domain.net.com` como nombre de sistema principal para el cortafuegos.)

   ```
   ftp ftp_gw.domain.net.com
   ```

2. El servidor proxy le preguntará su nombre de usuario:

```
USER:
```

3. Escriba su nombre de usuario en la red no protegida:

   ```
   USER: nombre usuario@nombre_sistema principal_ubicación_remota
   ```

4. A continuación, el sistema principal de destino le solicitará la contraseña del `username` especificado en el paso anterior.

   ```
   password:
   ```

5. Escriba su contraseña.

El valor del tiempo de espera por omisión para la conexión es de 60 segundos y para el proxy desocupado es de 7200 segundos (dos horas). Para cambiar los valores de tiempo de espera por omisión, consulte “Alteración temporal de los valores de tiempo de espera de los proxies FTP y Telnet” en la página 96.

Telnet

Utilice el proxy telnet para conectarse al servidor proxy del cortafuegos. Puede utilizar el nombre del sistema principal o la dirección de Internet. A continuación, tras la autentificación de sus credenciales, deberá utilizar el mandato telnet en el cortafuegos para conectarse al sistema principal deseado. Por ejemplo, utilizaremos telnet desde el interior de la red protegida, atravesando el cortafuegos con el nombre del sistema principal `telnet_gw`, para acceder al destino que nos interesa, `forhost.network.outside.com`.

1. Para iniciar el proceso, utilice telnet para acceder al sistema principal del cortafuegos. (Utilizaremos telnet_gw.domain.net.com como nombre del sistema principal para el cortafuegos.)

   ```
   telnet telnet_gw.domain.net.com
   ```

2. El servidor proxy le preguntará su nombre de usuario:

   ```
   login:
   ```

3. Especifique su nombre de usuario con autorización para utilizar el cortafuegos:

   ```
   login: jane_doe
   ```

El servidor validará su identidad en función del esquema de autentificación que se seleccionó al añadirse su nombre de usuario al cortafuegos (consulte el apartado “Adición de un usuario al IBM Firewall” en la página 75). Consulte el apartado “Métodos de autentificación” en la página 85 para obtener información acerca de cómo los servidores proxy autentifican usuarios.

Utilizará el shell oneact. Con el daemon del proxy telnet del IBM Firewall, todas las comunicaciones pasan a través del cortafuegos.

Si utiliza el shell oneact, tras haberse autentificado, el servidor proxy visualizará:

```
ENTER DESIRED HOST:
```

Escriba

```
telnet forhost.network.outside.com
```

El sistema principal externo le solicitará el nombre de usuario y la contraseña, pues ese sistema principal le reconoce. Éstos podrían ser distintos del nombre de usuario y contraseña que ha utilizado en el servidor proxy del cortafuegos.

El valor del tiempo de espera por omisión para la conexión es de 60 segundos y para el proxy desocupado es de 7200 segundos. Para cambiar los valores de tiempo de espera por omisión, consulte “Alteración temporal de los valores de tiempo de espera de los proxies FTP y Telnet” en la página 96.

Telnet Transparente

Puede ejecutar telnet de forma transparente a través del cortafuegos. Los proxies transparentes no necesitan ninguna autentificación del cortafuegos, por lo que no es necesario definir a los usuarios de los proxies transparentes como usuarios del proxy del cortafuegos. Los proxies transparentes sólo están permitidos desde la ubicación protegida del cortafuegos hacia la ubicación no protegida del cortafuegos. Para que el proxy transparente funcione, deberá seleccionarlo en el panel del cliente de configuración Política de seguridad.

1. Utilice telnet para acceder al sistema principal del cortafuegos. (Utilizaremos `ftp_gw.domain.net.com` como el nombre de nuestro sistema principal.)

   ```
   telnet telnet_gw.domain.net.com
   ```

2. El servidor proxy le preguntará su nombre de usuario:

   ```
   Login:
   ```

3. Escriba su nombre de usuario en la red no protegida:

   ```
   Login@sistema_principal_remoto
   ```

El sistema principal externo le solicitará el nombre de usuario y la contraseña, pues ese sistema principal le reconoce. Éstos podrían ser distintos del nombre de usuario y contraseña que ha utilizado en el servidor proxy del cortafuegos.

El valor del tiempo de espera por omisión para la conexión es de 60 segundos y para el proxy desocupado es de 7200 segundos. Para cambiar los valores de tiempo de espera por omisión, consulte “Alteración temporal de los valores de tiempo de espera de los proxies FTP y Telnet”.

Alteración temporal de los valores de tiempo de espera de los proxies FTP y Telnet

Tanto FTP como Telnet tienen valores de tiempo de espera para conectarse y también esperas de desocupación. Como valor por omisión, debe existir actividad en la sesión una vez cada 60 segundos, como mínimo, durante la conexión y autentificación del usuario. Esto se conoce como loginTimeout (Tiempo de espera de conexión).

Cuando la conexión se ha completado satisfactoriamente, debe existir actividad en la sesión una vez cada 7200 segundos, como mínimo, o la sesión se desconectará.

Puede alterar temporalmente estos valores por omisión creando un archivo `fwTimeout.cfg` en el directorio `ROOTDIR\config` especificando nuevos valores de tiempo de espera en segundos. El archivo `fwTimeout.cfg` debe tener el formato siguiente.

```
telnet
proxyTimeout=7200
loginTimeout=60

ftp
proxyTimeout=7200
loginTimeout=60
```

Capítulo 14. Supervisión del registro del cortafuegos

En este capítulo se describe cómo supervisar el registro de alertas en tiempo real. Cuando se viola un umbral configurado, se genera una alerta.

El IBM Firewall supervisa los mensajes enviados al registro del cortafuegos en busca de posibles situaciones de crisis basándose en los umbrales definidos por el usuario. En caso de producirse una violación de umbral, el cortafuegos entrega una alerta, de la forma que ha especificado el administrador del cortafuegos.

Definiciones de umbral

Un umbral se compone de parámetros de recuento y de tiempo — si un recuento (número de sucesos específicos) se excede en el tiempo especificado (minutos), ello indica que se ha violado el umbral y se genera un mensaje de alerta. El Supervisor de registro reconoce cuatros tipos de umbrales:

1. Anomalías de autentificación totales
2. Anomalías de autentificación para un ID de usuario determinado
3. Anomalías de autentificación que se originan desde un sistema principal determinado
4. Apariciones de un código de mensaje en el registro

Todos los umbrales pueden configurarse utilizando el cliente de configuración o la interfaz de la línea de mandatos. El IBM Firewall toma automáticamente cualquier cambio realizado en las definiciones de los umbrales.

Mensajes de alerta

Cuando se ha alcanzado un umbral, IBM Firewall genera un mensaje de alerta. La entrega del mensaje de alerta puede manifestarse en cualquiera de las cuatro formas siguientes:

1. Entrada en un archivo de registro:
   - Mediante el recurso `registro de alertas`, que puede configurarse utilizando el cliente de configuración o la línea de mandatos.
   - En el `recurso del cortafuegos`
2. Envíe un mensaje de correo a una lista de usuarios
3. Buscapersonas, según su configuración. Consulte el apartado “Soporte de notificación por buscapersonas” en la página 101.
4. Ejecución de un mandato definido por el usuario, con el mensaje de alerta como primer parámetro

El mensaje de alerta contiene información relacionada con la violación de umbral en particular. Por ejemplo:

```
ICA0001e: ALERTA – 20 anomalías de autentificación.
ICA0002e: ALERTA – 10 anomalías de autentificación para el usuario raíz.
ICA0003e: ALERTA – 15 anomalías de autentificación del sistema principal 56.67.78.89
ICA0004e: ALERTA – Código ICA1234e con 3 entradas de registro.
```

No se supervisan los mensajes de alerta y otros mensajes originados por el Supervisor de registro.

Configuración del supervisor de registro utilizando el cliente de configuración

En este apartado se describe cómo utilizar el cliente de configuración para configurar el supervisor de registro en tiempo real. Seleccione Registros del sistema en el árbol de navegación del cliente de configuración. Efectúe una doble pulsación en el icono de la carpeta de archivos para ampliar la vista. Pulse en **Umbrales del supervisor de registro**.

En el cuadro de diálogo **Administración de umbrales de supervisor de registro**, puede añadir, cambiar o suprimir una definición de umbral.

Adición de un supervisor de registro

Para añadir una definición de umbral, seleccione **NUEVO** en el cuadro de diálogo **Administración de umbrales de supervisor de registro** y pulse en **Abrir**. Aparecerá el cuadro de diálogo **Añadir supervisor de registro**. Cumplimente los campos siguientes:

1. Pulse en la flecha **Tipo de clase** para realizar su selección partir de la lista de tipos de clase. Los tipos de clase son:
   - Notificación por correo
   - Ejecutar mandato
   - Por umbral de anomalías de autentificación de usuario
   - Umbral de anomalías de autentificación totales
   - Por umbral de anomalías de autentificación del sistema principal
   - Umbral de mensaje
2. Si ha seleccionado el tipo de clase: Notificación por correo, especifique una dirección de correo electrónico. Puede definir varias clases de notificación por correo.

   Todos los mensajes de violación de umbral se envían a la dirección de correo electrónico especificada.
3. Si ha seleccionado el tipo de clase: Ejecutar mandato, especifique un nombre de archivo de mandato.

   El supervisor de registro ejecutará este mandato con el mensaje de alerta como primer parámetro. Sólo puede definir una clase de tipo ejecutar mandato.
4. Si ha seleccionado el tipo de clase: Umbral de mensaje, especifique un código de mensaje, el código estándar de los mensajes de registro de IBM Firewall que desea que se supervise.
5. Si ha seleccionado una de las clases de umbrales, cumplimente el campo de recuento de umbral.

   El recuento de umbral es el número máximo de sucesos anómalos permitidos en el período de tiempo especificado.
6. Si ha seleccionado una de las clases de umbral, cumplimente el campo de tiempo de umbral.

   El tiempo de umbral es el número de minutos desde que se produce la primera aparición de un suceso.

7. Si ha seleccionado una de las clases de umbral, efectúe una pulsación en Sí o en No para indicar si desea o no que se active una notificación por buscapersonas.
8. La especificación de un comentario es opcional.
9. Pulse en **Bien**.

Cambio de una definición de umbral

Para cambiar una definición de umbral, seleccione el elemento que va a cambiarse en el cuadro de diálogo **Administración de umbrales de supervisor de registro** y pulse en **Abrir**. Aparecerá el cuadro de diálogo **Cambiar supervisor de registro**.

1. Escriba los cambios que desea aplicar en los campos de recuento de umbral y de tiempo de umbral.

   El recuento de umbral es el número máximo de mensajes de autentificación anómala que pueden detectarse en el período de tiempo especificado. El tiempo de umbral es el número de minutos desde que se produce la primera aparición de un mensaje.
2. Pulse en **Bien**.

Supresión de una definición de umbral

Para suprimir una definición de umbral, seleccione el elemento que va a suprimirse en el cuadro de diálogo **Umbrales del supervisor de registro** y pulse en **Suprimir**. Se le solicitará que confirme la supresión. Pulse en **Sí** para confirmar la acción. Tenga en cuenta que la supresión no implica la supresión del archivo de registro. Significa suprimir la definición.

Soporte de notificación por buscapersonas

El cortafuegos puede enviar un mensaje al buscapersonas del administrador del sistema cuando se producen alertas de intrusión en el cortafuegos. Para definir un soporte de notificación por buscapersonas, deberá configurar los tres componentes del buscapersonas siguientes.

1. Personalización de mandatos - Este componente debe crearse y modificarse utilizando el cliente de configuración. Por omisión, toma el mandato del buscapersonas, que lo utiliza el supervisor de registros y que puede utilizarse desde la línea de mandatos. Este componente contendrá una entrada exclusiva que definirá el entorno del buscapersonas. Consulte el apartado “Personalización de mandatos” en la página 103 para obtener más información acerca de la definición y personalización de este componente.
2. Administración de proveedores de telefonía - Deberá definir un proveedor de telefonía adecuado antes de conectar el módem. Este componente contiene una lista con los proveedores de telefonía por omisión que se utilizan en los Estados Unidos. Si el proveedor de telefonía que está utilizando no es uno de los que se listan, añada su proveedor de telefonía a este componente. Consulte el apartado “Administración de proveedores de telefonía” en la página 104 para obtener más información.

   Valide los números de teléfono de los proveedores de telefonía existentes obteniéndolos de éstos. Cuando hable con los proveedores de telefonía, asegúrese de obtener el número de teléfono del módem del proveedor de

telefonía y los otros valores que son válidos para el servicio en particular que ha adquirido.

3. Administración de modems - Antes de conectar el módem, deberá crear definiciones de módem adecuadas. Estas definiciones contendrán toda la información relevante del módem que va a utilizar el soporte de notificación por buscapersonas. Este componente contiene una lista de los modems que puede elegir. Sin embargo, a esta lista puede añadir algunos modems que podrían no ser compatibles con el soporte del proveedor de telefonía. Consulte el apartado “Administración de modems” en la página 106 para obtener más información acerca del mantenimiento de las definiciones de módem.

Nota: El IBM Firewall da soporte al protocolo de comunicaciones Tele-AlphaNumeric Protocol (TAP) para el soporte de notificación por buscapersonas.

Proveedores de telefonía y modems que reciben soporte

El archivo de bases de datos de proveedores de telefonía contiene una lista con los proveedores de telefonía y los parámetros de transmisión que se relacionan a éstos. Puede añadir otros proveedores de telefonía. Algunos de los parámetros, además del nombre del proveedor de telefonía y el número de teléfono del módem, son:

- La longitud máxima del mensaje de un buscapersonas alfanumérico y los dígitos máximos de un buscapersonas numérico
- La velocidad en baudios, la paridad y la longitud de datos y bits de parada

Antes de utilizar un proveedor de telefonía determinado, asegúrese de que el proveedor de telefonía utiliza el protocolo TAP.

El código del buscapersonas dispone de definiciones de módem por omisión. Son:

- IBM MOD 448 14400 bps
- IBM 5853 2400 bps
- IBM 7852 28800 bps
- IBM 7855 2400 bps
- Compatible con Hayes genérico
- US Robotics Courier 9600 bps
- Zoom V.34

Configuración del soporte de notificación por buscapersonas

La Configuración de buscapersonas se utiliza para configurar el archivo de personalización de mandatos y para el mantenimiento de los proveedores de telefonía y los modems. Si está utilizando un buscapersonas, debe utilizar Configuración de buscapersonas para personalizar el entorno del buscapersonas antes de utilizar el Supervisor de registro.

Antes de empezar, debe obtener los números de teléfono correctos de los modems, el ID del buscapersonas y los parámetros del módem del proveedor de telefonía.

Para configurar el soporte de notificación por buscapersonas, seleccione Administración del sistema en el árbol de navegación del cliente de configuración. Efectúe una doble pulsación en el icono de la carpeta de archivos para ampliar la vista. Seleccione **Registros del sistema**. Efectúe una doble pulsación en el icono de la carpeta de archivos para ampliar la vista. Seleccione **Configuración de buscapersonas**.

Personalización de mandatos

Cuando selecciona **Configuración de buscapersonas** puede seleccionar el proveedor y módem que desea utilizar y escribir un mensaje para el buscapersonas.

Valores de la personalización de mandatos

Cuando selecciona **Configuración de buscapersonas** en el árbol de navegación, se muestra un cuadro de diálogo **Configuración de buscapersonas** con Valores de personalización de mandatos similares a los del cuadro de diálogo que se muestra en la Figura 26.

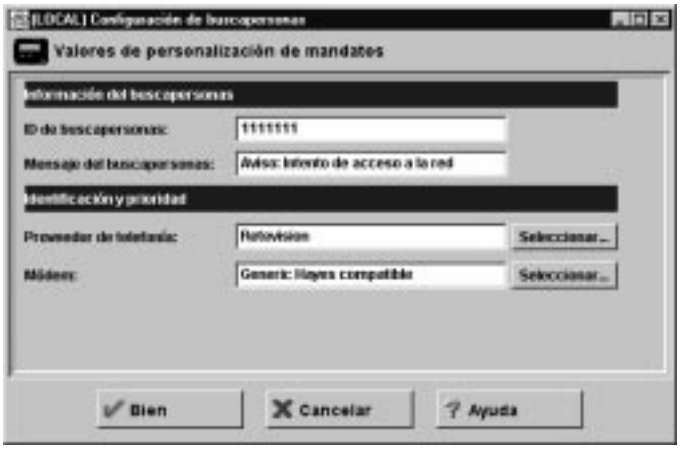

Figura 26. Configuración de buscapersonas

Escriba o seleccione valores en los campos de entrada que han de añadirse.

1. Escriba el ID del buscapersonas. Suele tratarse de un número PIN exclusivo que la empresa de su proveedor de telefonía asigna a su buscapersonas.
2. Escriba el mensaje del buscapersonas. Se trata de una serie de caracteres que contiene el mensaje por omisión que el usuario desea enviar. Para los buscapersonas numéricos, sólo puede ser un número. Para los buscapersonas alfanuméricos, puede ser un mensaje de texto. No exceda la longitud de mensaje máxima que se especifica en la configuración de su proveedor de telefonía o el mensaje podría truncarse. No utilice el carácter dos puntos (:). Si lo hace, se sustituirá por un espacio en blanco.
3. Si no se muestra ningún nombre de proveedor de telefonía, pulse en **Seleccionar** para definir un proveedor de telefonía. Se mostrará el cuadro de diálogo **Administración de proveedores de telefonía**. Consulte “Administración de proveedores de telefonía” en la página 104 para obtener detalles acerca de cómo cumplimentar este panel.
4. Si no se muestra ningún nombre de módem, pulse en **Seleccionar** para definir un módem. Se mostrará el cuadro de diálogo **Administración de modems de buscapersonas**. Consulte “Administración de modems” en la página 106 para obtener detalles acerca de cómo cumplimentar este panel.

5. Pulse en **Bien**.

Cambio de una personalización de mandatos

Cuando selecciona Configuración de buscapersonas en el árbol de navegación, se muestra el cuadro de diálogo **Configuración de buscapersonas** con Valores de personalización de mandatos.

1. Escriba o seleccione valores en los campos de entrada para modificar los valores de los campos de entrada de la personalización actual.
2. Pulse en **Bien**.

Supresión de una personalización de mandatos

1. Puede suprimir una entrada del cuadro de diálogo **Administración de proveedores de telefonía** o del cuadro de diálogo **Administración de modems de buscapersonas** seleccionando un elemento de la lista y efectuando una doble pulsación en **Suprimir**.

   Se le solicitará que confirme la supresión.
2. Pulse en **Sí** para confirmar la supresión o en **No** para volver al cuadro de diálogo **Configuración de buscapersonas**.

Si no existen ninguna entrada de personalización, el soporte de notificación por buscapersonas no podrá enviar ninguna página.

Administración de proveedores de telefonía

Desde el cuadro de diálogo **Configuración de buscapersonas**, diríjase al campo del nombre del proveedor de telefonía y pulse en **Seleccionar**. Se mostrará el cuadro un cuadro de diálogo **Administración de proveedores de telefonía** similar al que se muestra en la Figura 27.

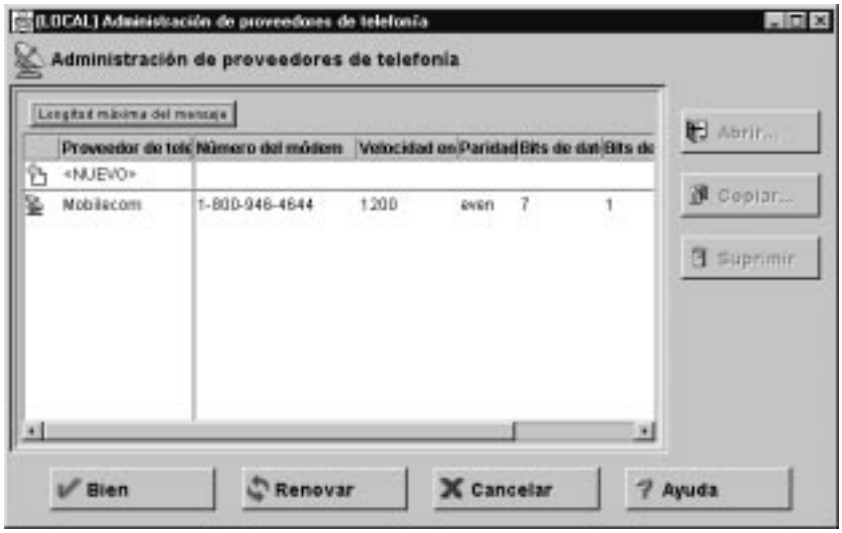

Figura 27. Administración de proveedores de telefonía

Adición de un proveedor de telefonía

Para añadir un nuevo proveedor de telefonía, seleccione **NUEVO** en el cuadro de diálogo **Administración de proveedores de telefonía** y pulse en **Abrir**. Escriba o seleccione valores en los campos de entrada correspondientes:

1. Escriba el nombre del proveedor de telefonía. Puede ser cualquier nombre en tanto que sea exclusivo y proporcione suficiente información para permitirle reconocer de qué proveedor de telefonía se trata.
2. Especifique el número de teléfono del proveedor de telefonía, que es el número de teléfono de un módem de la empresa del proveedor de telefonía y no el número para enviar mensajes al buscapersonas por voz u otro número de servicio. Debe ser el número del módem correcto para cobertura regional o nacional y el correspondiente a un buscapersonas numérico o alfanumérico, según los requisitos del dispositivo para el envío de mensajes al buscapersonas y el servicio que haya contratado.
3. Especifique TAP para el método de envío de mensajes al buscapersonas; es el único valor permitido.
4. Escriba la contraseña si el proveedor de telefonía admite o necesita una.
5. Puede especificar la longitud máxima del mensaje de un buscapersonas alfanumérico y los dígitos máximos de un buscapersonas numérico.
6. Especifique la velocidad en baudios. Pulse en la flecha y elija un valor de la lista.
7. Pulse en **Par**, **Impar** o **Ninguna** en el campo de paridad.
8. Elija los bits de datos por omisión; pulse en **7** o en **8**.
9. Elija los bits de parada por omisión; pulse en **1** o en **2**.
10. Pulse en **Bien**.

Cambio de un proveedor de telefonía

1. Seleccione el proveedor de telefonía que desea cambiar en el cuadro de diálogo **Administración de proveedores de telefonía** y pulse en **Abrir**.
2. Consulte el apartado “Adición de un proveedor de telefonía” para obtener una explicación de los campos que puede cambiar. El nombre del proveedor de telefonía en sí no puede cambiarse. Este campo estará inhabilitado.
3. Efectúe los cambios deseados.
4. Pulse en **Bien**.

Supresión de un proveedor de telefonía

1. Seleccione el proveedor de telefonía que desea suprimir en el cuadro de diálogo **Administración de proveedores de telefonía** y pulse en **Suprimir**.
2. Se le solicitará que confirme la supresión. Pulse en **Sí** para confirmar la acción.

   Nota: La base de datos de proveedores de telefonía siempre debe contener, como mínimo, un proveedor de telefonía. Si no se ha definido ningún proveedor de telefonía, el soporte de notificación por buscapersonas no funcionará correctamente.

Administración de modems

El módem manual contendrá información relevante acerca de cómo inicializar el módem. Puede que sea necesario coordinar los valores del módem con el proveedor de telefonía. En general, sólo reciben soporte los modems compatibles con Hayes que utilizan mandatos de módem estándar.

Desde el cuadro de diálogo **Configuración de buscapersonas**, diríjase al campo del nombre del módem y pulse en **Seleccionar**. Aparecerá un cuadro de diálogo **Administración de proveedores de telefonía** parecido al que se muestra en la Figura 28.

Figura 28. Administración de modems de buscapersonas

Puede añadir, cambiar o suprimir diversos modems utilizando este cuadro de diálogo.

Adición de un módem

Para añadir un nuevo archivo de definición de módem, seleccione **NUEVO** en el cuadro de diálogo **Administración de modems de buscapersonas** y pulse en **Abrir**. En el cuadro de diálogo **Añadir módem**, escriba o seleccione valores en los campos de entrada.

1. Escriba el nombre del módem. Puede ser cualquier nombre en tanto que sea exclusivo respecto a las demás definiciones y proporcione suficiente información para permitirle reconocer de qué módem se trata.
2. Especifique el número de Puerta COM, que define la Puerta COM serie a la que se conecta el módem. Especifique un número inferior a 10. Mientras que el módem debe configurarse para esta puerta a nivel de hardware, no debe definirse para Windows NT; si se hace, con ello se denegará el acceso a la puerta a las funciones del buscapersonas. Si el módem no coincide con los valores del hardware, el código del buscapersonas realizará intentos durante un prolongado espacio de tiempo y, finalmente, no resultarán satisfactorios.
3. Especifique la serie de inicialización, que debe definir el módem como módem de datos con eco en el nivel4 X y una velocidad en baudios fija definida por la ubicación local. No incluya el mandato AT. La función del buscapersonas lo colocará al inicio de la serie de inicialización.

4. Especifique el prefijo de línea externa. Este es el número que marca para obtener conexión con el exterior de la empresa.
5. Pulse en **Bien**.

Cambio de un módem

1. Para cambiar un archivo de definición de módem, seleccione un nombre de módem en el cuadro de diálogo **Administración de modems de buscapersonas** y pulse en **Abrir**.

   En el cuadro de diálogo **Cambiar módem** verá una lista de campos que puede cambiar para la definición del módem. Consulte el apartado “Adición de un módem” en la página 106 para obtener las explicaciones de estos campos.
2. Pulse en **Bien**.

Supresión de un módem

1. Para suprimir un archivo de definición de módem, seleccione un nombre de módem en el cuadro de diálogo **Administración de modems de buscapersonas** y pulse se **Suprimir**.
2. Se le solicitará que confirme la supresión. Pulse en **Sí** para confirmar la acción.

Registro de notificaciones por buscapersonas

El proceso de notificación por buscapersonas utiliza el programa de utilidad de registro del cortafuegos para grabar los registros de salida. Todos los mensajes y errores del buscapersonas se graban en el recurso syslog del cortafuegos general. Para obtener más información acerca de cómo configurar y utilizar los archivos de registro del cortafuegos, consulte Capítulo 15, “Gestión de registros y archivos” en la página 109.

Verificación de la configuración del buscapersonas

Puede verificar la configuración del buscapersonas utilizando el mandato `pager`. Consulte el manual *IBM eNetwork Firewall - Manual de consulta* para obtener detalles. Se recomienda especialmente utilizar el mandato del buscapersonas cada vez que defina o cambie la configuración para garantizar que el sistema, el módem, el proveedor de telefonía y los dispositivos para el envío del mensajes al buscapersonas pueden conversar entre sí correctamente y que los mensajes del buscapersonas pueden enviarse y recibirse realmente.

Ejecutar mandatos

Puede especificar un programa para que se invoque cada vez que se alcance un umbral de alerta. Para especificar un programa:

1. Pulse en **Administración de supervisores de registro** y efectúe una doble pulsación en **NUEVO**.

   Aparecerá el cuadro de diálogo **Añadir supervisor de registro**.
2. En el cuadro desplegable **Tipo de clase**, seleccione **Ejecutar mandato**. Ello habilita el campo **Nombre de archivo del mandato** del panel.
3. En el campo **Nombre de archivo del mandato**, especifique el nombre de la vía de acceso calificada al completo del programa que desea invocar cuando se alcance un umbral de alerta.

El directorio de trabajo para los mandatos ejecutados por el monitor de registros es `\winnt\system32`. Sólo se definen variables de entorno de sistema ya que el shell de mandatos se presenta desde un proceso de sistema. No se definen variable de entorno de usuario. En general el programa presentado debería utilizar nombres de archivo permitidos en lugar de confiar en variables de vía de acceso.

El cortafuegos pasará el mensaje de la Alerta completo como primer parámetro del programa, como se indica a continuación:

```
Alertas de anomalías de autentificación totales: ICA0001e
Alertas por anomalías de autentificación de usuario: ICA0002e
Alertas por anomalías de autentificación del sistema principal: ICA0003e
Alertas de umbral de mensaje: ICA0004e
```

Consulte el manual *IBM eNetwork Firewall - Manual de consulta* para obtener una descripción completa de estos mensajes.

Capítulo 15. Gestión de registros y archivos

En este capítulo se describe cómo utilizar los recursos de registro mediante el cliente de configuración. Cuando los usuarios intentan acceder a los sistemas principales a través de los diversos servidores del IBM Firewall, el IBM Firewall graba las entradas en el archivo de registro que mantiene el `servicio de registro del IBM Firewall`.

El IBM Firewall puede generar grandes volúmenes de información de registro, dependiendo de la configuración del cortafuegos. Las entradas del registro pueden proceder de gran diversidad de puntos, como los socks y los filtros especiales. Además, los archivos de registro pueden grabarse con gran diversidad de niveles de gravedad; por ejemplo, *depuración, información*, o *error*. En este capítulo también se explica cómo utilizar los recursos de gestión de registros y de gestión de archivos de registro para gestionar el tamaño de los archivos y registros.

Creación y archivo del archivo de registro utilizando el cliente de configuración

El cliente de configuración puede utilizarse para la gestión de registros y la gestión de archivos de registro. Se da por supuesto que el espacio de disco disponible es suficiente para contener toda la información de registro. El cortafuegos genera información de depuración y de errores rutinaria en el recurso de `registro del cortafuegos`. Sólo el administrador principal del cortafuegos dispone de acceso al recurso de `registro del cortafuegos`. Los mensajes de alerta se dirigen al recurso de registro de alertas . La información administrativa del registro de comprobación se dirige al recurso de registro de comprobación .

Para que el funcionamiento de los programas de utilidad de informes sea correcto, es importante que sólo los mensajes del registro del cortafuegos aparezcan en sus archivos de entrada. Ningún otro recurso debería dirigirse al mismo archivo que el `registro del cortafuegos`, por lo que el registro del cortafuego debe definirse de acuerdo con ello.

Si desea ver las alertas en el panel principal del cliente de configuración, deberá dirigir las alertas a un archivo designado como recurso de `registro de alertas`. Ese archivo no debe designarse para nada más.

Los niveles de prioridad siguientes son cumulativos, donde la *depuración* captura la mayor parte de la información. *Crítico* sólo captura los sucesos más graves del cortafuegos.

- Depuración
- Información
- Advertencia
- Error
- Crítico

Se recomienda empezar por el nivel *información* hasta que los procedimientos del cortafuegos sean estables. Entonces, podrá cambiar a *advertencia* o *error* para reducir la actividad del registro y el tamaño del registro del sistema.

Los niveles de prioridad no se corresponden exactamente con el sufijo del código de mensaje *(i,e,w,s..)*. Quizás deba hacer pruebas para determinar cómo *desactivar* algunos mensajes.

Adición de recursos de registro

En el árbol de navegación del cliente de configuración, efectúe una doble pulsación en el icono de la carpeta de archivos Administración del sistema para ampliar la vista. Efectúe una doble pulsación en el icono de la carpeta de archivos Registros del sistema para ampliar la vista. Seleccione Recursos de registro. El cuadro de diálogo **Recursos de registro** muestra el conjunto de recursos de registro actualmente habilitados.

1. Seleccione **NUEVO** en el cuadro de diálogo **Recursos de registro** y pulse en **Abrir** para añadir una entrada syslog a los recursos actualmente habilitados.

   Aparecerá el cuadro de diálogo **Añadir recursos de registro**, como se muestra en la Figura 29.

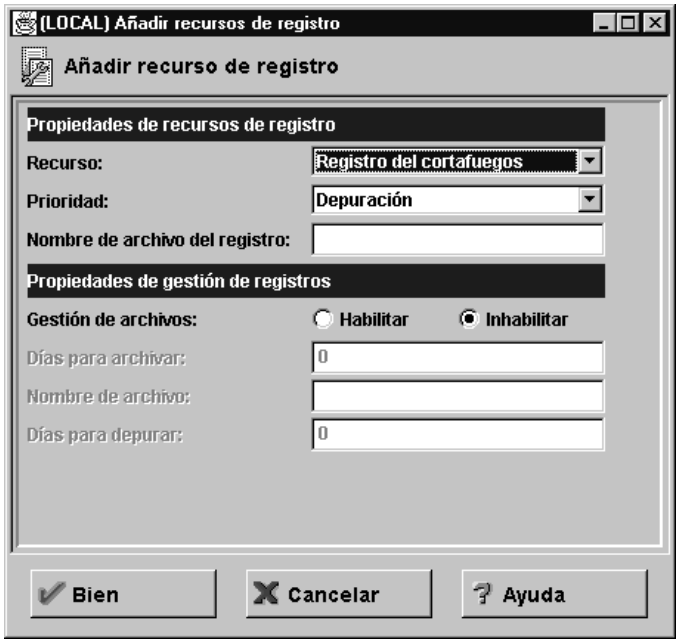

Figura 29. Añadir recursos de registro

2. Pulse en la flecha **Tipo** para seleccionar el tipo. El tipo es el Nombre de archivo.
3. El recurso de registro determina el tipo y la fuente de la información que se registra. Pulse en la flecha **Recurso** para seleccionar uno de los recursos de registro siguientes:
   - Registro del cortafuegos - registros generales del cortafuegos, incluido el registro de filtros
   - Registro de alertas - estado del daemon del supervisor de registro y advertencias de violación de umbral que se utilizan para poblar la Visualización de alertas
   - Registro de correo

4. Pulse en la flecha **Prioridad** para elegir la prioridad. Las prioridades del registro se listan de menor a mayor gravedad. La prioridad que seleccione será el nivel mínimo que habrá de registrarse.
5. Especifique el nombre del archivo de registro. El nombre de archivo del registro debe tener una vía de acceso absoluta (deberá empezar con una unidad y una barra inclinada invertida \) y la vía de acceso al archivo debe existir.
6. La gestión de archivos sólo puede utilizarse con un recurso de registro de tipo *nombre de archivo*. Cuando se habilita, el tamaño del archivo de registro puede reducirse periódicamente. La habilitación de la gestión de archivos significa que debe establecer los parámetros de los que depende en mandato `fwlogmgmt`. Consulte “Archivo de registros” en la página 112. Puede habilitar o inhabilitar los parámetros de gestión de archivos.
7. Seleccione el número de días completos durante los cuales deberá archivarse la actividad del registro o registros en un registro de anotaciones activo. El valor debe ser cero o superior. El archivo se producirá cuando un mandato `fwlogmgmt -l` detecte registros de anotaciones activos que cumplan con estos criterios. Cuando se calcula el número de días que ha de conservarse un registro de anotaciones, la gestión de registros no incluye el presente día.
8. Especifique un nombre de archivo y una vía de acceso completa. El IBM Firewall proporciona una función de archivo por omisión, que utiliza un directorio. Sin embargo, puede utilizar funciones de archivo de conexión si lo desea.
9. Seleccione el número de días completos transcurridos los cuales un archivo de registro archivado deberá suprimirse del archivo. El valor debe ser cero o superior. La depuración se producirá cuando un mandato `fwlogmgmt -a` detecte un archivo o archivo archivados se cumpla con estos criterios. Cuando se calcula el número de días que ha de conservarse un archivo archivado, la gestión de registros no incluye el presente día.
10. Pulse en **Bien**.

Cambio de los recursos de registro

1. Seleccione la entrada del registro del cortafuegos que desea cambiar en el cuadro de diálogo **Recursos de registro** y pulse en **Abrir**.

   Aparecerá el cuadro de diálogo **Cambiar recursos de registro**.
2. Cambie los campos deseados. Consulte el apartado “Adición de recursos de registro” en la página 110 para obtener una explicación de los campos.
3. Pulse en **Bien**.

Supresión de recursos de registro

1. Seleccione una entrada del registro del cortafuegos entre las actualmente habilitadas en el cuadro de diálogo **Recursos de registro** y pulse en **Suprimir**.

   Aparecerá el panel **Suprimir advertencia**.
2. Pulse en **Bien** si desea continuar con la supresión. Pulse en **Cancelar** si ha cambiado de idea. Con ello no se suprime el archivo de registro real.

Archivo de registros

El proceso de archivo:

- Elimina los registros que han de eliminarse de un registro activo
- Los coloca en un archivo por separado
- Comprime el archivo resultante
- Coloca el nuevo archivo en un directorio de archivo

Para iniciar un programa de gestión de registros para archivar registros acumulados, tiene dos opciones:

1. Ejecutar el mandato `fwlogmgmt -l` desde la línea de mandatos periódicamente o
2. Definir el mandato `fwlogmgmt -l` como un Servicio planificado NT.

La depuración de los archivos del registro consiste en suprimir los archivos archivados que han de eliminarse del directorio de archivo.

Para depurar los archivos archivados, tiene dos opciones:

1. Ejecutar `fwlogmgmt -a` desde la línea de mandatos periódicamente o
2. Definir el mandato `fwlogmgmt -a` como un Servicio planificado NT.

Los registros y archivos que han de eliminarse se determinan mediante los valores especificados en las definiciones de los recursos de registro, como se describe en “Adición de recursos de registro” en la página 110.

La forma más eficaz o adecuada de ejecutar el proceso de gestión de registros es definirlo como Servicio planificado NT. Inícielo utilizando el objeto Servicios del panel de control.

Por ejemplo, si desea definir el proceso de archivo de la gestión de registros para que se ejecute todos los días a las 03:00 horas, escriba

```
at 3:00 /every:M,T,W,Th,F,S,Su fwlogmgmt -l
```

DLL de conexión

Consulte el *Manual de consulta del IBM eNetwork Firewall* para obtener información acertca de la DLL de conexión de archivador de registrso que puede utilizar para sustituir la DDL por omisión del cortafuegos.

Salidas de la gestión de registros

El recurso de gestión de registros realiza algunas comprobaciones de integridad preliminares antes de proceder con otra actividad de la gestión de registros. Si se detecta algún problema, se envían diagnósticos al recurso de registro del cortafuegos cuando ejecuta el mandato `fwlogmgmt` desde la línea de mandatos.

Los recursos de registro Mail o admin audit (local0) lestán sujetos a diferentes normas de archivado que otros recursos. Todos los recursos de archivo necesitan que el archivo esté habilitado para ser archivados. Sin embargo, registros del cortafuegos (local4) y de alerta (local1) sólo se archivan si sus fechas exceden los

criterios especificados en la definición de recursos en el momento en que se ejecuta el proceso de archivo; mientras que *todo* el archivo de registro de correo o auditoría se archivará cada vez. Igualmente,la información en el registro de correo se considera para finalidades de depuración y generalmente es de poca utilidad archivarla. El resto de información de correo, genealmente más útil, se almacena en el registro (local4) del cortafuegos.

Programas de utilidad de informes

Puede utilizar las funciones del programa de utilidad de informes como ayuda para generar informes a partir de los archivos de registro actuales o registrados. Los programas de utilidad de informes generan los archivos tabulados de la información administrativa que se organizan y formatean para que se correlacionen fácilmente con las tablas de bases de datos relacionales. Estas tablas ayudan al administrador del cortafuegos a analizar:

- La utilización general del cortafuegos
- Los errores del proceso del cortafuegos
- Los intentos de acceso no autorizado a la red protegida.

Mediante la utilización de los programas de utilidad y el registro del cortafuegos, el administrador puede crear un archivo de texto normal de los mensajes. Además, los archivos tabulados pueden generarse e importarse a las tablas de un sistema de bases de datos relacionales, como la familia de productos DB2. El administrador puede entonces utilizar el Lenguaje de Consulta Estructurada (SQL) para consultar los datos y generar informes.

Los Programas de utilidad de informes se instalan como parte de la instalación del cortafuegos. También pueden instalarse por separado y ejecutarse en un sistema principal que no sea cortafuegos. El cliente de configuración puede utilizarse para ejecutarlos en un cortafuegos. En una máquina que no sea de cortafuegos, utilice la línea de mandatos.

Para que el funcionamiento de los programas de utilidad de informes sea correcto, es importante que sólo los mensajes del `registro del cortafuegos` aparezcan en sus archivos de entrada. Ningún otro recurso debería dirigirse al mismo archivo que el `registro del cortafuegos`,

por ello, debe definir el registro del cortafuegos de acuerdo con ello.

No intente utilizar programas de utilidad de informes en ningún archivo de registro anterior al IBM Firewall para AIX V3R1. Sin embargo puede utilizar los programas de utilidad de informes para procesar archivos de registro de IBM Firewall para AIX V3R1 o posterior. También puede usarlos para procesar el registro su de AIX. Consulte el manual *IBM eNetwork Firewall - Manual de consulta* para obtener información más detallada acerca de los programas de utilidad de informes.

Ejecución de programas de utilidad de informes utilizando el cliente de configuración

En el árbol de navegación del cliente de configuración, efectúe una doble pulsación en el icono de la carpeta de archivos Administración del sistema para ampliar la vista. Efectúe una doble pulsación en el icono de la carpeta de archivos Registros del sistema para ampliar la vista. Seleccione **Programas de utilidad de informes**.

Aparecerá el cuadro de diálogo **Programas de utilidad de informes**, como se muestra en la Figura 30 en la página 114.

Figura 30. Programas de utilidad de informes

1. Para el archivo por omisión que proporciona el IBM Firewall, el nombre de la vía de acceso del archivo de registro es el directorio que contiene archivos de registro comprimidos. En el campo del nombre de archivo del archivo de registro, especifique el directorio que ha especificado en el campo de directorio de archivo del cuadro de diálogo **Recursos de registro**. Especifique el nombre de la vía de acceso absoluta del directorio de archivos. Si desea ver un archivo de registro que no se ha archivado, deje este campo en blanco.
2. Seleccione el **Tipo de informe**. Para ver el texto del mensaje de registro ampliado, seleccione **Registro de texto**. Para crear archivos tabulados para la utilización de DB2, seleccione **Registro de tablas**. Si importa los archivos resultantes a DB2, puede ejecutar consultas SQL en los datos del registro. Consulte el manual *IBM eNetwork Firewall - Manual de consulta* para obtener más información.
3. El nombre de archivo del registro es uno de los archivos de registro archivados comprimidos u otro `registro del cortafuegos` válido o el nombre de un archivo de registro su de AIX. Si ha realizado una entrada en el campo del directorio de archivo del archivo de registro, puede pulsar en la flecha **Nombre del archivo de registro** para elegir el registro con el que trabajar. Si no ha especificado ningún archivo de registro en el paso 1, el nombre del archivo de registro que especifique aquí debe ser el nombre de un archivo de registro del cortafuegos no comprimido válido o un archivo de registro su de AIX. Deberá especificar una vía de acceso completa.
4. Seleccione el **tipo de registro**, que será **cortafuegos** o **su de AIX**.
5. Especifique la **Vía de acceso y nombre del archivo para el texto de salida**.
6. Seleccione **Sí** para añadir los resultados de una petición de registro de tablas a los archivos tabulados existentes o **No** para sustituir los archivos existentes.
7. Este campo le permite seleccionar determinados tipos de mensajes para colocarlos en el archivo de texto de salida. El contenido de este campo se trata como los parámetros que se colocan en un mandato `Buscar` de Windows NT

estándar. Por ejemplo, si escribe "ICA0" en el campo (deben incluirse las comillas), es como si ejecutara el mandato siguiente:

```
fwlogtxt < my.log | find "ICA0"
```

A continuación se muestran algunas entradas de ejemplo que puede colocar en este campo y sus resultados:

```
FILTRO                          RESULTADO
"ICA0"          Lista mensajes de alerta de umbral del supervisor de
                registros
"ICA3"          Lista mensajes relacionados con el Socks
                (n  ICA3000 - 3999)
"ICA2010"       Sólo lista las apariciones del mensaje ICA2010
/V "ICA3"       Lista todos los mensajes excepto los mensajes del Socks
/C "ICA001"     Cuenta el número de mensajes ICA0001
```

8. Cuando se pulsa en **Bien**, el archivo o archivos solicitados se colocan en el directorio de salida especificado.
9. El área Resultados de los programas de utilidad de informes muestra los mensajes de error del programa de utilidad de informes que se ha ejecutado. Para ver el texto de registro que resulta de un tipo de informe Registro de texto, pulse en **Visor de registros** en el panel principal del cliente de configuración del cortafuegos y especifique el nombre del archivo de salida calificado al completo. Los archivos .tbl que resultan de un tipo de informe de Registro de tablas pueden cargarse en una base de datos, tal como se describe en el *Manual de consulta del IBM eNetwork Firewall.*

Capítulo 16. Conversión de direcciones de red

Con el crecimiento explosivo de Internet, el agotamiento de direcciones de IP se ha convertido en un problema de primer orden. La conversión de direcciones de red (NAT) proporciona una solución al problema del agotamiento de direcciones de IP gracias a la reutilización de direcciones.

Las direcciones en una red privada se pueden asignar a partir de un espacio de dirección enorme (normalmente un espacio de dirección de clase A 10.0.0.0). Estas direcciones son privadas y no están expuestas a Internet. Por tanto, estas direcciones se pueden volver a utilizar por otra red de IP. Se utiliza una sola dirección registrada de IP para esconder varias direcciones de red privadas. La NAT convierte las direcciones y números de puesta sin registrar en direcciones de Internet y números de puerta registrados que son válidos. En la dirección de entrada, la NAT convierte de nuevo la dirección de Internet y los números de puerta registrados en direcciones y números de puerta sin registrar. La ventaja de la NAT es que permite a la red que utiliza direcciones privadas o ilegales comunicarse de forma transparente con sistemas principales en Internet, logrando de hecho que la red privada tenga un mayor espacio de dirección. Además, al utilizar la NAT, las direcciones en la red privada quedan ocultas del resto del mundo, con lo que se proporciona un nivel de seguridad adicional.

Figura 31 muestra una operación básica de NAT en un entorno de IBM Firewall.

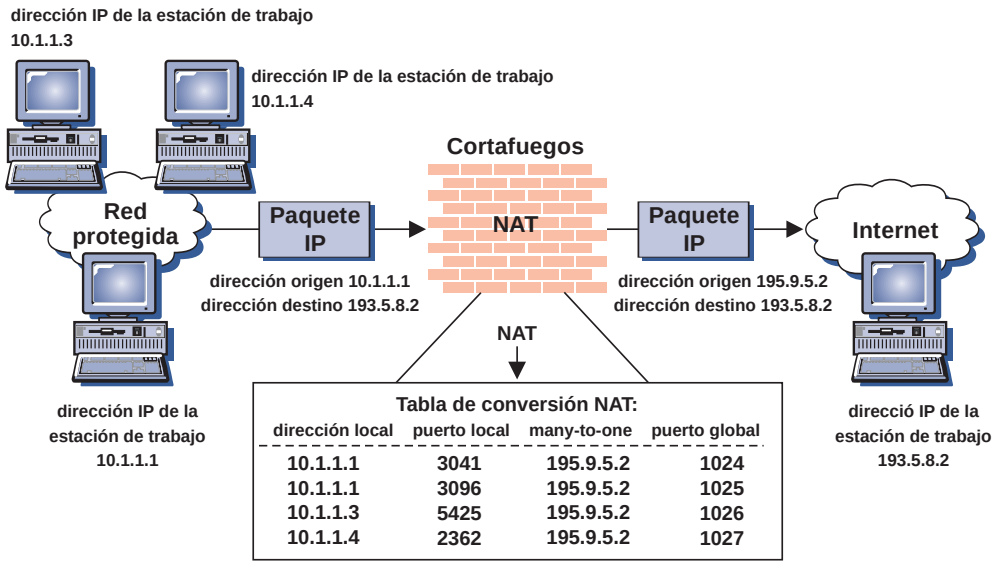

Figura 31. Conversión de direcciones de red

Los paquetes TCP/UDP generados por sistemas principales protegidos tienen sustituida su dirección de origen sustituida con una dirección de Internet registrada. La puerta del sistema principal protegido se convertirá en un número de puerta exclusivo. Todos los paquetes de salida tendrán la misma dirección de origen pero un número de puerta exclusivo. Esta forma de conversión, a la que se conoce como conversión Many-to-one, permite que varios sistemas principales protegidos se escondan detrás de una única dirección. Las sumas de comprobación del paquete en el encabezamiento IP y el pseudo encabezamiento TCP/UDP se actualizan. El número máximo de conexiones concurrentes está limitado a 64536, (en realidad

64512) ya que las puertas 0–1023 están reservadas. Se proporciona soporte a las conexiones de entrada con tablas de conversión con entradas estáticas (antes que dinámicas). Por ejemplo, el sistema principal 193.5.8.2 puede iniciar una conexión TCP con el sistema principal 10.1.1.1 (utilizando la dirección global 195.9.5.2) sólo si existe una entrada estática en la tabla de conversión NAT que correlaciona 195.9.5.2 en 10.1.1.1.

Todos los paquetes generados por las aplicaciones TCP/UDP se pueden convertir. Las dificultades aparecen si los datos de aplicación contenidos en el paquete IP contienen una dirección IP. Una aplicación particularmente problemática para la conversión de direcciones es el FTP. La conexión de control FTP emite mandatos "PORT" o respuestas "PASV" que contienen en el mensaje una dirección IP codificada en ASCII. En este caso, la NAT debe modificar no sólo las direcciones en el encabezamiento IP sino también la dirección ASCII y el número de puesta en la carga útil.

Con el release de un próximo APAR, las opciones de conversión MAP y Many-to-one permitirán que se conviertan los paquetes ICMP de entrada y salida. Los paquetes de respuesta ICMP de entrada (PING, indicación de la hora, máscara de dirección) y todos los paquetes de error (destino inalcanzable, apagar el origen, redireccionamientos, tiempo excedido y mensajes de paquete erróneo) se convertirán sólo si existe una entrada previa de tabla de conversión, con la excepción de los de redireccionamientos. Los redireccionamientos ICMP pasarán por la NAT sin convertirse. Dependerá de las reglas del filtro permitir o denegar redireccionamientos ICPM.

Se proporciona soporte a los paquetes ICPM de consulta/respuesta de salida (pregunta/respuesta PING, pregunta/respuesta de indicación de la hora, pregunta/respuesta de máscara de dirección) al convertir la dirección protegida del paquete y el identificador de consulta ICPM, de tal manera los paquetes ICPM de distintos sistemas principales protegidos puedan compartir una única dirección registrada.

Los administradores deberían de vigilar el flujo de algunos paquetes ICPM entre redes protegidas y no protegidas, sobre todo los de respuesta de máscara de dirección y los redireccionamientos. Para más información sobre los asistentes de seguridad para permitir el tráfico ICPM en el cortafuegos, consulte el siguiente manual en CD, que aparece en bibliografía, de título: *Guarding the Gates Using the IBM eNetwork Firewall for NT 3.2*.

Implantación de IBM eNetwork Firewall NAT

La implantación de IBM Firewall NAT proporciona soporte a la conversión básica de direcciones como se ha descrito anteriormente con las siguientes advertencias:

- Las aplicaciones TCP/UDP (excepto las de FTP como se describe a continuación) que contienen información de direcciones IP en la carga útil sólo tendrán convertidos los campos de encabezamiento del paquete como se ha descrito antes. Esto implica que aplicaciones UDP, como por ejemplo DNS o SNMP, no tendrán convertida información de direcciones contenida en la carga útil.
- Los mandatos FTP PORT se convierten por completo. Sin embargo, la dirección incorporada en un paquete de respuesta PASV no se convierte.

- Los mensajes de cifrado y pregunta/respuesta ICMP se convierten. Esto permite que, por ejemplo, los PING de salida operen correctamente así como el descubrimiento MTU de vías TCP.
- La NAT no detecta una desconexión del TCP, sino que confía en una espera desocupada configurable antes de eliminar una entrada dinámica de la tabla de conversión e insertar de nuevo la dirección IP registrada en la agrupación de direcciones disponibles.

Interacción de ejemplo entre NAT, filtros y túneles.

Figura 32 muestra una interacción de ejemplo entre NAT, filtros y túneles.

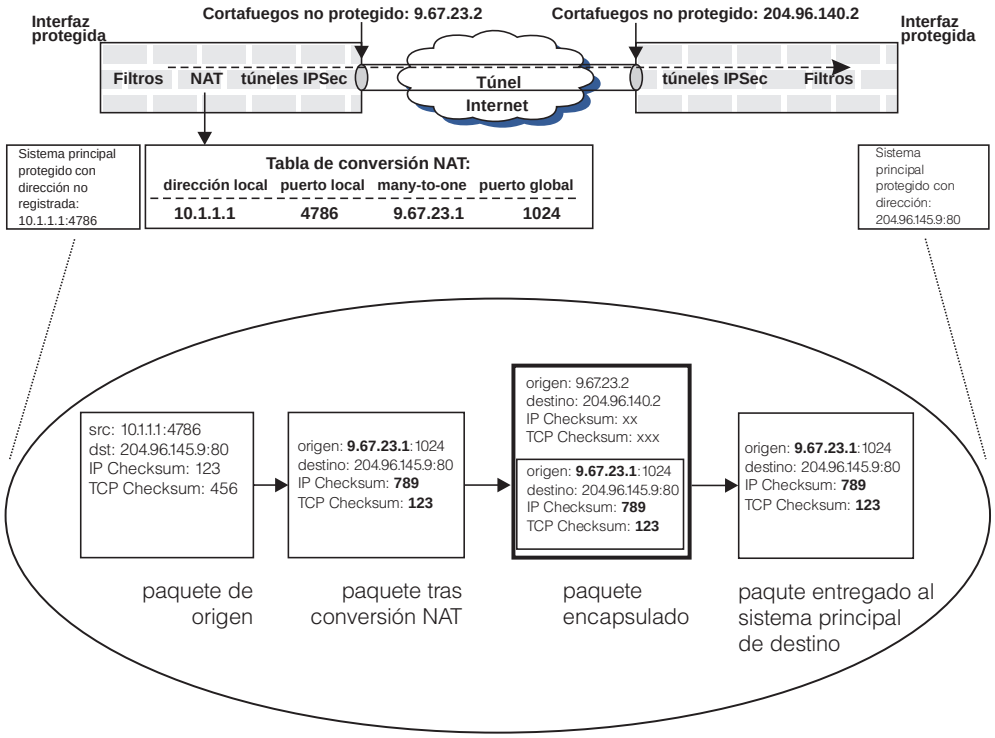

Figura 32. Interacción de ejemplo entre NAT, filtros y túneles

Partimos de que un túnel IPSec ESP se establece de forma manual entre los cortafuegos 9.67.23.2 y 204.96.140.2. La NAT se activa sólo en el cortafuegos 9.67.23.2 porque esta red protegida utiliza direcciones privadas. La red protegida en el otro lado del túnel no utiliza NAT. Además de mostrar la conversión básica NAT (los campos en negrita en el segundo paquete de la izquierda muestran los campos en el paquete que se modifican durante la conversión de direcciones de salida), Figura 32 también muestra que el paquete convertido del sistema principal está encapsulado en un paquete IP que *no* se convierte.

En general, el filtro se aplica a paquetes de salida antes que la conversión NAT y a los de entrada después. De esta manera las reglas del filtro están basadas en direcciones sin convertir. Cuando están implicados NAT y túneles, las reglas del filtro en el cortafuegos que tiene activada la NAT se basan también en direcciones sin convertir. Al otro lado del túnel (partiendo de que la NAT no está activada en este cortaguegos), las reglas del filtro para los paquetes de entrada se basan en direcciones de origen y destino convertidas (para los casos de entrada y de salida

respectivamente). Si la NAT está activada a ambos lados del túnel, lo especificado anteriormente se aplica a las dos direcciones.

Si se usa el escenario ilustrado en Figura 32 en la página 119 como ejemplo, y se parte de que el objetivo es permitir que el sistema principal protegido 10.1.1.1 se comunique con el sistema principal protegido 204.96.145.9 en un túnel, el cortafuegos conectado al 10.1.1.1 debe tener una regla del filtro que permita 10.1.1.1 comunicarse con 204.96.145.9 en un túnel. En el otro cortafuegos conectado con el sistema principal de destino, se necesita una regla del filtro que permita la comunicación entre 9.67.23.1 y 204.96.145.9 a través del túnel.

Más sobre NAT

Utilice la NAT si desea permitir:

- El acceso directo de una máquina detrás de un cortafuegos a un sitio no protegido mientras se protege la dirección en esa máquina protegida.
- Que varias máquinas sin direcciones registradas compartan una dirección registrada de manera que puedan llegar a páginas de Internet.
- Que otras máquinas de ubicaciones no protegidas accedan a un servidor detrás de un cortafuegos.

Obtenga las direcciones registradas para NAT de su proveedor de servicios Internert. Todas las direcciones que se utilicen para NAT no se pueden utilizar para otros propósitos.

Hay cuatro posibilidades de NAT:

Many-to-one Implica convertir una dirección protegida y número de puerto de un paquete de manera que varias (hasta 65536) direcciones internas puedan compartir una dirección IP registrada. Esta dirección IP registrada compartida esconderá direcciones locales, pero además, necesitará otra dirección de Internet registrada para la dirección no protegida del cortafuegos. La configuración de la NAT identificará la dirección de Internet registrada que se utiliza para la conversión de puertas a partir de una entrada Many-to-one.

Convertir Se utiliza para crear una lista de direcciones protegidas que se convertirán.

Excluir Se utiliza para crear una lista de direcciones protegidas que no se convertirán.

Correlación Se utiliza para reservar una dirección registrada específica para una dirección protegida específica.

Configuración de la Conversión de direcciones de red mediante el cliente de configuración

1. En el árbol de navegación del cliente de configuración, efectúe una doble pulsación en el icono de la carpeta de archivos Conversión de direcciones para ampliar la vista. Efectúe una doble pulsación en el icono de la carpeta de archivos NAT para ampliar la vista.

2. Seleccione **Configuración NAT** para configurar el módulo de Conversión de direcciones de red.

   Aparece la **lista de conversión de direcciones de red**

3. Las entradas de conversión de direcciones de red contenidas en el archivo de configuración NAT se muestran en este recuadro de diálogo. También puede añadir, cambiar o suprimir entradas NAT.

Añadir entrada NAT

1. Seleccione**Nuevas** en la **Lista de conversión de direcciones de red** y pulse **Abrir** para añadir nuevas entradas al archivo de configuración NAT.

   Aparecerá el cuadro de diálogo **Añadir NAT**.

2. En el cuadro de diálogo **Añadir NAT**, pulse la flecha en el tipo de campo NAT y seleccione una de los siguientes:

   - Direcciones de red registradas Many-to-one: Añade las direcciones IP especificadas a las direcciones IP reservadas. Los parámetros son direcciones IP reservadas y el tiempo de espera asociado con la tabla de conversión.
   - Convertir direcciones de red protegidas: especifica una gama de direcciones IP protegidas que requieren conversión de direcciones de red.
   - Excluir direcciones de red protegidas: especifica una gama de direcciones IP protegidas que deberían excluirse de cualquier conversión de direcciones de red.
   - Correlación de direcciones de red protegidas: Define una conversión estática de direcciones IP de correspondencia exacta de protegida a registrada.

Dirección de red registrada Many-to-one

Una entrada de dirección registrada Many-to-one convierte una dirección protegida y número de puerto de un paquete de manera que varias (hasta 65536) direcciones internas puedan compartir una dirección IP registrada. Así podrá esconder varias direcciones locales con la única dirección IP registrada. (Necesitará una dirección de Internet registrada adicional para la dirección no protegida del cortafuegos).

Cuando un sistema principal protegido envía paquetes a una red no protegida, se asigna una dirección IP registrada. Esta dirección IP registrada exclusiva se utiliza para transportar una trama IP entre el IBM Firewall y las máquinas fuera de la red protegida.

Si ha seleccionado en la pantalla Añadir NAT la opción Many-to-one, escriba los siguientes valores:

Dirección IP registrada Se obtiene de su proveedor de servicios de Internet. Será una dirección IP decimal punteada tras la cual se esconderán todas las direcciones protegidas.

Seleccione un objeto de red pulsando **Seleccionar** para que aparezca el cuadro de diálogo**Seleccione el objeto de red**. Seleccione un objeto de red y pulse **Aceptar**. El objeto de red se añade al campo de

objetos de red en el cuadro de diálogo **Añadir configuración NAT**. También puede escribir directamente un valor en el campo si antes no se ha creado un objeto de red.

Valor de tiempo de espera

Escriba el número de minutos que la conversión de una dirección puede permanecer desocupada antes de que la NAT libere las direcciones IP registradas. Este valor de espera sólo se aplica a la conversión de direcciones que utilizan una dirección IP registrada en el intervalo de direcciones IP que especifica esta entrada.

El tiempo por omisión es de 15 minutos. El intervalo de valores va de 5 a 45.

Convertir dirección de red protegida

Una entrada para convertir direcciones IP protegidas define un grupo de direcciones de red protegidas que necesitan la NAT para efectuar la conversión de direcciones IP. Por omisión, NAT ejecuta conversión de direcciones en todas las direcciones IP protegidas en el conjunto para convertir direcciones IP protegidas.

Si ha seleccionado Convertir en la pantalla Añadir NAT, escriba los siguientes valores:

Dirección IP protegida Especifica una dirección IP decimal punteada que identifica el intervalo de direcciones Ip protegidas que necesitan conversión de direcciones de red.

Seleccione un objeto de red pulsando **Seleccionar** para que aparezca el cuadro de diálogo**Seleccione el objeto de red**. Seleccione un objeto de red y pulse **Aceptar**. El objeto de red se añade al campo de objetos de red en el cuadro de diálogo **Añadir configuración NAT**. También puede escribir directamente un valor en el campo si antes no se ha creado un objeto de red.

Máscara de dirección IP protegida

Especifica una máscara, como una máscara de subred que especifica los bits en la dirección IP protegida que se utiliza para identificar un intervalo de direcciones IP. Los bits en estas máscaras que se definen como 0 indican que las posiciones de bit que tienen 0 o 1 están incluidas en el intervalo de direcciones IP. De esta manera, al especificar 255.255.255.255 en la máscara, se indica que sólo una dirección IP protegida está incluida en esta entrada de conversión, mientras que una máscara de 255.255.255.0 indica que las direcciones IP de clase C requieren conversión de la dirección.

Excluir direcciones de red protegidas

Una entrada para excluir direcciones IP protegidas define un grupo de direcciones de red protegidas que no necesitan NAT para ejecutar la conversión de direcciones IP. Por omisión, NAT ejecuta conversión de direcciones en todas las direcciones IP protegidas en el conjunto para convertir direcciones IP protegidas.

Si ha seleccionado Excluir en la pantalla de diálogo **Añadir NAT** escriba los siguientes valores:

Dirección IP protegida Especifica una dirección IP decimal punteada que identifica el intervalo de direcciones IP protegidas que deberían excluirse de cualquier conversión de direcciones de red.

Seleccione un objeto de red pulsando **Seleccionar** para que aparezca el cuadro de diálogo**Seleccione el objeto de red**. Seleccione un objeto de red y pulse **Aceptar**. El objeto de red se añade al campo de objetos de red en el cuadro de diálogo **Añadir configuración NAT**. También puede escribir directamente un valor en el campo si antes no se ha creado un objeto de red.

Máscara de dirección IP protegida
Especifica una máscara, como una máscara de subred que especifica los bits en la dirección IP protegida que se utiliza para identificar un intervalo de direcciones IP. Los bits en estas máscaras que se definen como 0 indican que las posiciones de bit que tienen 0 o 1 están incluidas en el intervalo de direcciones IP. De esta manera, al especificar 255.255.255.255 en la máscara, se indica que sólo una dirección IP protegida se especifica en esta entrada, mientras que una máscara de 255.255.255.0 indica que las direcciones IP de clase C quedan excluidas de la conversión de la dirección.

Correlación de direcciones de red protegidas

Una entrada de correlación de direcciones IP protegidas define una correlación de correspondencia exacta de una dirección IP protegida a una dirección IP registrada. Esta correlación de direcciones Ip de correspondencia exacta permite a los clientes de aplicaciones externas, como por ejemplo los clientes FTP o telnet, establecer sesiones TCP con máquinas servidores que residen en la red protegida. Las direcciones IP registradas en las entradas de correlación de direcciones IP protegidas pueden solapar el espacio de direcciones IP especificado por las entradas reservadas de direcciones IP registradas.

Si ha seleccionado Correlación en el cuadro de diálogo **Añadir configuración NAT**, escriba los siguientes valores:

Dirección IP protegida Una dirección IP decimal punteada que debería convertirse en una dirección IP registrada especificada.

Seleccione un objeto de red pulsando **Seleccionar** para que aparezca el cuadro de diálogo**Seleccione el objeto de red**. Seleccione un objeto de red y pulse **Aceptar**. El objeto de red se añade al campo de

objetos de red en el cuadro de diálogo **Añadir configuración NAT**. También puede escribir directamente un valor en el campo si antes no se ha creado un objeto de red.

Campo de dirección IP registrada

Una dirección IP decimal punteada en la que se debería convertir una dirección IP protegida especificada.

Seleccione un objeto de red pulsando **Seleccionar** para que aparezca el cuadro de diálogo**Seleccione el objeto de red**. Seleccione un objeto de red y pulse **Aceptar**. El objeto de red se añade al campo de objetos de red en el cuadro de diálogo **Añadir configuración NAT**.

Cambiar la entrada NAT

Seleccione una entrada NAT existente del cuadro de diálogo **Configuración NAT** y pulse **Abrir** para cambiar las entradas de conversión de red en el archivo de configuración NAT.

Borrar una entrada NAT

1. Seleccione una entrada NAT existente del cuadro de diálogo**Configuración NAT** y pulse **Borrar** para eliminar la entrada de conversión de red en el archivo de configuración NAT.

   Aparecerá un cuadro de diálogo de confirmación

2. Elija sí o no.

Activación NAT

1. En el árbol de navegación del cliente de configuración, efectúe una doble pulsación en el icono de la carpeta de archivos Conversión de direcciones para ampliar la vista. Efectúe una doble pulsación en el icono de la carpeta de archivos NAT para ampliar la vista.
2. Seleccione **Activación NAT** y aparecerá el cuadro de diálogo
3. Puede seleccionar cualquiera de los siguientes y pulsar **Ejecutar**:
   - Validar entradas de conversión de direcciones de red contenidas en un archivo de configuración NAT.
   - Activar/Actualizar la configuración para mostrar las entradas de conversión de direcciones re de que se están utilizando en el módulo NAT.
   - Desactivar NAT para inhabilitar la conversión de direcciones de red.
   - Habilitar el registro cronológico para habilitar el registro de conversiones de direcciones de red.
   - Inhabilitar el registro cronológico para inhabilitar el registro de conversiones de direcciones de red.

Registro cronológico

La NAT anotará varias condiciones de error siempre que los registros de NAT y de filtro estén habilitados. El registro de NAT se habilita mediante el panel**Activación NAT** o usando del mandato **fwnat**. El registro de filtro se habilita mediante el panel **Servicio de registros** o usando el mandato **fwlog**.

Las siguientes actividades se registrarán en el servicio de registro del cortafuegos:

- Actualizaciones de las tablas NAT del administrador (por ejemplo, entradas estáticas o MAP)
- Actualizaciones dinámicas de la tabla de conversiones NAT
- Mensajes de error
- Intentos sin éxito de conversión que hacen que se descarte el paquete
- Cada vez que se activa o desactiva la conversión NAT

Creación de reglas de filtro para NAT

Una vez que se ha realizado la configuración NAT, se debe configurar las reglas de filtro para las conexiones que van a utilizar NAT. Consulte Capítulo 8, “Control del tráfico a través del cortafuegos” en la página 45 y utilice los servicios predefinidos que hay para las conexiones directas. Algunos ejemplos de servicios predefinidos que existen para las conexiones directas son:

- HTTP directamente
- Telnet directamente

Consulte el “Creación de conexiones utilizando los servicios predefinidos” en la página 46 para obtener más información.

Si desea que venga un servicio directamente a la red, deberá crearlo antes. Consulte “Utilización del cliente de configuración para crear servicios” en la página 66 para obtener información acerca de cómo hacerlo.

Apéndice A. Avisos

Las referencias que se hacen en esta publicación a productos, programas o servicios de IBM no implican que IBM tenga intención de comercializarlos en todos los países en los que opera. Cualquier referencia a un producto, programa o servicio de IBM no pretende indicar ni implica que sólo pueda utilizarse ese producto, programa o servicio de IBM. De acuerdo con la propiedad intelectual vigente de IBM u otros derechos con protección legal, podrá utilizarse cualquier producto, programa o servicio funcionalmente equivalente en lugar del producto, programa o servicio de IBM. La valoración y verificación de su funcionamiento conjuntamente con otros productos, a excepción de los que IBM designa de forma expresa, son responsabilidad del usuario.

IBM podría tener patentes o solicitudes de patentes pendientes acerca del tema que se describe en este documento. La adquisición de este documento no le concede ninguna licencia sobre tales patentes. Puede enviar sus consultas acerca de las licencias, por escrito, a:

IBM Director of Licensing
IBM Corporation
500 Columbus Avenue
Thornwood, NY 10594
USA

Los propietarios de licencias de este programa que deseen recibir información acerca de la misma con la finalidad de permitir: (i) el intercambio de información entre programas creados independientemente y otros programas (incluido éste) y (ii) la mutua utilización de la información que se ha intercambiado, deben ponerse en contacto con:

IBM Corporation
P.O. Box 12195
3039 Cornwallis
Research Triangle Park, NC 27709-2195
USA

Esta información podría estar disponible, de acuerdo a los términos y condiciones correspondientes, incluyendo, en algunos casos, el pago de una tarifa.

El programa bajo licencia que se describe en este documento y todo el material bajo licencia disponible para éste los proporciona IBM de acuerdo con los términos del IBM Customer Agreement.

Este documento no se ha creado para su utilización productiva y se adquiere tal cual, sin garantías de ningún tipo y, por la presente, se renuncia a todas las garantías, incluyendo las garantías de comercialización e idoneidad para una finalidad determinada.

Este producto incluye software desarrollado por la University of California, Berkeley y sus colaboradores.

Marcas registradas

Los términos siguientes son marcas registradas de IBM Corporation en los Estados Unidos y/o en otros países:

- Common User Access
- DB2
- eNetwork
- IBM
- OS/2

El logotipo de Microsoft, Windows, Windows NT, y Windows 95 son marcas registradas o nombres comerciales de Microsoft Corporation.

Java y HotJava son marcas registradas de Sun Microsystems, Inc.

Los otros nombres de empresas, productos y servicios, que podrían indicarse mediante un doble asterisco (**), pueden ser marcas registradas o marcas de servicio de otros.

Bibliografía

Para obtener información adicional acerca de la seguridad en Internet, visite la página de presentación del IBM eNetwork Firewall en la dirección **http://www.software.ibm.com/enetwork/firewall**.

Información en publicaciones de IBM

A continuación se listan otras fuentes de información de IBM acerca de los cortafuegos, la seguridad en Internet y temas que tratan la seguridad general.

Temas acerca del cortafuegos

Los documentos siguientes están disponibles en el CD-ROM del IBM Firewall y en la página de presentación del IBM eNetwork Firewall.

- *Guía del usuario del IBM eNetwork Firewall*, GC10-3279
- *Manual de consulta del IBM eNetwork Firewall*, SC10-3280
- *Guarding the Gates Using the IBM eNetwork Firewall for NT 3.2*, SG24-5209

Temas acerca de Internet y de la World Wide Web

- *A Guide to the Internet Connection Servers*, SG24-4805
- *Accessing CICS Business Applications from the World Wide Web*, SG24-4547
- *Accessing OS/390 OpenEdition MVS from the Internet*, SG24-4721
- *Accessing the Internet*, SG24-2597
- *Building the Infrastructure for the Internet*, SG24-4824
- *Cool Title about the AS/400 and Internet*, SG24-4815
- *The Domino Defense: Security in Lotus Notes and the Internet*, SG24-4848
- *Examples of Using MQSeries on WWW*, SG24-4882
- *How to Secure the Internet Connection Server for MVS/ESA*, SG24-4803
- *Lotus Domino Server Release 4.5 on AIX Systems: Installation, Customization, and Administration*, SG24-4694
- *Netscape Proxy Server*, SK2T-7444
- *Running CICS Transactions through the Web: The CICS Internet Gateway to VSE/ESA*, SG24-4799
- *Safe Surfing: How to Build a Secure World Wide Web Connection*, SG24-4564
- *Teach Yourself CGI Programming with PERL in a Week*, SR23-7343
- *Using the Information Super Highway*, GG24-2499
- *World Wide Web Access to DB2*, SG24-4716

Temas acerca de la seguridad general

- *The Basics of IP Network Design*, SG24-2580
- *Elements of Security: AIX V4.1*, GG24-4433
- *Enterprise-Wide Security Architecture and Solutions Presentation Guide*, SG24-4579
- *HACMP/6000 Customization Examples*, SG24-4498
- *IBM Global Network (IGN) Security Policy*, GC34-2206
- *IBM Security Architecture: Securing the Open Client/Server Distributed Enterprise*, SC24-8135
- *IBM Systems Monitor: Anatomy of a Smart Agent*, SG24-4398
- *Security Overview of Open Systems Networking*, GG24-3815
- *Systems Monitor for AIX User's Guide*, SC31-8173
- *TCP/IP Tutorial and Technical Overview*, GG24-3376

Información en publicaciones especializadas

Las publicaciones especializadas siguientes están relacionadas con TCP/IP y UNIX:

- Albitz, Paul, and Cricket Liu. *DNS and BIND*. Sebastopol, CA: O'Reilly and Associates, 1997. (ISBN: 1-56592-236-0)
- Costales, Brian with Eric Allman. *Sendmail*. O'Reilly and Associates, Inc. (ISBN: 1-56592-222-0)
- Hunt, Craig. *TCP/IP Network Administration*. O'Reilly and Associates, Inc. (ISBN: 0-937175-82-X)
- Nemeth, Snyder, et al. *UNIX System Administration Handbook*. Prentice Hall. (ISBN: 0-13-151051-7

Las publicaciones especializadas siguientes están relacionadas con los cortafuegos y con la seguridad en Internet:

- Ahuja, Vijay. *Network and Internet Security*. Boston: Academic Press Professional, 1996. (ISBN: 0120455951)
- Ahuja, Vijay. *Secure Commerce on the Internet*. Boston: Academic Press Professional, 1997. (ISBN: 0120455978)
- Anderson, Bart, et al. *The Waite Group's UNIX Communications and the Internet*. Indianapolis, IN: Sams Pub., 1995. (ISBN: 0672305372)
- Atkins, Derek, et al. *Internet Security: Professional Reference*. Indianapolis, IN: New Riders Publishing, 1996. (ISBN: 1562055577)
- Chapman, D. Brent, and Elizabeth D. Zwicky. *Building Internet Firewalls*. Sebastopol, CA: O'Reilly and Associates, 1995. (ISBN: 1565921240)
- Cheswick, Willam R., and Steven M. Bellovin. *Firewalls and Internet Security*. New York: Addison-Wesley, 1994. (ISBN: 0201633574)
- Cooper, Frederic J., et al. *Implementing Internet Security*. Indianapolis, IN: New Riders Publishing, 1995. (ISBN: 1562054716)
- Curry, David. *UNIX System Security: Guide for Users and Systems Administrators*. Sebastopol, CA: O'Reilly and Associates, 1994. (ISBN: 0201563274)
- Garfinkel, Simson, and Gene Spafford. *Practical UNIX Security*. Sebastopol, CA: O'Reilly and Associates, 1991. (ISBN: 0937175722)
- Garfinkel, Simson, and Gene Spafford. *Practical UNIX and Internet Security*. Sebastopol, CA: O'Reilly and Associates, 1996. (ISBN: 1565921488)
- Hare, Chris, and Karanjit Siyan. *Internet Firewalls and Network Security*. Indianapolis, IN: New Riders Publishing, 1996. (ISBN: 1562056328)
- Randall, Neil. *Teach Yourself the Internet in a Week*. Indianapolis, IN: Sams.Net, 1995. (ISBN: 0672307359)
- Stallings, William. *Internet Security Handbook*. Foster City, CA: IDG Books, 1995. (ISBN: 0077092546)
- Stevens, W. Richard. *TCP/IP Illustrated*. Reading, MA: Addison-Wesley, 1994. (ISBN: 0201634953)

Glosario

Puede acceder al glosario IBM Software en la dirección:
http://www.networking.ibm.com/nsg/nsgmain.htm.

Índice

T

U

V

Hoja de Comentarios

IBM eNetwork Firewall para Windows NT
Guía del usuario
Versión 3 Release 2.1.1

Número de Publicación GC10-3279-01

En general, ¿está Ud. satisfecho con la información de este libro?

	Muy satisfecho	Satisfecho	Normal	Insatisfecho	Muy insatisfecho
Satisfacción general	□	□	□	□	□

¿Cómo valora los siguientes aspectos de este libro?

	Muy bien	Bien	Acep-table	Insatisfecho	Muy insatisfecho
Organización	□	□	□	□	□
Información completa y precisa	□	□	□	□	□
Información fácil de encontrar	□	□	□	□	□
Utilidad de las ilustraciones	□	□	□	□	□
Claridad de la redacción	□	□	□	□	□
Calidad de la edición	□	□	□	□	□
Adaptación a los formatos, unidades, etc. del país	□	□	□	□	□

Comentarios y sugerencias:

Nombre

Dirección

Compañía u Organización

Teléfono

Hoja de Comentarios
GC10-3279-01

Corte o Doble
Por la Línea

Dóblese por la línea de puntos **Por favor no lo grape** Dóblese por la línea de puntos

PONER
EL
SELLO
AQUÍ

IBM, S.A.
National Language Solutions Center
Av. Diagonal, 571
08029 Barcelona
España

Dóblese por la línea de puntos **Por favor no lo grape** Dóblese por la línea de puntos

Corte o Doble
Por la Línea

Printed in the United States of America
on recycled paper containing 10%
recovered post-consumer fiber.

GC10-3279-01