IBM SecureWay® Boundary Server para Windows NT® y AIX

Puesta a punto

Versión 2.0

GC10-3502-00

IBM SecureWay® Boundary Server para Windows NT® y AIX

Puesta a punto

Versión 2.0

GC10-3502-00

Nota

Antes de utilizar esta información y el producto al que da soporte, asegúrese de leer la información general contenida en el Apéndice B, “Avisos” en la página 35.

Esta edición se aplica a la versión 2, release 0, modificación 0 del producto IBM SecureWay Boundary Server (GC31-8733-00) y a todos los releases y modificaciones posteriores hasta que se indique lo contrario en nuevas ediciones.

Segunda edición (octubre 1999)

Contenido

Acerca de este manual

Este manual describe la planificación, instalación, configuración, utilización y resolución de problemas de IBM SecureWay®Boundary Server para Windows NT® y AIX.

Es importante que tenga conocimientos sólidos sobre cortafuegos, redes privadas virtuales, seguridad de contenidos y administración de redes antes de instalar y configurar SecureWay Boundary Server. Puesto que se instalará y se configurará un cortafuegos que controlará la entrada y la salida de la red, primero es necesario comprender cómo funciona la red. En especial, es necesario comprender los temas básicos sobre direcciones IP, nombres totalmente calificados y máscaras de subred.

A quién va dirigido este manual

Este manual va dirigido a los administradores de red o de seguridad del sistema que instalen, administren y utilicen IBM SecureWay Boundary Sever.

Preparación para el año 2000

Estos productos están preparados para el año 2000. Si se utilizan de acuerdo con la documentación relacionada, pueden procesar, proporcionar y recibir correctamente datos de fecha de los siglos XX y XXI, siempre que todos los demás productos (por ejemplo, hardware, software y firmware) utilizados intercambien datos de fecha adecuadamente con los primeros.

Servicio y soporte

Póngase en contacto con IBM para obtener servicio y soporte para todos los productos incluidos en la oferta IBM SecureWay FirstSecure. Algunos de estos productos pueden hacer referencia a soporte que no sea de IBM. Si adquiere estos productos como parte de la oferta FirstSecure, póngase en contacto con IBM para obtener servicio y soporte.

Cómo se organiza este manual

Este manual contiene los capítulos siguientes:

- El Capítulo 1, “Visión general de SecureWay Boundary Server” en la página 1 proporciona una visión general de SecureWay Boundary Server y de sus componentes.
- El Capítulo 2, “Introducción a IBM SecureWay Boundary Server” en la página 5 proporciona información sobre los motivos por los que se necesita SecureWay Boundary Server.
- El Capítulo 3, “Antes de instalar SecureWay Boundary Server” en la página 11 proporciona información sobre cómo planificar SecureWay Boundary Server.
- El Capítulo 4, “Requisitos para IBM SecureWay Boundary Server (SBS)” en la página 15 proporciona información acerca de los requisitos mínimos para SecureWay Boundary Server.

- El Capítulo 5, “Instalación y configuración de SecureWay Boundary Server” en la página 17 describe la instalación y la configuración de SecureWay Boundary Server en los sistemas operativos Windows NT y AIX.
- El Capítulo 6, “Documentación relacionada” en la página 29 indica dónde se puede encontrar más documentación sobre SecureWay Boundary Server y documentación sobre los productos relacionados.

Convenios

Este manual emplea los convenios siguientes:

Convenio	Significado
negrita	Elementos de la interfaz de usuario tales como recuadros de selección, botones y mandatos
monoespaciado	Valores por omisión de sintaxis y directorios relevantes para SecureWay Boundary Server
->	Muestra una serie de selecciones de un menú. Por ejemplo, seleccionar **Archivo-> Ejecutar** significa seleccionar **Archivo** y, a continuación, pulsar **Ejecutar**

Información en la Web

La información sobre actualizaciones de última hora de SecureWay Boundary Server está disponible en la dirección Web siguiente:

http://www.ibm.com/software/security/boundary/library

La información sobre actualizaciones de otros productos IBM SecureWay FirstSecure está disponible en la dirección Web siguiente:

http://www.ibm.com/software/security/firstsecure/library

Novedades

La versión 2.0 de SecureWay Boundary Server contiene varias características nuevas. Las características nuevas más significativas se listan a continuación.

Integración con SecureWay Policy Director

SecureWay Policy Director puede gestionar los usuarios del proxy cortafuegos, siempre que el cortafuegos esté habilitado para SecureWay Boundary Server. Los usuarios del proxy cortafuegos se definen para los servicios de cortafuegos siguientes:

- Telnet
- FTP
- HTTP
- Socks

Los usuarios y sus políticas asociadas se almacenan en la base de datos LDAP (Lightweight Directory Access Protocol).

SecureWay Directory proporciona LDAP para mantener información de directorios en una ubicación central para almacenamiento, actualizaciones, recuperación e

intercambio. SecureWay Policy Director gestiona los usuarios del proxy cortafuegos en la base de datos LDAP.

Eficiencias en el direccionamiento

Las eficiencias en el direccionamiento utilizan un complemento Finjan SurfinGate para limitar el circuito del tráfico de red para filtrar el contenido.

Bloqueo de intrusiones

La línea de mandatos se programa para crear reglas DENY dinámicas en el cortafuegos. El bloqueo de intrusiones se puede incluir en un script automatizado.

IBM SecureWay Firewall 4.1

IBM SecureWay Firewall para Windows NT ofrece:

Servicio de acceso remoto

El servicio de acceso remoto de Windows NT (RAS) proporciona conexiones de red con soportes de marcación, RDSI o X.25 utilizando el protocolo de punto a punto (PPP). NDISWAN es un controlador de red que se proporciona como parte del RAS y que realiza una conversión de los datos de PPP subyacentes de modo que se parezcan a datos de LAN de Ethernet.

Mejoras de IBM SecureWay Firewall para AIX 4.1

IBM SecureWay Firewall para AIX ofrece:

Soporte de IPSec mejorado

IBM SecureWay Firewall 4.1 incluye un soporte de IPSec mejorado, que incluye el cifrado DES triple y el soporte de nuevas cabeceras. También da soporte a la interoperatividad con servidores y direccionadores IBM, así como muchos productos VPN que no son IBM y que dan soporte a las nuevas cabeceras.

Multiprocesador simétrico (SMP)

Los usuarios del cortafuegos pueden aprovechar las características de multiprocesador del RS/6000 para las mejoras en el rendimiento y escalado.

Mejoras de filtros

Se han mejorado los filtros para proporcionar un mejor rendimiento con la configuración. Puede ajustar el rendimiento de su cortafuegos eligiendo dónde ubicar los diferentes tipos de reglas de filtros. Además, se anota cronológicamente el número de veces que se utiliza una conexión.

Asistente para la instalación

Un asistente le ayuda a configurar inicialmente IBM SecureWay Firewall. Este asistente para la instalación permite que los nuevos usuarios tengan

una configuración de cortafuegos básica activa y en funcionamiento después de instalar IBM Firewall.

Auditor de seguridad de la red

El Auditor de seguridad de la red (NSA) comprueba que no haya agujeros en la seguridad o errores de configuración en los servidores de la red y en el cortafuegos. Se ha mejorado para que sea más rápido y sólido.

Soporte del idioma nacional para el alemán

Ahora se ofrece Soporte del idioma nacional para el alemán, además de portugués brasileño, portugués, inglés, francés, italiano, japonés, coreano, chino simplificado, español y chino tradicional.

Conversión de direcciones de red

Se ha mejorado la conversión de direcciones de red (NAT) para dar soporte a correlaciones de varias direcciones a una. Estas correlaciones son de varias direcciones internas, privadas o no registradas, a una sola dirección legal registrada utilizando números de puerto para crear correlaciones exclusivas.

Funciones comunes soportadas por AIX y Windows NT

Security Dynamics ACE/Server

Security Dynamics ACE/Server proporciona dos factores de autenticación. Esta característica ha sido mejorada y protege los recursos de red y datos de intrusiones accidentales o intencionadas potencialmente devastadoras.

Mejoras del proxy de correo seguro

Se ha mejorado el proxy de correo seguro de IBM Firewall para que incluya las nuevas funciones siguientes:

- Algoritmos contra SPAM, incluido el bloqueo de mensajes procedentes de usuarios de SPAM conocidos (una lista de exclusión), comprobaciones de verificación sobre la validez de los mensajes y la posibilidad de responder a los mismos (maneras conocidas de bloquear mensajes no deseables), límites configurables sobre el número de receptores por mensajes de correo, límites configurables sobre el tamaño máximo de un mensaje
- Soporte contra la suplantación, incluida la integración con potentes mecanismos de autenticación
- Soporte de condición de excepción SNMP y soporte para MADMAN MIB
- Rastreo de mensajes, incluida la capacidad de rastrear sin errores mensajes entre el cortafuegos y Domino

Mejoras de Socks protocol, versión 5

Se ha actualizado Socks protocol versión 5 para que incluya autenticación de ID de usuario y contraseña (UNPW), autenticación por petición de identificación y respuesta (CRAM) y complementos de autenticación.

Se ha mejorado el registro cronológico para que los usuarios posean más control al clasificar los mensajes de anotación cronológica y al especificar niveles de registro cronológico.

Proxy HTTP

IBM SecureWay Firewall proporciona una implantación de proxy HTTP, con toda clase de características, basada en el producto IBM Web Traffic Express (WTE). El proxy HTTP maneja de modo eficaz las peticiones del navegador mediante IBM Firewall, con lo que elimina la necesidad de un servidor de socks para la navegación por la Web. Los usuarios pueden acceder a información de Internet útil, sin que por ello comprometan la seguridad de las redes internas. El navegador debe estar configurado para utilizar un proxy HTTP.

MIMEsweeper 2.0 para SecureWay

MIMEsweeper tiene tres componentes principales: **MAILsweeper 4.1_2**, **WEBsweeper 3.2_5** y **WEBsweeper 1.0_2**. Algunas de las mejoras son:

MAILsweeper

MAILsweeper 4.1_2 para SMTP es una actualización importante del producto estrella de Content Technologies, MIMEsweeper. Presenta las nuevas funciones siguientes:

- Una arquitectura de política jerárquica y fácil de usar proporciona la flexibilidad para aplicar políticas desde el nivel apropiado de la organización hasta un usuario individual
- Una interfaz gráfica de usuario (GUI) que cumple el estándar de la industria simplifica la configuración del software, la creación de políticas y la administración
- La nueva característica Split Delivery es una función de la implantación de políticas jerárquicas de la versión 4. En mensajes para varios receptores, se aplican políticas para cada receptor. Los receptores autorizados reciben el mensaje, mientras que éste se deniega a los receptores no autorizados
- El proceso de mensajes de varias hebras mejora la productividad y proporciona solidez al permitir que continúe el proceso del mensaje, al utilizar las hebras restantes, en el caso de un error en una o más hebras
- MAILsweeper, junto con productos antivirus de otros proveedores, proporciona la detección y la depuración de virus en mensajes y archivos adjuntos
- El análisis avanzado de texto mediante las expresiones NEAR, AND, NOT y OR permiten una enorme flexibilidad a la hora de crear escenarios completos y efectivos basados en la arquitectura o la sintaxis del mensaje
- Herramientas de auditoría mejoradas que pueden enviar datos a cualquier base de datos que cumpla con los requisitos ODBC
- Soporte de servidor de Lista negra a tiempo real (RBL), que lista los sitios de los que se sabe que procede correo basura. MAILsweeper puede rechazar conexiones que procedan de cualquier sistema principal de esta lista.
- La seguridad del contenido es más fácil de gestionar mediante atractivos informes / gráficos / estadísticas del tráfico de correo electrónico
- Integración con directorios LDAP

- Ahora la Notificación de servicio de entrega (DSN) da soporte a SNMP y NT Alerter

WEBsweeper

- Las mejoras de rendimiento adicionales aceleran la velocidad de proceso de datos.
- Funciona con exploradores de virus para tráfico HTTP y FTP

WEBsweeper HTTPS

- Ahora WEBsweeper proporciona soporte completo para aplicaciones de comercio electrónico basadas en la Web mediante una nueva solución de proxy HTTPS

SurfinGate 4.05

Las mejoras en SurfinGate incluyen:

Inspección de contenido en JavaScripts

SurfinGate 4.05 busca operaciones de JavaScript potencialmente problemáticas y para los JavaScripts que entren en conflicto con la política de seguridad de la empresa. SurfinGate 4.05 permite que los administradores establezcan y apliquen de manera central una política para JavaScript, Java y ActiveX, con el filtrado inteligente de cookies y scripts de VisualBasic.

Supervisión del rendimiento de misión crítica

SurfinGate 4.05 incluye una herramienta automática que detecta comportamientos anormales (por ejemplo, errores de ejecución) y reinicia SurfinGate en caso de anomalía. Esta función de seguridad es esencial para zonas de misión crítica.

Gestión de política incrementada

SurfinGate entra perfiles de applet no resueltos en la base de datos para su bloqueo automático. Los administradores pueden editar la lista de applets/controles.

Soporte para FTP y el protocolo SSL

SurfinGate 4.05 supervisa el código móvil en los canales del protocolo de transferencia de archivos (FTP), vigilando código que en otras circunstancias entraría de Internet inadvertidamente. Además del FTP, SurfinGate supervisa el código móvil en el tráfico HTTP y hace pasar dicho tráfico por dispositivos adicionales.

Integración de complemento con el proxy HTTP de cortafuegos

SurfinGate funcionará como proxy en una cadena de proxys o a través de un complemento en Web Traffic Express en el cortafuegos para NT.

Capítulo 1. Visión general de SecureWay Boundary Server

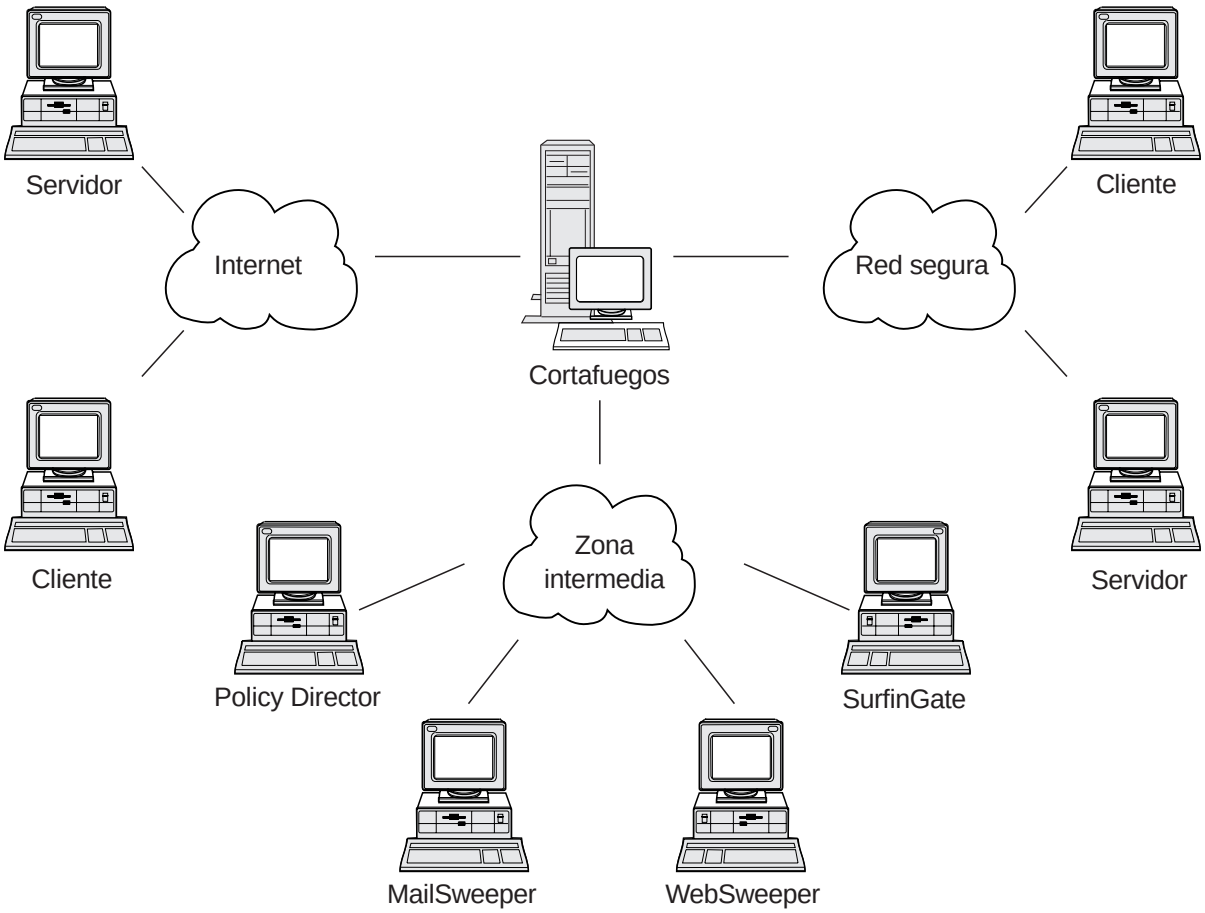

Figura 1. Ejemplo de configuración de IBM SecureWay Boundary Server

Este ejemplo muestra cinco estaciones de trabajo que utilizan los componentes MAILsweeper, WEBsweeper, Policy Director y SurfinGate para supervisar y direccionar el tráfico de la Web y el correo entre clientes y servidores mediante un cortafuegos. Para este ejemplo utilizaremos cinco estaciones de trabajo separadas físicamente.

Ejemplos típicos de SecureWay Boundary Server

Se recomienda que utilice las máquinas siguientes para una instalación mínima:

Tabla 1. Requisitos de hardware para productos componentes de Boundary Server

Producto	**Máquina**
IBM Firewall	Windows NT o AIX
MAILsweeper	Windows NT
WEBsweeper	Windows NT
SurfinGate	Windows NT

Si desea aprovechar completamente SecureWay Boundary Server, SecureWay Policy Director debe estar en su red. Esto permite que los usuarios del proxy cortafuegos se almacenen en SecureWay Directory (LDAP).

Ejemplo de HTTP (cortafuegos en Windows NT): En un escenario típico, se originaría una petición HTTP de contenido en Internet en la máquina cliente. La petición se dirigiría primero a WEBsweeper. En la vía de salida, WEBsweeper simplemente enviaría la petición por proxy al proxy HTTP de cortafuegos.

En el proxy HTTP de cortafuegos se autenticaría el usuario. Si esta es la primera petición de una sesión de navegación de un cliente, se presentaría la petición de ID de usuario y contraseña. El ID de usuario se utilizaría para buscar la política de seguridad del cliente en la base de datos LDAP que administra Policy Director. En función de la política de autenticación HTTP para el cliente, y del resultado de la comprobación de la contraseña entrada, la petición seriá denegada o se le permitiría proceder. La operación de autenticación puede requerir más accesos a la base de datos LDAP o a Security Dynamics ACE/Server. En peticiones posteriores de la misma sesión de navegación, el navegador proporcionará el ID de usuario y la contraseña automáticamente. No se pedirá identificación al cliente, pero cada petición se autenticará mediante el mismo proceso que en la primera petición.

Si la autenticación se realiza satisfactoriamente, la petición se enviará por proxy al servidor solicitado en Internet.

Cuando el proxy HTTP de cortafuegos reciba de nuevo el contenido del servidor de Internet, el complemento SurfinGate examinará dicho contenido. El complemento dispondrá de la información de grupo correspondiente al usuario, obtenida de la base de datos LDAP sobre la que basar decisiones de política. Si el contenido no contiene nada de interés para SurfinGate, pasará rápidamente a través del complemento con una carga de proceso mínima. El complemento filtrará el contenido que incluya JavaScript. El contenido que incluya Java o ActiveX se reenviará al servidor SurfinGate para su filtrado y el contenido filtrado se devolverá al proxy HTTP de cortafuegos. El contenido resultante del proceso del complemento SurfinGate se volverá a enviar al servidor WEBsweeper.

Cuando el contenido llegue nuevamente al servidor WEBsweeper, se filtrará de acuerdo con las políticas de WEBsweeper y, a continuación, se devolverá al cliente.

Ejemplo de HTTP (cortafuegos en AIX): En AIX el flujo del tráfico es esencialmente idéntico, excepto que el complemento SurfinGate no está disponible para el cortafuegos de AIX. Por tanto, el servidor SurfinGate se debe configurar como un proxy en una cadena de proxys del cliente al cortafuegos. Se debe configurar WEBsweeper para reenviar peticiones al servidor SurfinGate, en lugar de enviarlas directamente al proxy HTTP de cortafuegos. Se debe configurar el servidor SurfinGate para reenviar peticiones al proxy HTTP de cortafuegos. No habrá información de grupo disponible en el servidor SurfinGate, de modo que las decisiones de política solamente se pueden basar en la dirección IP.

Ejemplo de correo: MAILsweeper se configura como una pasarela de correo. El contenido del correo que llega al servidor MAILsweeper se filtra antes de reenviarlo al siguiente servidor de correo.

Cada servidor de correo seguro debe configurarse para que reenvíe peticiones de correo de cliente al servidor MAILsweeper. Debe configurarse el intercambiador de correo de cortafuegos para que reenvíe el correo de entrada al servidor MAILsweeper.

MAILsweeper debe configurarse para que envíe el correo dirigido a dominios externos al intercambiador de correo del cortafuegos. MAILsweeper debe estar configurado para que envíe el correo dirigido a dominios internos al servidor de correo seguro correcto.

Capítulo 2. Introducción a IBM SecureWay Boundary Server

En este capítulo se proporciona una visión general de SecureWay Boundary Server y se incluyen las secciones siguientes:

- "Qué es SecureWay Boundary Server"
- "Por qué es necesario SecureWay Boundary Server"
- "Cómo encaja SecureWay Boundary Server en FirstSecure"
- "Componentes de SecureWay Boundary Server" en la página 6

Qué es SecureWay Boundary Server

IBM SecureWay Boundary Server ofrece, por primera vez, una solución completa para la seguridad de límites. SecureWay Boundary Server proporciona protección de cortafuegos, red privada virtual (VPN) y seguridad de contenidos. SecureWay Boundary Server combina la tecnología de la industria de seguridad con una solución integrada respaldada por los servicios y el soporte de IBM. Esta solución incluye:

- IBM SecureWay Firewall 4.1 (incluye Security Dynamic ACE/Server)
- MIMEsweeper de Content Technologies
  - MAILsweeper 4.1_2
  - WEBsweeper 3.2_5
  - Proxy HTTPS WEBsweeper 1.0_2
- SurfinGate 4.05 de Finjan
  - Servidor SurfinGate
  - SurfinConsole
  - Base de datos SurfinGate
  - Complemento SurfinGate para la integración WTE para Windows NT 1.0

Por qué es necesario SecureWay Boundary Server

Los límites seguros son necesarios en todas partes: entre departamentos, como el de informática y el de recursos humanos, entre la red de las oficinas centrales y las sucursales, entre la red de la empresa e Internet, entre las aplicaciones de la Web de la empresa y los clientes, entre la red o las aplicaciones de la empresa y los socios comerciales. La seguridad en los límites no sólo protege la red, las aplicaciones y la información, sino que, además, amplía su alcance. Una seguridad de límites requiere el control de las personas que acceden a la red y la información que entra o sale de la red.

Cómo encaja SecureWay Boundary Server en FirstSecure

IBM SecureWay FirstSecure es un paquete de productos integrados. Proporciona una infraestructura completa que ayuda a asegurar todos los aspectos sobre redes en Internet y otras redes. Ayuda a crear, sobre las inversiones actuales, ofertas modulares e interoperativas y a minimizar el coste total de propiedad para realizar e-business de manera segura. Proporciona protección contra virus, control de acceso, control de contenidos del tráfico, cifrado, certificados digitales, cortafuegos, kits de herramientas y servicios de implantación.

Boundary Server es un paquete de productos que encaja con FirstSecure. Crea un límite con Internet que se puede utilizar para bloquear virus dañinos en potencia (empleando los productos adjuntos de exploración de virus), JavaScript, applets Java, controles de ActiveX e incluso el correo basura (SPAM). Con Boundary Server, puede controlar de forma exacta lo que desea que entre en su red procedente de Internet. Con SecureWay Policy Director, gestiona los usuarios del proxy cortafuegos y sus políticas de autenticación.

Componentes de SecureWay Boundary Server

Los tres componentes de SecureWay Boundary Server son IBM Firewall, MIMEsweeper y SurfinGate. SecureWay Boundary Server proporciona la integración con IBM SecureWay Policy Director.

Visión general de IBM SecureWay Boundary Server

IBM SecureWay Boundary Server proporciona a grandes organizaciones la protección, el control de acceso y la seguridad de contenidos que se precisan para realizar e-business abriendo de manera segura la empresa a clientes, proveedores y socios. Las características comprenden lo siguiente:

- Protección de cortafuegos para la red
- Red privada virtual (VPN) para ampliar el alcance de la red
- Explorador de contenidos para tráfico de Web y correo electrónico para proteger los datos, la imagen, la fiabilidad y la productividad de la empresa

SecureWay Boundary Server combina la mejor tecnología de la industria con una solución integrada respaldada por los servicios y el soporte de IBM. Se encuentra disponible para los sistemas operativos AIX y Windows NT.

Función de SecureWay Boundary Server

SecureWay Boundary Server aplica la tecnología de filtrado de paquetes, de proxys y Socks, y la seguridad de contenidos para ocultar y proteger la red y los sistemas. Estas tecnologías permiten que los administradores definan de manera explícita qué datos pueden entrar a la red o salir de ella. Esto contribuye a evitar los denominados "denial of service attacks" (ataques tipo denegación de servicio) y los intentos por parte de piratas informáticos de penetrar en la red, además de limitar las responsabilidades legales. SecureWay Boundary Server ofrece una solución VPN que le permite sustituir servidores remotos y bancos de módems con una solución basada en Internet.

Cuando se despliega con Policy Director, SecureWay Boundary Server ofrece autenticación de usuarios utilizando un plan central basado en políticas. Se puede utilizar el software antivirus con SecureWay Boundary Server para proporcionar protección contra virus en su sitio.

Visión general de IBM SecureWay Policy Director

Policy Director es una solución autónoma de gestión de seguridad y autorización que proporciona una seguridad de extremo a extremo en recursos de intranets y extranets diseminadas geográficamente. Una extranet es una red privada virtual (VPN) que utiliza funciones de control de acceso y seguridad para restringir el uso de una o más intranets conectadas a Internet a suscriptores seleccionados. Policy Director proporciona servicios de autenticación, autorización, seguridad de datos y

gestión de recursos. Utilice Policy Director junto con aplicaciones estándar basadas en Internet para crear intranets y extranets seguras y correctamente gestionadas.

Función de IBM SecureWay Policy Director

Cuando se emplea con SecureWay Boundary Server, IBM SecureWay Policy Director proporciona almacenamiento de políticas de usuario del proxy e información sobre autenticación.

Visión general de IBM SecureWay Firewall

IBM SecureWay Firewall es un programa de seguridad de redes. Un cortafuegos es un punto de bloqueo entre una o mas redes privadas, internas y seguras y otras redes o Internet. Un cortafuegos evita la comunicación entrante o saliente no deseada o no autorizada en la red segura.

Función de IBM SecureWay Firewall

IBM SecureWay Firewall limita el acceso entre una red protegida, Internet y otros conjuntos de redes. También lleva a cabo lo siguiente:

- Limita la entrada de personas en un punto cuidadosamente controlado
- Evita que los atacantes se acerquen a otras defensas
- Limita la salida de personas en un punto cuidadosamente controlado
- Los cortafuegos internos evitan que puedan acceder a información interna y sensible los empleados no autorizados
- Limita el tráfico que puede entrar y salir de la red

Visión general de MIMEsweeper

MIMEsweeper proporciona seguridad de contenidos al analizar los datos que pasan a través del cortafuegos por correo electrónico o por la World Wide Web. La seguridad de contenidos permite que las organizaciones gestionen de modo efectivo asuntos comerciales relacionados con el uso del correo electrónico y la World Wide Web. Estos asuntos se pueden dividir en integridad de la red e integridad del negocio.

El filtrado de la integridad de la red puede:

- Identificar y eliminar virus en el correo electrónico entrante y saliente
- Filtrar tipos de archivos no deseables
- Gestionar archivos de tamaño excesivo
- Proteger redes de la congestión o la pérdida de servicios debido a la saturación a causa de un envío de correo masivo

El filtrado de la integridad del negocio puede:

- Evitar fisuras en la confidencialidad y la pérdida de secretos comerciales
- Limitar la exposición a responsabilidades legales
- Reducir las pérdidas ocasionadas por el mal uso de los servicios de correo electrónico y la World Wide Web por parte de los empleados
- Evitar la pérdida de servicios de red debido a un mal uso o a ataques hostiles

Las amenazas a la integridad de la red pueden dañar o borrar datos, perturbar el flujo del correo e inutilizar el hardware del sistema, lo que comporta la

desactivación de la red, la pérdida de productividad y elevados costes de limpieza y recuperación.

Sin embargo, las amenazas a la integridad del negocio pueden ser todavía más destructivas, con el resultado de enormes costes legales, la pérdida de la propiedad intelectual y daños en la reputación y la credibilidad de la empresa. Los asuntos de integridad del negocio pueden hacer que las operaciones comerciales queden paralizadas.

MIMEsweeper es el producto líder de la industria para la protección de organizaciones ante asuntos de integridad de la red y el negocio que surgen por el uso del correo electrónico e Internet por parte de la organización.

Función de MIMEsweeper

MIMEsweeper puede realizar lo siguiente:

- Añadir una declaración de limitación de responsabilidad legal al correo saliente
- Proteger documentos y datos confidenciales
- Autorizar y controlar a los usuarios de el correo electrónico y de la Web
- Poner en cuarentena o bloquear material ofensivo
- Bloquear el correo basura
- Explorar el contenido apropiado en archivos adjuntos o bajados
- Detener virus y códigos dañinos
- Bloquear páginas y sitios Web inapropiados
- Informar, anotar cronológicamente y archivar

Visión general de SurfinGate

SurfinGate 4.05 es una herramienta de seguridad del código móvil para cualquier negocio que utilice Internet, extranet o intranet para transacciones comerciales. Mediante la inspección de contenidos en el código móvil, que incluye JavaScript, SurfinGate contribuye a proteger las redes informáticas de daños hostiles o no intencionados, incluidos el espionaje industrial, la modificación de datos y la eliminación de información. El proceso de inspección de contenidos de SurfinGate inspecciona el contenido de código móvil Java, JavaScript y ActiveX a nivel de pasarela, lejos de recursos críticos, y asigna un ID exclusivo y un perfil de seguridad de applet (ASP) al código, advirtiendo cualquier fisura en la seguridad. SurfinGate identifica código potencialmente problemático antes de que entre en la red.

SurfinGate 4.05 incluye cuatro componentes:

- Servidor SurfinGate
- SurfinConsole
- Base de datos SurfinGate
- Complemento SurfinGate para la integración WTE para Windows NT

El servidor SurfinGate actúa como un servidor de proxy HTTP. SurfinGate se puede colocar como parte de una cadena de proxys junto con el proxy HTTP del cortafuegos y el proxy WEBsweeper. Para Windows NT, puede utilizarse alternativamente como complemento para el proxy HTTP de cortafuegos. Cuando se utiliza como complemento, SurfinGate obtendrá información de grupo para el usuario del proxy que realiza la petición. Las políticas de filtrado de SurfinGate pueden basarse en esta información de grupo. Esta arquitectura permite detener e

inspeccionar el tráfico de código móvil antes de que tenga lugar cualquier ataque. Este componente proporciona protección relacionada con política de seguridad de la empresa.

SurfinConsole es una interfaz fácil de usar que sirve para gestionar y configurar la política de seguridad de la empresa respecto al código móvil. SurfinConsole puede controlar varios servidores SurfinGate de la red y puede aplicar reglas de código móvil a toda la empresa por usuario, por grupo o mediante listas personalizadas de código aceptable o no aceptable.

La base de datos SurfinGate almacena detalles de perfiles de seguridad de applet (ASP), incluida la información referente a usuarios y grupos y a sus políticas de seguridad correspondientes. La base de datos puede emplear un motor de base de datos de acceso incorporado o una base de datos Oracle existente. Dado que SurfinGate inspecciona el contenido del código móvil sobre la marcha, la base de datos no es necesaria para la seguridad, pero ayuda a mejorar el rendimiento en operaciones a gran escala.

Función de SurfinGate

SurfinGate proporciona lo siguiente:

- Un servidor de inspección de contenidos a nivel de pasarela para applets de Java, controles de Active, JavaScript
- Supervisión a tiempo real e inspección dinámica
- La aplicación de la política de seguridad para código móvil basado en Web
- La inspección de "código móvil" (por ejemplo, applets de Java, controles de ActiveX, JavaScript, scripts de Visual Basic, complementos y cookies)

SurfinGate puede funcionar con un proxy en una cadena de proxys o a través de un complemento de WTE en el cortafuegos para Windows NT.

Capítulo 3. Antes de instalar SecureWay Boundary Server

En este capítulo se describen los métodos para prepararse a fin de instalar SecureWay Boundary Server utilizando el asistente, y se incluyen las secciones siguientes:

- "Cómo prepararse"
- "SecureWay Boundary Server" en la página 13

Cómo prepararse

En esta sección se detalla el método para preparar los componentes para SecureWay Boundary Server.

Integración con SecureWay Policy Director

Para una instalación básica de IBM SecureWay Policy Director en Windows NT o AIX, lleve a cabo lo siguiente:

1. Compruebe que su sistema operativo está configurado apropiadamente para que dé soporte a Policy Director.
2. Determine los componentes de servidor que se ajustarán mejor a sus requisitos de despliegue y las máquinas en las que se instalarán dichos componentes.
3. Instale y configure una infraestructura DCE, si no hay ninguna.
4. Instale y configure SecureWay Directory (LDAP).
5. Configure el Servicio de autorización certificada (CAS) si llevará a cabo la autenticación certificada del cliente.
6. Instale el cliente NetSEAT.
7. Instale los componentes de servidor de Policy Director.
8. Instale la Consola de gestión.

Para obtener más información acerca de Policy Director, consulte el manual *Policy Director Up and Running 3.0*.

SecureWay Firewall

Para una instalación básica de IBM Firewall en Windows NT o AIX, lleve a cabo lo siguiente:

1. Asegúrese de que cumple los requisitos previos listados en el apartado "Requisitos de hardware para SecureWay Boundary Server" en la página 15.
2. Planifique la configuración de IBM Firewall. Decida de antemano las funciones que desea utilizar del cortafuegos y el modo en que desea utilizarlas.
3. Indique al cortafuegos qué interfaces están conectadas a redes seguras. Para que el cortafuegos funcione correctamente, debe tener una interfaz segura y una interfaz no segura. En el árbol de navegación del cliente de la configuración, abra la carpeta System Administration (Administración del sistema) y pulse **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 **Change (Cambiar)**.

Nota: Si tiene intención de conectarse a Internet, póngase en contacto con su suministrador de servicio de Internet (ISP) para obtener una dirección IP registrada para la interfaz no segura del cortafuegos.

4. Configure su política de seguridad general accediendo al diálogo **Security Policy (Política de seguridad)** en la carpeta System Administration (Administración del sistema). Para configuraciones típicas de cortafuegos:
   - Permita consultas del DNS
   - Deniegue mensajes de difusión general a la interfaz no segura
   - Deniegue socks a los adaptadores que no sean seguros
5. Configure el servicio de nombres de dominio y el servicio de correo. No habrá comunicación eficiente si no proporciona una resolución del DNS. Acceda a estas funciones desde la carpeta System Administration (Administración del sistema) en el árbol de navegación del cliente de la configuración.
6. Defina los elementos clave de su red o redes en el cortafuegos utilizando la función **Network Objects (Objetos de red)** en el árbol de navegación del cliente de la configuración. Los objetos de red controlan el tráfico a través del cortafuegos. Defina como objetos de red los elementos clave siguientes:
   - Interfaz segura del cortafuegos
   - Interfaz no segura del cortafuegos
   - Red segura
   - Cada subred de la red segura
   - Un objeto de red del sistema principal para los servidores Security Dynamics y para los servidores de dominio Windows NT, si procede
7. Habilite los servicios en el cortafuegos. Son métodos (por ejemplo, socks o proxy) mediante los cuales los usuarios de la red segura pueden acceder a la red no segura. Los servicios que se implanten dependerán de las decisiones que se tomen en la fase de planificación. La implantación de un servicio requiere a menudo configuraciones de conexión para permitir el paso de ciertos tipos de tráfico. Por ejemplo, si desea que los usuarios de red segura naveguen por la Web en Internet utilizando el proxy HTTP, no sólo necesitará configurar el daemon del proxy HTTP en el cortafuegos, sino que también deberá configurar conexiones para permitir el tráfico HTTP. Si va a instalar Policy Director, consulte la sección “Integración con SecureWay Policy Director” en la página 11.
8. **Sólo para Windows NT:** puesto que el proceso de protección inhabilita NETBIOS, si desea utilizar para la autenticación las contraseñas de dominio de Windows NT, debe configurar el código de cliente de Windows que implemente la capacidad de buscar dominios de Windows NT fiables para fines de autenticación. Los servidores Windows NT fiables deben tener nombres y direcciones de sistema principal TCP/IP, así como conectividad TCP/IP entre ellos y el cortafuegos. El administrador del cortafuegos necesita crear conexiones entre el cortafuegos y el servidor Windows NT fiable a fin de permitir que el tráfico fluya entre ambos.
9. Si utiliza la conversión de direcciones de red, póngase en contacto primero con su ISP para obtener una dirección de Internet registrada para utilizarla en la conversión de varias direcciones a una. Esta dirección se añade a la dirección que ha solicitado en el paso 3 en la página 11. A continuación, vaya al panel *Add NAT Configuration (Añadir configuración NAT)* para añadir la dirección de Internet registrada en el campo *Many-to-One IP Address (Dirección IP de varias a una)*.

Siguiendo estos pasos debería obtener una configuración básica de cortafuegos activa y en funcionamiento. IBM Firewall proporciona otras funciones, como

registros cronológicos del sistema que le ayudan a garantizar la seguridad de la red.

Si el cortafuegos se cierra de manera normal o anormal, los datos de configuración no se ven afectados porque se guardan en la unidad del disco duro y se vuelven a activar automáticamente cuando se rearranca. Sin embargo, aparecerán algunos mensajes de anotación cronológica que indiquen que algunas conexiones activas, por ejemplo, una sesión FTP activa, se han interrumpido.

SecureWay Boundary Server

Puede utilizar el asistente de SecureWay Boundary Server para definir el cortafuegos de modo que utilice IBM SecureWay Policy Director para que la administración de usuarios se integre con Policy Director. Opcionalmente, este asistente configura el proxy HTTP del cortafuegos para que pase información de autenticación al complemento SurfinGate (sólo para Windows NT).

La información que precisará para configurar IBM SecureWay Boundary Server para el cortafuegos es la siguiente:

- El dominio y nombre del sistema principal del servidor IBM SecureWay Directory que utilizará el cortafuegos.
- El número del puerto de comunicación del servidor IBM SecureWay Directory. El puerto por omisión es el 389.
- La contraseña SecurityMaster para el servidor IBM SecureWay Directory.
- El nombre de dominio que se utilizará para distinguir a los usuarios del proxy para este cortafuegos. Los cortafuegos que utilicen este nombre administrarán el mismo conjunto de usuarios. Normalmente se utiliza el nombre de sistema principal totalmente calificado de la máquina del cortafuegos.
- El nombre del administrador del cortafuegos, utilizado para acceder a los usuarios del proxy que se almacenan en SecureWay Directory. A este nombre se le otorga acceso para modificar todos los usuarios del proxy creados en SecureWay Policy Director. Debería utilizarse el nombre de sistema principal totalmente calificado de la máquina del cortafuegos.
- El nombre distinguido que utiliza el IBM SecureWay Directory como raíz desde el que se empieza a buscar usuarios del cortafuegos en la base de datos. Debería ser el sufijo creado en SecureWay Directory para almacenar usuarios de Policy Director.
- Una contraseña para el ID del administrador del cortafuegos, que se empleará al conectarse con el servidor IBM SecureWay Directory.

Será necesario crear una conexión para permitir que el tráfico fluya entre el cortafuegos y el servidor SecureWay Directory.

Asegúrese de que cumple los requisitos previos listados en el apartado “Requisitos de hardware para SecureWay Boundary Server” en la página 15.

SurfinGate

Para prepararse para utilizar SurfinGate, debe tener instalado el Service Pack 5 de Windows NT. Asegúrese de que cumple los requisitos previos listados en el apartado “Requisitos de hardware para SecureWay Boundary Server” en la página 15.

Realice lo siguiente para prepararse para utilizar SurfinGate:

- Si utiliza una base de datos Oracle, debe estar configurada.

- Si utiliza el cortafuegos de Windows NT, es necesario decidir si se utilizará la modalidad de proxy o de complemento.
- Para habilitar el complemento SurfinGate en WTE, instale el complemento SurfinGate en la máquina del cortafuegos y ejecute el asistente de SecureWay Boundary Server.
- Será necesario crear una conexión para permitir que el tráfico fluya entre el complemento SurfinGate y el servidor SurfinGate.

MIMEsweeper

Para prepararse para utilizar MIMEsweeper, es preciso entender cómo funcionará la red. Asegúrese de que cumple los requisitos previos listados en el apartado “Requisitos de hardware para SecureWay Boundary Server” en la página 15.

MAILsweeper

Si configura MIMEsweeper, MAILsweeper y WEBsweeper deben estar en máquinas separadas.

Lleve a cabo las tareas siguientes antes de configurar MAILsweeper:

- Determine los dominios de correo que utiliza internamente. Debe configurarse MAILsweeper y el intercambiador de correo del cortafuegos para que acepten correo para cada uno de estos dominios de correo.
- Determine los servidores de correo seguro que dan soporte a cada uno de estos dominios. MAILsweeper debe estar configurado para reenviar el correo dirigido a uno de los dominios de correo al servidor de correo seguro correcto.
- Determine la dirección del servidor MAILsweeper. Cada servidor de correo seguro debe configurarse para que reenvíe el correo recibido de clientes internos al servidor MAILsweeper.
- Determine la dirección del cortafuegos. MAILsweeper debe configurarse para reenviar el correo dirigido a dominios externos al intercambiador de correo del cortafuegos.

WEBsweeper

Lleve a cabo las tareas siguientes antes de configurar WEBsweeper:

- Determine la dirección del servidor WEBsweeper. Esto será necesario en cada uno de los navegadores Web clientes de la red. Los navegadores deben configurarse para que utilicen el servidor WEBsweeper como sus proxys para HTTP, FTP y HTTPS.
- Determine la dirección de la interfaz segura del cortafuegos. WEBsweeper debe estar configurado para que reenvíe las peticiones de proxy al proxy HTTP que reside en el cortafuegos.
- Si no desea que los clientes puedan saltarse el filtrado de contenidos de la Web, deberá establecer una conexión en el cortafuegos que limite el acceso por proxy al servidor WEBsweeper y/o SurfinGate.

Capítulo 4. Requisitos para IBM SecureWay Boundary Server (SBS)

En este capítulo se describen los requisitos mínimos para SecureWay Boundary Server.

Requisitos de hardware para SecureWay Boundary Server

Los requisitos de hardware para los productos que componen Boundary Server se muestran en la tabla siguiente.

Tabla 2. Requisitos de hardware para productos componentes de Boundary Server

Componente de Boundary Server	Tipo de máquina	Espacio de disco	Memoria	Otros
Policy Director	N/A	64 MB	16 MB	N/A
IBM Firewall	• Windows NT: 266 MHz o superior • AIX: máquina RS/6000 que soporte 4.3.2	Windows NT: 200 MB AIX: 200 MB	Windows NT: 64 MB AIX: 128 MB	2 tarjetas de interfaz de red (NIC)
ACE/Server	• Windows NT: 166 MHz o superior (sólo de un procesador) • AIX: máquina que soporte AIX 4.2	• Software de servidor primario: 50 MB • Servidor de seguridad: 22MB • Base de datos de usuario inicial: 4MB • Instalación: 240 MB	Mínimo: 32 MB	Los requisitos reales de almacenamiento se basan en la cantidad de usuarios
MAILsweeper	Windows NT: procesador 400 MHz o superior	1 GB	128 MB	N/A
WEBsweeper	Windows NT: procesador 450 MHz o superior	1 GB	128 MB	N/A
Requisitos del sistema de WEBsweeper para un entorno de gran volumen	Windows NT: procesador 450 MHz o superior	3 GB	512 MB	N/A
Servidor SurfinGate 4.05	Windows NT: procesador 233 MHz o superior	20 MB	256 MB	N/A
Consola SurfinGate 4.05	Windows NT: procesador 233 MHz o superior	15 MB	64 MB	N/A

Nota: Para conocer más detalles, consulte la configuración e instalación para varios idiomas de la versión de IBM SecureWay Firewall para AIX o Windows NT. Además, se requieren 138 MB de espacio de disco para el navegador Netscape.

Requisitos de software para SecureWay Boundary Server

Los requisitos de software para los productos que componen Boundary Server se muestran en la tabla siguiente.

Tabla 3. Requisitos mínimos de software para productos componentes de Boundary Server

Producto	Windows	AIX	Otros
Servidores Policy Director	Windows NT versión 4.0 con Service Pack 5	4.3.1	N / A
IBM Firewall	Windows NT versión 4.0 con Service Pack 5	4.3.2	N / A
SecureWay Boundary Server	IBM SecureWay Firewall 4.1	IBM SecureWay Firewall 4.1	N / A
MAILsweeper	Windows NT versión 4.0 con Service Pack 5; Internet Explorer 4.01 o posterior; Microsoft Management Console 1.1; unidad NTFS; Windows Messaging	N / A	Las herramientas antivirus que se deseen
WEBsweeper	Windows NT versión 4.0 con Service Pack 5	N / A	Las herramientas antivirus que se deseen
Servidor SurfinGate	Windows NT versión 4.0 con Service Pack 5	N / A	N / A
Consola SurfinGate 4.05	Windows NT versión 4.0 con Service Pack 5 o Windows 95	N / A	N / A

Capítulo 5. Instalación y configuración de SecureWay Boundary Server

En este capítulo se explica cómo configurar e instalar SecureWay Boundary Server en Windows NT y AIX.

- "Instalación de los componentes de SecureWay Boundary Server"
- "Configuración de los componentes de SecureWay Boundary Server" en la página 19
- "Bloqueo de intrusiones" en la página 26

Instalación de los componentes de SecureWay Boundary Server

En esta sección encontrará ayuda para instalar IBM SecureWay Firewall, SurfinGate y MIMEsweeper para Windows NT y AIX.

Instalación de SecureWay Firewall

Para obtener más información acerca de una configuración básica de IBM SecureWay Firewall para Windows NT y AIX, consulte el apartado "Cómo prepararse" en la página 11. Se explica cómo definir una interfaz segura, cómo determinar la política de seguridad y cómo definir objetos de red. Para obtener más información acerca de la instalación de SecureWay Firewall, consulte los manuales *IBM SecureWay Firewall Installation Guide for AIX* e *IBM SecureWay Firewall Installation Guide for Windows NT*.

Instalación de SecureWay Directory

Si utiliza la característica LDAP de SecureWay Boundary Server, debe instalar SecureWay Directory; consulte el manual *IBM SecureWay Policy Director Up and Running 3.0*.

El servidor SecureWay Directory debe ubicarse en el lado seguro del cortafuegos, o dentro de la zona segura intermedia del cortafuegos (DMZ).

Instalación de SecureWay Policy Director

Si utiliza la característica LDAP de SecureWay Boundary Server, debe instalar SecureWay Policy Director (consulte el manual *IBM SecureWay Policy Director Up and Running 3.0*).

Instalación de SecureWay Boundary Server

Para instalar SecureWay Boundary Server en Windows NT, lleve a cabo lo siguiente:

- Instale SecureWay Firewall para Windows NT
- Desde el CD de SecureWay Boundary Server, ejecute setup.exe
- Elija el idioma y pulse **OK (Aceptar)**

- InstallShield le preguntará dónde desea instalar SecureWay Boundary Server. El directorio de Windows NT por omisión es C:\Archivos de programa\IBM\SBS
- Rearranque

Para instalar SecureWay Boundary Server en AIX, lleve a cabo lo siguiente:

- Instale SecureWay Firewall para AIX
- Inserte el CD y realice la instalación utilizando SMITTY
- Seleccione Software Installation and Maintenance (Instalación y mantenimiento de software)
- Seleccione Install and Update Software (Instalar y actualizar software)
- Seleccione Install and Update from Latest Available Software (Instalar y actualizar del software disponible más reciente)
- Cuando se le pregunte el dispositivo INPUT, liste las selecciones y elija la unidad de CD-ROM
- Liste las selecciones de SOFTWARE a instalar y elija sbs.
- Pulse **Intro** para instalar el software
- Rearranque

Instalación de SurfinGate

SurfinGate tiene dos componentes: el Servidor SurfinGate y la Consola SurfinGate. Para instalar los dos componentes de SurfinGate, consulte la guía de instalación, que se encuentra en `\docs\install.pdf`, en el CD de SurfinGate.

Complemento SurfinGate

Para instalar el complemento SurfinGate en IBM SecureWay Firewall para Windows NT, consulte la guía de instalación, que se encuentra en el directorio `\docs` del CD de SurfinGate.

Instalación de MIMEsweeper

MIMEsweeper tiene tres componentes: MAILsweeper, WEBsweeper y WEBsweeper HTTPS.

Debe instalarse MAILsweeper 4.1 en una partición NTFS.

Instalación de MAILsweeper

Para instalar MAILsweeper, consulte el documento *Getting Started Guide* ubicado en `\install\MSW4_0_2\docs\qsg.pdf`, en el CD de MIMEsweeper.

NO instale MAILsweeper en la misma máquina que el proxy de HTTP de WEBsweeper.

NO instale MAILsweeper en la misma máquina que el proxy HTTPS de WEBsweeper.

Si instala `MAPI32.dll` desde el CD de Windows NT y, a continuación, instala Microsoft Management Console 1.1 desde el CD de MIMEsweeper, la versión correcta de `MAPI32.dll` se sobregraba con una versión de nivel anterior instalada con Microsoft Management Console. Después de instalar Microsoft Management Console, asegúrese de instalar la versión 4.0 o posterior de `MAPI32.dll`. La `dll` se encuentra normalmente en el componente Windows Messaging.

Instalación de WEBsweeper

Para instalar WEBsweeper, consulte el documento *Administrator's Guide* ubicado en `\install\WSW3_2_5\docs\manual.pdf` del CD de MIMEsweeper.

NO instale WEBsweeper en la misma máquina que MAILsweeper.

Instalación de WEBsweeper HTTPS

Para instalar WEBsweeper HTTPS, consulte el documento *Readme* ubicado en `\install\WSWHTTPS1_0_2\readme.txt` del CD de MIMEsweeper.

NO instale el proxy HTTPS de WEBsweeper en la misma máquina que MAILsweeper.

Configuración de los componentes de SecureWay Boundary Server

Configuración de SecureWay Firewall

Para una instalación básica de IBM Firewall:

1. Planifique la instalación de IBM Firewall. Decida de antemano las funciones que desea utilizar del cortafuegos y el modo en que desea utilizarlas.
2. Indique al cortafuegos qué interfaces están conectadas a redes seguras. Para que el cortafuegos funcione correctamente, debe tener una interfaz segura y una interfaz no segura. En el árbol de navegación del cliente de la configuración, abra la carpeta System Administration (Administración del sistema) y pulse **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 **Change (Cambiar)**.
3. Configure su política de seguridad general accediendo al diálogo **Security Policy (Política de seguridad)** en la carpeta System Administration (Administración del sistema). Para configuraciones típicas de cortafuegos:
   - Permita consultas del DNS
   - Deniegue mensajes de difusión general a la interfaz no segura
   - Deniegue socks a los adaptadores que no sean seguros
4. Configure el servicio de nombre de dominio y el servicio de correo. No habrá comunicación eficiente si no proporciona una resolución del DNS. Acceda a estas funciones desde la carpeta System Administration (Administración del sistema) en el árbol de navegación del cliente de la configuración.
5. Defina los elementos clave de su red en el cortafuegos utilizando la función **Network Objects (Objetos de red)** en el árbol de navegación del cliente de la configuración. Los objetos de red controlan el tráfico a través del cortafuegos. Defina como objetos de red los elementos clave siguientes:
   - Interfaz segura del cortafuegos
   - Interfaz no segura del cortafuegos
   - Red segura
   - Cada subred de la red segura
   - Un objeto de red del sistema principal para los servidores Security Dynamics y para los servidores de dominio Windows NT, si procede
6. Habilite los servicios en el cortafuegos. Son métodos (por ejemplo, socks o el proxy) mediante los cuales los usuarios de la red segura pueden acceder a la red no segura. Los servicios que se implanten dependerán de las decisiones

que tome en la fase de planificación. La implantación de un servicio requiere a menudo configuraciones de conexión para permitir el paso de ciertos tipos de tráfico. Por ejemplo, si desea que los usuarios de red segura naveguen por la Web en Internet utilizando el proxy HTTP, no sólo necesitará configurar el daemon del proxy HTTP en el cortafuegos, sino que también deberá configurar conexiones para permitir el tráfico HTTP.

7. Configure los usuarios del cortafuegos. Si requiere autenticación para funciones tales como el acceso de salida a la Web o para administradores del cortafuegos, es necesario que defina dichos usuarios en el cortafuegos. Si tiene intención de utilizar SecureWay Policy Director para almacenar usuarios del proxy en LDAP, no cree usuarios de proxy en este momento. Utilice la consola de Policy Director para crear usuarios del proxy de cortafuegos durante la configuración de Policy Director.

Estos pasos deberían ayudarle a obtener una configuración básica de cortafuegos activa y en funcionamiento. IBM Firewall proporciona otras funciones, como registros cronológicos del sistema que le ayudan a garantizar la seguridad de la red.

Si el cortafuegos se cierra de manera normal o anormal, los datos de configuración no se ven afectados porque se guardan en la unidad del disco duro y se vuelven a activar automáticamente cuando se rearranca. Sin embargo, aparecerán algunos mensajes de anotación cronológica que indiquen que algunas conexiones activas, por ejemplo, una sesión FTP activa, se han interrumpido.

Configuración de SecureWay Firewall para la integración de Policy Director

El cortafuegos debe estar configurado para utilizar IBM SecureWay Policy Director con el asistente de SecureWay Boundary Server a fin de sacar partido de la integración con Policy Director. Si no se utiliza IBM SecureWay Policy Director, sólo la interfaz gráfica de usuario del cortafuegos (GUI) define a los usuarios del proxy. SecureWay Policy Director no puede gestionar a estos usuarios.

Se deberá crear una conexión para que SecureWay Firewall se comunique con SecureWay Directory. SecureWay Directory debe estar en un lado seguro del cortafuegos, ya sea la zona segura intermedia, ya sea la red segura.

Para obtener más información sobre cómo configurar conexiones, consulte los manuales *IBM SecureWay Firewall User's Guide for Windows NT* e *IBM SecureWay Firewall User's Guide for AIX*. Más adelante encontrará información para configurar la conexión.

Para la petición, los elementos siguientes serán necesarios para definir la regla de salida:

- El origen será la dirección del adaptador seguro del cortafuegos.
- El destino será la dirección de SecureWay Directory.
- El puerto de origen será mayor que 1023.
- El puerto de destino será igual a 389.
- La interfaz será segura.
- El direccionamiento será local.
- La dirección será de salida.

Para la respuesta, los elementos siguientes serán necesarios para definir la regla de entrada:

- El origen será la dirección de SecureWay Directory.
- El destino será la dirección del adaptador seguro del cortafuegos.
- El puerto de origen será igual a 389.
- El puerto de destino será mayor que 1023.
- La interfaz será segura.
- El direccionamiento será local.
- La dirección será de entrada.

A continuación se muestra un ejemplo de la conexión:

```
# Servicio : ldap
# Descripción :

permit 9.67.130.153 255.255.255.255 9.67.141.85
255.255.255.255 tcp gt 1023 eq 389 secure both
outbound l=y f=y t=0 e=none a=none

permit 9.67.141.85 255.255.255.255 9.67.130.153
255.255.255.255 tcp/ack eq 389 gt 1023 secure local
inbound l=y f=y t=0 e=none a=none
```

Ejecute el asistente de configuración de SecureWay Boundary Server. Seleccione la opción que habilita el cortafuegos para que funcione con Policy Director. Para más información, consulte el apartado “Configuración de SecureWay Boundary Server para la integración de Policy Director” en la página 23.

Configuración de SecureWay Firewall para que utilice el complemento SurfinGate (sólo para Windows NT)

Se deberá crear una conexión para que SecureWay Firewall se comunique con el servidor SurfinGate. El servidor SurfinGate debería estar en el lado seguro del cortafuegos.

Para obtener más información sobre cómo configurar conexiones, consulte el manual *IBM SecureWay Firewall User's Guide for Windows NT*. Más adelante encontrará información para configurar la conexión.

Para la petición, los elementos siguientes serán necesarios para definir la regla de salida:

- El origen será la dirección del adaptador seguro del cortafuegos.
- El destino será la dirección del servidor SurfinGate.
- El puerto de origen será mayor que 1023.
- El puerto de destino será igual a 3141.
- La interfaz será segura.
- El direccionamiento será local.
- La dirección será de salida.

Para la petición, los elementos siguientes serán necesarios para definir la regla de entrada:

- El origen será la dirección del servidor SurfinGate.
- El destino será la dirección del adaptador seguro del cortafuegos.
- El puerto de origen será igual a 3141.
- El puerto de destino será mayor que 1023.
- La interfaz será segura.

- El direccionamiento será local.
- La dirección será de entrada.

A continuación se muestra un ejemplo de una conexión de tales características:

```
# Servicio : comunicación con el complemento SurfinGate
# Descripción :

permit 9.67.143.113 255.255.255.255 9.67.143.115 255.255.255.255 tcp gt 1023 eq 3141
secure local outbound l=y f=y
permit 9.67.143.115 255.255.255.255 9.67.143.113 255.255.255.255 tcp eq 3141 gt 1023
secure local inbound  l=y f=y
```

Nota: Las conexiones deben estar en la misma línea.

Asimismo, necesitará configurar el servidor SurfinGate para que permita el paso a los datos que se explorarán. En SurfinConsole, (la interfaz de administración de SurfinGate) deberá marcar la opción **Plugin Mode (Modalidad de complemento)** bajo la pestaña General. Además, deberá entrar la dirección y el número de puerto del proxy HTTP del cortafuegos en el campo Next Proxy (Proxy siguiente) de la pestaña Proxy.

Configuración de SecureWay Firewall para que utilice MAILsweeper

El intercambiador de correo definido en SecureWay Firewall debe apuntar a la máquina de MAILsweeper en lugar del servidor real de correo seguro. MAILsweeper entregará el correo a los servidores de correo seguros.

Configuración de SecureWay Policy Director

Asegúrese de que se ha instalado SecureWay Directory. Debe conocer la dirección de la máquina donde está instalado SecureWay Directory, el puerto de comunicación, el ID de administrador del servidor de SecureWay Directory y su contraseña.

Instale el cliente LDAP de SecureWay Directory en la misma máquina que SecureWay Policy Director. (Puede que el cliente ya esté instalado si utiliza la misma máquina para SecureWay Directory y para SecureWay Policy Director.)

Debe modificar el esquema de LDAP de SecureWay Directory para dar soporte a usuarios del proxy (eProxyUsers) de Policy Director. Las adiciones en el esquema se almacenan en dos archivos proporcionados por Policy Director. Necesitará los archivos secschema.def y puschema.def, ubicados en el directorio /schema del CD de Policy Director.

Para modificar el esquema de LDAP en el servidor SecureWay Directory, ejecute los mandatos siguientes en la máquina de Policy Director:

```
ldapmodify -h
<SISPRINCLDAP> -p <PUERTOLDAP>  -D <IDADMINLDAP>  -w
<CONTRASEÑALDAP>  -f secschema.def

ldapmodify -h <SISPRINCLDAP> -p <PUERTOLDAP> -D
<IDADMINLDAP> -w <CONTRASEÑALDAP>  -f puschema.def
```

Donde:

- <SISPRINCLDAP> es el nombre del servidor SecureWay Directory
- <PUERTOLDAP> es el puerto de comunicación del servidor

- <IDADMINLDAP> es el ID del administrador
- <CONTRASEÑALDAP> es la contraseña del administrador

Una vez que haya modificado el esquema LDAP para dar soporte a usuarios del proxy, debe habilitar la manipulación de usuarios del proxy para la consola de Policy Director. Para realizar esto, debe quitar el signo de comentario de la línea Proxyusers TaskView en el archivo console.properties, ubicado en el directorio \Archivos de programa\IBM\IVConsole.

Configuración de SecureWay Directory

Debe definir un sufijo para SecureWay Directory que se utilizará como la raíz en la que se almacenarán los usuarios de Policy Director. Para añadir un sufijo a LDAP, consulte el manual *IBM SecureWay Directory Administrator's Guide*. Por ejemplo, un sufijo típico sería:

```
o=yourcompany,c=yourcountry
```

Una vez que haya añadido el sufijo para almacenar usuarios de Policy Director, debe definir su Lista de control de acceso (ACL) correctamente. Debe proporcionar todos los derechos de acceso al nuevo sufijo para el grupo de seguridad de Policy Director. El nombre distinguido (DN) del grupo de seguridad de Policy Director es:

```
cn=securitygroup,secauthority=default
```

Configuración de SecureWay Boundary Server para la integración de Policy Director

Puede configurar SecureWay Boundary Server mediante el asistente. Este asistente le guía por los pasos necesarios para configurar el cortafuegos para que funcione con otros productos de Boundary Server y Policy Director. Los paneles que siguen le hacen preguntas sobre su servidor LDAP. Una vez haya rellenado toda la información necesaria, el asistente configurará el cortafuegos para que utilice la misma base de datos LDAP que utiliza Policy Director para la política de grupos y usuarios. Este asistente también puede configurar y desconfigurar el proxy HTTP del cortafuegos para que pase información de autenticación al complemento SurfinGate (sólo en el cortafuegos de Windows NT).

Para configurar IBM SecureWay Boundary Server, ejecute el asistente de SecureWay Boundary Server. En AIX, ejecute el mandato **sbswizard** y, en Windows NT, seleccione **Inicio->Programas->SecureWay Boundary Server**. Esto hará que aparezca el asistente de SBS.

1. Seleccione la opción **Set up Firewall to share an LDAP database with Policy Director (Configurar el cortafuegos para compartir la base de datos LDAP con Policy Director)**.
2. Responda a las preguntas que aparecerán utilizando la información contenida en el apartado “SecureWay Boundary Server” en la página 13.

Configuración de SecureWay Boundary Server para habilitar el complemento SurfinGate (sólo para Windows NT)

Seleccione **Inicio->Programas->SecureWay Boundary Server**. Esto hará que aparezca el asistente de SBS.

1. Seleccione la opción **Configure the Firewall HTTP Proxy to pass authentication information to the SurfinGate plugin (Configurar el proxy**

HTTP del cortafuegos para que pase información de autenticación al complemento SurfinGate).

2. Complete el diálogo.

Configuración de SurfinGate

En Windows NT existen dos modos de configurar SurfinGate:

- Como un proxy en cadena
- Como un complemento del proxy HTTP del cortafuegos

En AIX hay un modo de configurar SurfinGate:

- Como un proxy en cadena

Configuración de SurfinGate como un proxy en cadena

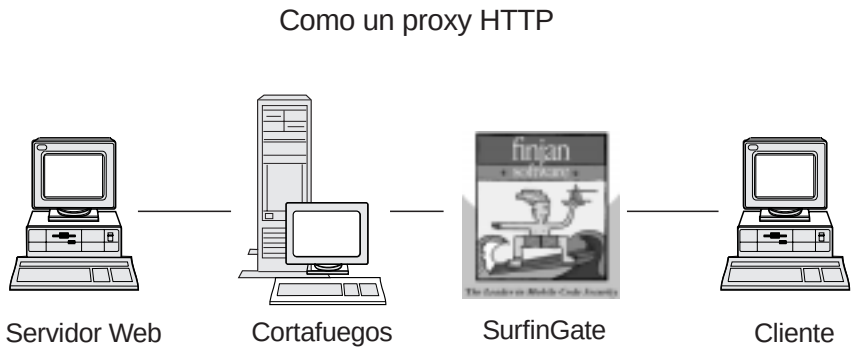

Figura 2. Configuraciones de SurfinGate

Los navegadores Web del cliente deben configurarse para que utilicen SurfinGate como el proxy para HTTP, FTP y HTTPS. Asegúrese de especificar el número de puerto de comunicación de SurfinGate (el valor por omisión es 8080).

En SurfinConsole (la interfaz de administración de SurfinGate) necesitará marcar la opción **Proxy Mode (Modalidad de proxy)** de la pestaña General. Además, debe entrar la dirección y el número de puerto del proxy HTTP del cortafuegos en el campo Next Proxy (Proxy siguiente) de la pestaña Proxy. De modo alternativo, si ya tiene definidos otros proxys, puede apuntar a ellos como el siguiente proxy.

Configuración de SurfinGate como complemento para el proxy HTTP del cortafuegos

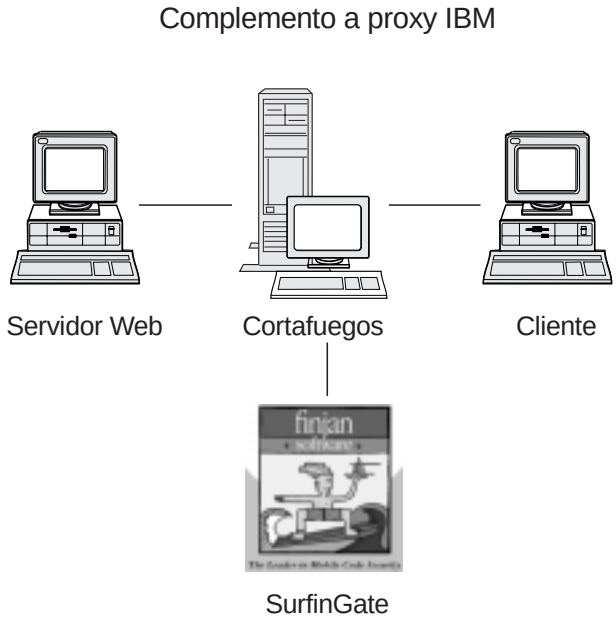

Figura 3. Configuraciones de SurfinGate

Los navegadores Web del cliente deben configurarse para que utilicen el proxy HTTP del cortafuegos como el proxy para HTTP, FTP y HTTPS. Especifique el número de puerto de comunicación del proxy HTTP del cortafuegos (el valor por omisión es 8080).

En SurfinConsole (la interfaz de administración de SurfinGate) necesitará marcar la opción **Plugin Mode (Modalidad de complemento)** de la pestaña General. Además, debe entrar la dirección y el número de puerto del proxy HTTP del cortafuegos en el campo Next Proxy (Proxy siguiente) de la pestaña Proxy.

Nota: Esta función sólo está disponible en SecureWay Firewall para Windows NT.

Configuración de MIMEsweeper

Configuración de MAILsweeper

Figura 4. Configuraciones de MAILsweeper

Si tiene un entorno sencillo, debe configurarse MAILsweeper respondiendo a las preguntas que aparecen durante la instalación. Para realizar una configuración adicional, lleve a cabo lo siguiente: **Inicio->Programas->MAILsweeper for SMTP->MAILsweeper for SMTP Console.** Para obtener más información consulte el manual *MAILsweeper Getting Started Guide.*

Configuración de WEBsweeper

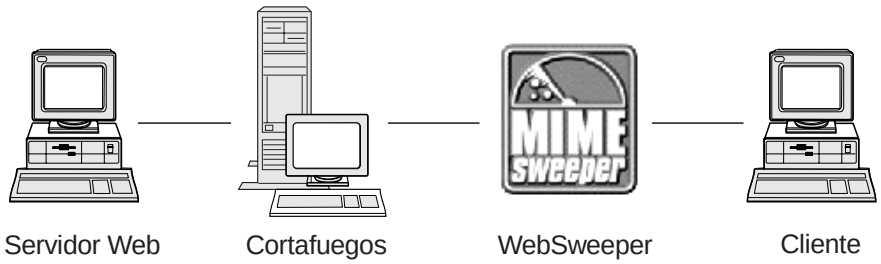

Figura 5. Configuraciones de WEBsweeper

Para realizar la configuración, vaya al Panel de control y seleccione el applet de WEBsweeper. Para obtener mas información, consulte el documento *WEBsweeper Administrator's Guide* del CD de MIMEsweeper.

Configuración de WEBsweeper HTTPS

Para realizar la configuración, vaya al Panel de control y seleccione el applet de WEBsweeper HTTPS. Para obtener más información, consulte el manual *WEBsweeper Administrator's Guide.*

Bloqueo de intrusiones

Utilice los programas de utilidad de la línea de mandatos para crear filtros que puedan bloquear direcciones IP específicas. Las direcciones a bloquear pueden determinarse de modo dinámico como resultado de la inspección de contenidos. Los mandatos son los siguientes:

- fwadd_deny
- fwdelete_dynamic

fwadd_deny

Si se invoca el programa sin parámetros, se solicitará el formato de los parámetros requeridos.

Los parámetros son los siguientes:

ID de filtro

Para el cortafuegos de Windows NT Firewall, se aplica lo siguiente: Se puede asignar un ID a los filtros a fin de organizar su mantenimiento. Los ID se asignan en orden ascendente, comenzando por 1. Si el ID proporcionado es mayor que el siguiente número de ID disponible, el ID asignado será el siguiente número de ID disponible y no el número de ID que se proporciona al programa. Por ejemplo, si hay unas reglas con el ID 1 y se intenta crear un conjunto de reglas de filtro con el ID 3, se le asignará el ID 2. Se puede asignar el mismo número de ID a varias reglas. Cuando las reglas se suprimen utilizando el programa delete_dynamic, se hace referencia a las mismas por su ID; por eso,

cuando cree reglas por ID, tenga previsto suprimirlas en grupo si comparten el mismo ID.

Al añadir una regla se visualiza el número de ID utilizado.

ID de filtro

Para el cortafuegos de AIX, se aplica lo que sigue: El ID se puede asignar por número. Por ejemplo, si decide que el ID del filtro es 12, se le asignará ID=12. En AIX no puede haber filtros asignados con el mismo número de ID. Cada filtro tendrá su ID propio y exclusivo.

Dirección IP de origen

La dirección IP que vaya a utilizarse para el origen de los paquetes debe entrarse en notación decimal y con puntos, por ejemplo 255.255.255.255.

Máscara IP de origen

Este campo se utiliza junto con la dirección IP de origen y se entra en notación decimal y con puntos. Por ejemplo, si la dirección IP de origen entrada es 10.5.8.0 y la máscara IP de origen es 255.255.255.0, coincidirán todos los paquetes de 10.5.8.1 a 10.5.8.255.

Dirección IP de destino

La dirección IP que vaya a utilizarse para el destino de los paquetes debe entrarse en notación decimal y con puntos, por ejemplo 255.255.255.255.

Máscara IP de destino

Este campo se utiliza junto con la dirección IP de destino y se entra en notación decimal y con puntos. Por ejemplo, si la dirección IP de destino entrada es 10.5.8.0 y la máscara IP de destino es 255.255.255.0, coincidirán todos los paquetes de 10.5.8.1 a 10.5.8.255.

Adaptador

La especificación de adaptador es la siguiente:

S adaptadores designados como seguros

N adaptadores designados como no seguros

B todos los adaptadores (tanto seguros como no seguros)

Los paquetes originados en el(los) adaptador(es) que pertenezcan al tipo especificado coincidirán con la regla.

Ámbito

El ámbito de un paquete que atraviesa el cortafuegos se especifica con este parámetro, que puede tener uno de los valores siguientes:

L paquetes locales

R paquetes direccionados

B paquetes locales y direccionados

Dirección

Especifica el tráfico de entrada, salida o en ambas direcciones.

I tráfico de entrada

O tráfico de salida

B tráfico de entrada y salida

Registro cronológico

Especifique Y para activar el registro cronológico y N para desactivarlo para la actividad de filtro dinámico.

fwdelete_dynamic

Si se invoca este programa sin parámetros, se listan todos los filtros dinámicos definidos actualmente.

```
>>>>  Dynamic Rule Id           =  1
 >>>>>>>>  Jump                 =  0
 >>>>>>>>  Filter Action        =  Deny
 >>>>>>>>  Source Address       =  9.192.8.7
 >>>>>>>>  Source Mask          =  255.255.255.0
 >>>>>>>>  Destination Address  =  9.192.240.1
 >>>>>>>>  Destination Mask     =  255.255.255.0
 >>>>>>>>  Protocol             =  Any
 >>>>>>>>  Source Port          =  Any 0
 >>>>>>>>  Destination Port     =  Any 0
 >>>>>>>>  Adapter              =  Both (Secure and NonSecure)
 >>>>>>>>  Scope                =  Both (Routed and Local)
 >>>>>>>>  Direction            =  Both (Inbound and Outbound)
 >>>>>>>>  Tunnel Id            =  0
 >>>>>>>>  Logging Enabled      =  Unavailable
 >>>>>>>>  Fragments Allowed    =  No
```

Nota: El mandato `fwdelete_dynamic` debe utilizarse para comprobar en primer lugar que las reglas a suprimir tienen el ID esperado.

Cuando se invoca el programa con un ID de filtro válido, se suprimen las reglas dinámicas y el número de reglas suprimidas se visualizan del modo x Reglas encontradas con ID: x.

AVISO: **Si intenta añadir un filtro duplicado, se le notificará que dicho filtro ya existe. Si intenta añadir un filtro sin un ID de filtro, recibirá un error de aviso.**

El bloqueo de intrusiones de AIX se puede alterar temporalmente si existen reglas en el conjunto de reglas del nivel superior. Si se utiliza el bloqueo de intrusiones, la mayoría de las reglas deben estar en el conjunto de reglas del nivel inferior. Las reglas dinámicas se añaden en medio de estos dos conjuntos de reglas. Si hay una regla en el nivel superior que permite el tráfico, no será posible desactivar el tráfico con las reglas dinámicas.

Comprobación de la configuración

Una vez haya realizado toda la instalación descrita en los capítulos anteriores, es necesario comprobarla. Para comprobar la configuración de SecureWay Boundary Server, realice lo que sigue:

1. Configure un usuario del proxy del cortafuegos utilizando Policy Director. Defina al usuario para que utilice la contraseña del cortafuegos para telnet seguro y defina la contraseña para el usuario.
2. Ejecute el asistente de SecureWay Boundary Server para establecer el enlace entre el cortafuegos y SecureWay Directory (LDAP).
3. Desde un cliente seguro, inicie una sesión telnet de proxy.
4. Entre la configuración del usuario en Policy Director.
5. Se le solicitará una contraseña.
6. Ahora está autenticado.

Capítulo 6. Documentación relacionada

Puede utilizar la documentación listada en este capítulo para encontrar más información acerca de IBM SecureWay Boundary Server Versión 2.0 y productos relacionados.

IBM SecureWay FirstSecure

El manual *IBM SecureWay FirstSecure Planificación e integración, Versión 2.0* contiene información acerca de FirstSecure. Este manual describe FirstSecure y los productos que lo componen, y ayuda a comenzar la planificación para utilizar todos los productos IBM SecureWay.

IBM SecureWay Firewall

Los documentos siguientes contienen información acerca de IBM SecureWay Firewall para Windows NT y están disponibles en los formatos PDF y HTM en el directorio `x:\books\en_US` del CD de IBM SecureWay Firewall:

- *IBM SecureWay Firewall for Windows NT Setup and Installation*
- *IBM SecureWay Firewall for Windows NT User's Guide*
- *IBM SecureWay Firewall for Windows NT Reference*
- *Guarding the Gates Using the IBM eNetwork Firewall for Windows NT 3.3* (un libro rojo)

Los documentos siguientes contienen información acerca de IBM SecureWay Firewall para AIX y están disponibles en los formatos PDF y HTM en el directorio `books/en_US` del CD de IBM SecureWay Firewall:

- *IBM SecureWay Firewall for AIX Setup and Installation*
- *IBM SecureWay Firewall for AIX User's Guide*
- *IBM SecureWay Firewall for AIX Reference*
- *A Comprehensive Guide to Virtual Private Networks, Volume 1: IBM Firewall, Servers and Client Solutions* (un libro rojo)

MIMEsweeper

MAILsweeper

Los documentos siguientes contienen información acerca de MAILsweeper y están disponibles en los formatos PDF y HTM en el directorio \install del CD de MIMEsweeper:

- *Getting Started Guide* se encuentra en \install\MSW4_0_2\Doc\qsg.pdf
- El archivo Léame (Readme) se encuentra en \install\MSW4_0_2\README.htm

WEBsweeper

Los documentos siguientes contienen información acerca de WEBsweeper y están disponibles en los formatos PDF y HTM en el directorio \install del CD de MIMEsweeper:

- *WEBsweeper Administrator's Guide* se encuentra en \install\WSW3_2_5\Doc\manual.pdf
- La nota del release se encuentra en \install\WSW3_2_5\Doc\RELNOTES.htm

Proxy HTTPS de WEBsweeper

El documento siguiente contiene información acerca del proxy HTTPS de WEBsweeper y está disponible en formato TXT en el directorio \install del CD de MIMEsweeper:

- El archivo Léame (Readme) se encuentra en \install\WSWHTTPS1_0_2\readme.txt

SurfinGate

Los documentos siguientes contienen información acerca de SurfinGate y están disponibles en formato PDF en el directorio \docs del CD de SurfinGate:

- *SurfinGate Installation Guide* se encuentra en \Docs\install.pdf
- *SurfinGate User's Manual* se encuentra en \Docs\manual.pdf
- La nota del release se encuentra en \Docs\SFG 405 RelNotes.pdf.htm
- La información acerca del complemento SurfinGate se encuentra en el directorio \docs.

Apéndice A. Resolución de problemas

Este capítulo le ayudará a detectar y resolver problemas relacionados con SecureWay Boundary Server.

Resolución de problemas comunes de IBM SecureWay Firewall

Problemas de direccionamiento

IBM Firewall proporciona una función en el recuadro de diálogo **Security Policy (Política de seguridad)** llamada *Test IP Routing (Comprobación del direccionamiento IP)*, que puede ser de utilidad a la hora de depurar problemas de direccionamiento. Habilite este recuadro de selección, active su configuración de conexión y habilite el registro cronológico de reglas de conexión. A continuación examine el `firewall log (archivo de anotaciones cronológicas del cortafuegos)` para visualizar información detallada sobre todos los paquetes que fluyen a través del cortafuegos.

Realice estas comprobaciones utilizando primero direcciones IP y, a continuación, utilizando nombres de sistemas principales.

No se puede realizar ping hacia sistemas principales desde el cortafuegos

Explicación del problema
La interfaz de red no está configurada correctamente.

Acción recomendada
Consulte la documentación de su sistema operativo.

Explicación del problema
La conexión a una red no segura no está configurada correctamente.

Acción recomendada
Póngase en contacto con su suministrador de servicio de Internet para obtener ayuda.

Explicación del problema
Si la red segura está aislada detrás de un direccionador, el cortafuegos debe tener una ruta estática a dicho direccionador. Utilice `netstat -rn` para comprobar el direccionamiento estático:

```
netstat -rn
```

La salida debería ser la siguiente para Protocol Family 2:

```
Destination  Gateway          Flags     ....
default      nrr.nrr.nrr.nrr  UG
nnn.nnn.nnn  nnn.nnn.nnn.nnn  U
sss.sss.sss  sss.sss.sss.sss  U
ss1.ss1.ss1  srr.srr.srr.srr  UG
127          127.0.0.1        U
```

Figura 6. Salida de ejemplo de netstat -rn.

nrr.nrr.nrr.nrr
representa el direccionador para Internet y es la ruta por omisión. La ruta por omisión es una ruta estática (Flag=UG).

nnn.nnn.nnn
representa el dominio no seguro. Es una ruta de interfaz (Flag=U).

nnn.nnn.nnn.nnn
representa la interfaz no segura.

sss.sss.sss
representa el dominio seguro. Es una ruta de interfaz (Flag=U).

sss.sss.sss.sss
representa la interfaz segura.

ss1.ss1.ss1
representa un subdominio del lado seguro de la red, y srr.srr.srr.srr representa el direccionador para ese subdominio. Es una ruta estática (Flag=UG).

127.0.0.1
es el bucle de retorno o el sistema principal local. Es una ruta de interfaz (Flag=U).

Debería tener una ruta de interfaz para cada interfaz y la ruta por omisión debería apuntar al direccionador del lado no seguro del cortafuegos.

Acción recomendada
Añada una ruta estática a su direccionador. Póngase en contacto con el administrador del direccionador. Utilice el mandato `route add`.

Explicación del problema
Puede ser que la máscara de subred de la interfaz segura o el sistema principal que intenta contactar sean incorrectos.

Acción recomendada
Utilice los progamas de utilidad de la configuración del cliente para corregir los valores de máscara.

No se puede realizar ping a sistemas principales no seguros desde sistemas principales seguros (or viceversa)

Explicación del problema
Cada direccionador adyacente al cortafuegos debe contener una ruta estática que especifique el cortafuegos como la pasarela para redes de destino del otro lado del cortafuegos.

Acción recomendada
Póngase en contacto con el administrador del direccionador.

Explicación del problema
Si su red segura utiliza direcciones no registradas y direccionables en la red no segura, incluidas direcciones privadas, tal como se especifica en RFC 1597, los paquetes no se direccionarán de vuelta al remitente.

Acción recomendada
Sólo para Windows NT: utilice un cliente con una dirección registrada. Puede utilizarse la característica NAT del cortafuegos para tráfico TCP y UDP, pero NAT no convertirá las direcciones en paquetes ICMP como ping.

Acción recomendada
Sólo para AIX: utilice un cliente con una dirección registrada.

Anomalías en el DNS

Nota: El DNS es sólo para Windows NT.

Explicación del problema

Ha recibido mensajes de error del DNS porque ha configurado Microsoft DNS Service con Microsoft DNS Service Manager.

Acción recomendada

Consulte las instrucciones de instalación y

1. Elimine Microsoft DNS suprimiendo todo el directorio: `\winnt\system32\DNS`
2. Vuelva a instalar Microsoft DNS
3. Rearranque
4. Vuelva a instalar el arreglo (hotfix) del DNS
5. Rearranque

Resolución de problemas comunes–MIMEsweeper

WEBsweeper y MAILsweeper no parecen funcionar en la misma máquina

Explicación del problema

Hay problemas al intentar ejecutar MAILsweeper y WEBsweeper en la misma máquina.

Acción recomendada

Instale MAILsweeper en una máquina y WEBsweeper en otra.

El rendimiento de WEBsweeper es lento

Explicación del problema

Se producen retardos no satisfactorios al bajar contenidos de la Web al utilizar WEBsweeper.

Acción recomendada

1. Inhabilite el registro cronológico utilizando el applet de WEBsweeper del Panel de control.
2. Instale WEBsweeper en el hardware más rápido que pueda permitirse.

Problemas de licencia con WEBsweeper

Explicación del problema

Si se instala WEBsweeper 3.2_5 en una máquina que tenía instalada una versión previa de WEBsweeper, puede producirse un conflicto de claves de licencia. Si al iniciar WEBsweeper aparece un mensaje de error interno de Windows 2140, compruebe el registro de la aplicación en el visor de sucesos. El mensaje de WEBsweeper es el siguiente: "Error de PAKMSG: el nombre de usuario entra en conflicto con la sección de licencia definida anteriormente."

Acción recomendada

Elimine la clave de licencia antigua del registro de Windows. Cargue regedit y busque en la vía de acceso \\HKEY_LOCAL_MACHINE\SOFTWARE\Content Technologies\MIMEsweeper\License. Si hay más de una clave, suprima la que no tiene la etiqueta "IBM MIMEsweeper System". Rearranque el sistema.

WEBsweeper presenta problemas al bajar archivos de gran tamaño

Explicación del problema

Puede ser que WEBsweeper no tenga más memoria virtual para almacenar archivos mientras realiza el filtrado.

Acción recomendada

Aumente la cantidad de memoria física en el servidor WEBsweeper.

Resolución de problemas comunes—SurfinGate

SurfinConsole deja de responder cuando Microsoft Internet Explorer está abierto

Explicación del problema

La aplicación SurfinConsole presenta un comportamiento extraño o deja de responder cuando Internet Explorer está abierto. Estas dos aplicaciones entran en conflicto y no se pueden ejecutar el mismo tiempo.

Acción recomendada

No cargue Internet Explorer y SurfinConsole al mismo tiempo.

El rendimiento del complemento SurfinGate es lento

Explicación del problema

La bajada de código móvil a través de la Web es muy lenta al utilizar el complemento SurfinGate.

Acción recomendada

Asegúrese de que el campo Next Proxy (Proxy siguiente) está definido en el proxy HTTP de SecureWay Firewall en la sección de proxys de SurfinConsole.

Apéndice B. Avisos

Las referencias que se hacen en esta publicación a productos, programas o servicios de IBM no implican que IBM tenga la intención de comercializarlos en todos los países en los que IBM realiza operaciones. Las referencias a programas, productos o servicios de IBM no pretenden establecer o implicar que sólo puedan utilizarse los productos, programas o servicios de IBM. En su lugar se puede utilizar cualquier producto, programa o servicio funcionalmente equivalente que no vulnere los derechos legales de propiedad intelectual u otros derechos legalmente protegidos de IBM. La evaluación y verificación del funcionamiento junto con otros productos, excepto los expresamente designados por IBM, es responsabilidad del usuario.

IBM puede tener patentes o solicitudes de patente pendientes que afecten a los temas tratados en este documento. La entrega de este documento no otorga ninguna licencia sobre dichas patentes. Puede enviar consultas de licencias, por escrito, a IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, NY 10504–1785, Estados Unidos.

Los usuarios con licencia de este programa que deseen información acerca del mismo para poder: (i) intercambiar la información entre programas creados de forma independiente y otros programas (incluido éste) y (ii) utilizar, de forma mutua, la información intercambiada, deben ponerse en contacto con:

Site Counsel, IBM SWG
IBM Corporation
P.O. Box 12195
3039 Cornwallis
Research Triangle Park, NC 27709-2195
Estados Unidos

NO se otorga licencia de este programa bajo los términos del IBM Customer Agreement (ICA). Se otorga licencia bajo los términos del "IBM International Program License Agreement" (IPLA).

Este documento no está ideado para un uso de producción y se proporciona tal cual sin garantías de ningún tipo, y se rechazan todas las garantías, incluidas las garantías de comerciabilidad e idoneidad para un propósito concreto.

Este producto incluye software de sistema creado y puesto a disposición por el CERN. Este reconocimiento se mencionará por completo en cualquier producto que contenga software de sistema del CERN o bien partes del mismo.

Marcas registradas

Los términos siguientes son marcas registradas de IBM Corporation en los Estados Unidos y/o en otros países:

AIX

IBM

Microsoft y Windows NT son marcas registradas de Microsoft Corporation.

**SurfinGate es una marca registrada de Finjan Software, Ltd.

**MIMEsweeper, **MAILsweeper y **WEBsweeper son marcas registradas de Content Technologies, Ltd.

Otros nombres de empresas, productos y servicios, que pueden estar marcados con dos asteriscos (**), pueden ser marcas registradas o de servicio de otras compañías.

Glosario

A

asistente. Diálogo dentro de una aplicación que utiliza instrucciones paso a paso para guiar al usuario durante una tarea específica.

C

cliente. Sistema o proceso informático que solicita el servicio de otro proceso o sistema informático, al que se hace referencia habitualmente como servidor. Varios clientes pueden compartir el acceso a un servidor común.

cortafuegos. Unidad funcional que protege y controla la conexión de una red a otras redes. El cortafuegos evita que el tráfico de comunicaciones no deseado o no autorizado entre en la red protegida, y permite que solamente el tráfico de comunicaciones seleccionado salga de la red protegida.

D

dirección de servidor. Código exclusivo asignado a cada sistema que proporciona servicios compartidos a otros sistemas de una red; por ejemplo, un servidor de archivos, un servidor de impresión o un servidor de correo. Una dirección IP estándar es un campo de dirección de 32 bits. La dirección de servidor puede ser la dirección IP decimal y con puntos o bien el nombre del sistema principal.

dirección IP. Dirección de protocolo de Internet. Dirección exclusiva de 32 bits que especifica la ubicación real de cada dispositivo o estación de trabajo de una red. También se conoce como dirección de Internet.

DMZ. Zona intermedia. Dispositivo que evita que los usuarios externos obtengan acceso directo a un servidor que contiene datos de la empresa.

F

FTP (protocolo de transferencia de archivos). Protocolo de aplicación utilizado para transferir archivos entre sistemas de una red. El FTP requiere un ID de usuario y, a veces, una contraseña para permitir el acceso a archivos de un sistema principal remoto.

I

ICMP. Protocolo de mensajes de control de Internet. Protocolo utilizado para manejar mensajes de control y errores en la capa del protocolo de Internet (IP). Se devuelven informes de problemas y destinos de datagrama incorrectos a la fuente original del datagrama.

interfaz de bucle de retorno. Interfaz que pasa por alto funciones de comunicación innecesarias cuando la información va dirigida a una entidad del mismo sistema.

Internet. Colección de redes interconectadas a nivel mundial que utiliza el conjunto de protocolos de Internet y que permite acceso público.

intranet. Red privada y segura que integra los estándares y aplicaciones de Internet (como los navegadores Web) a la infraestructura informática existente de la organización.

IP. Protocolo de Internet. Protocolo sin conexión que direcciona datos a través de una red o redes interconectadas. El IP actúa de intermediario entre las capas de protocolo superiores y la capa física.

IPSEC. Seguridad del protocolo de Internet. Un estándar en desarrollo para la seguridad en la capa de proceso de red o de paquetes de las comunicaciones de red.

N

NAT. Conversión de direcciones de red. En un cortafuegos, conversión de direcciones IP seguras en direcciones externas registradas. Esto permite la comunicación con redes externas, pero crea máscaras de las direcciones IP que se utilizan dentro del cortafuegos.

P

pasarela. Unidad funcional que conecta dos redes con arquitecturas distintas.

PICS. Plataforma para la selección de contenidos de Internet. Los clientes habilitados para PICS permiten que los usuarios determinen la calificación de los servicios que desean usar y, para cada servicio de calificación, que establezcan las calificaciones aceptables y las inaceptables.

ping. Mandato que envía a un sistema principal, una pasarela o un direccionador paquetes de protocolo de mensajes de control de Internet (ICMP) con solicitudes de retorno, de las que se espera recibir una respuesta.

por omisión. Valor, atributo u opción que se da por supuesto cuando no se especifica ninguno de forma explícita.

protocolo. Conjunto de reglas que rigen el funcionamiento de unidades funcionales en un sistema de comunicaciones, si debe tener lugar la comunicación. Los protocolos pueden determinar detalles de bajo nivel de interfaces entre máquinas, como el orden en el que se envían los bits de un byte; también pueden determinar intercambios de alto nivel entre programas de aplicación, como la transferencia de archivos.

puerto. Número que identifica un dispositivo de comunicaciones abstracto. Los servidores Web utilizan el puerto 80 por omisión.

S

servicio. Función proporcionada por uno o más nodos; por ejemplo, HTTP, FTP, Telnet.

servidor. Sistema que proporciona servicios compartidos a otros sistemas de una red; por ejemplo, un servidor de archivos, un servidor de impresión o un servidor de correo.

shell. Software que acepta y procesa líneas de mandato de una estación de trabajo de un usuario. El shell de Korn es uno de los varios shells disponibles en UNIX.

SMTP. Protocolo de transferencia de correo sencillo. En el conjunto de protocolos de Internet, un protocolo de aplicación que sirve para transferir correo entre usuarios del entorno de Internet. El SMTP especifica las secuencias de intercambio de correo y el formato de los mensajes. Da por supuesto que el protocolo de control de transmisiones (TCP) es el protocolo subyacente.

T

TCP. Protocolo de control de transmisiones. Un protocolo de comunicaciones utilizado en Internet. El TCP proporciona el intercambio fiable de información entre sistemas principales. Utiliza el IP como protocolo subyacente.

TCP/IP. Protocolo de control de transmisiones/protocolo de Internet. Un conjunto de protocolos ideados para permitir la comunicación entre redes, independientemente de la tecnología en comunicaciones utilizada en cada red.

Telnet. Protocolo de emulación de terminal, un protocolo de aplicación TCP/IP para el servicio de conexión remota. Telnet permite al usuario de un sitio obtener acceso a un sistema principal remoto como si la estación de trabajo del usuario estuviera directamente conectada a dicho sistema principal remoto.

tiempo de espera. Intervalo de tiempo asignado para que se realice una operación.

U

UDP. Protocolo de datagrama de usuario. En el conjunto de protocolos de Internet, protocolo que proporciona un servicio de datagramas no fiable y sin conexión. Habilita un programa de aplicación en una máquina o proceso para que envíe un datagrama a un programa de aplicación de otra máquina o proceso. El UDP utiliza el protocolo de Internet (IP) para entregar los datagramas.

V

VPN. Red privada virtual (VPN). Red formada por uno o más túneles IP seguros que conectan dos o más redes.

W

Web. Red de servidores HTTP que contienen programas y archivos, muchos de los cuales son documentos de hipertexto que enlazan con otros documentos en servidores HTTP. También se le denomina World Wide Web.

WTE. Web Traffic Express (WTE). Servidor de proxy de almacenamiento en antememoria que puede contribuir a acelerar el tiempo de respuesta del usuario final mediante planes de almacenamiento en antememoria altamente eficientes. El filtrado PICS flexible ayuda a los administradores de red a controlar el acceso a la información basada en Web de una ubicación central.

Hoja de Comentarios

IBM SecureWay® Boundary Server para Windows NT® y AIX
Puesta a punto
Versión 2.0

Número de Publicación GC10-3502-00

Por favor, sírvase facilitarnos su opinión sobre esta publicación (utilidad, facilidad de lectura, ...), sugiriendo posibles adiciones y supresiones, y liste los errores y omisiones específicos (indicando número de página). Todos los comentarios y sugerencias pasarán a ser propiedad de IBM, sin incurrir por ello en ninguna obligación para con el remitente.

Sus comentarios nos ayudarán a mejorar las futuras ediciones de esta publicación. Cada una de las observaciones que se reciban será detenidamente revisada por las personas responsables de la redacción, traducción y/o revisión de este material. Sírvase anotar sus comentarios en esta hoja y remitirla a la dirección que figura preimpresa al dorso.

Nombre

Dirección

Compañía u Organización

Teléfono

Hoja de Comentarios
GC10-3502-00

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
AQUI

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

GC10-3502-00

Corte o Doble
Por la Línea

Número Pieza: CT6RZES

Printed in the United States of America
on recycled paper containing 10%
recovered post-consumer fiber.

GC10-3502-00