IBM® SecureWay® FirstSecure

Planificación e integración

Versión 2

IBM® SecureWay® FirstSecure

Planificación e integración

Versión 2

Nota

Antes de utilizar esta información y el producto al que da soporte, lea detenidamente la información general incluida en el Apéndice A, “Avisos” en la página 101.

Primera edición (Octubre 1999)

Este manual es la traducción de la publicación original en inglés IBM SecureWay FirstSecure - Planning and Integration. Esta edición es aplicable a la versión 2 de IBM SecureWay FirstSecure y a todos los releases y modificaciones siguientes hasta que se indique lo contrario en nuevas ediciones.

Contenido

Figuras

Tablas

Acerca de este manual

IBM® SecureWay® FirstSecure, conocido también como FirstSecure, es una infraestructura completa que ayuda a la empresa a:

- Proteger todos los aspectos relacionados con interconexión de redes a través de la Web y de otras redes.
- Aprovechar las inversiones en e-business actuales, mediante ofertas modulares que le permiten añadir seguridad según un despliegue planificado.
- Reducir el coste total de propiedad para realizar e-business de forma segura.

Este manual describe FirstSecure, los productos que componen FirstSecure, y le ayuda a iniciar la planificación del uso de estos productos.

Los productos que se describen en este manual forman parte de un release por etapas. Es posible que no todos los productos estén disponibles al mismo tiempo en todos los países. Consulte a su representante de ventas de IBM acerca de la disponibilidad de cualquiera de estos productos.

Las figuras de este manual

Las figuras de este manual son únicamente para fines de planificación. Cada figura ilustra únicamente una de las innumerables disposiciones de servidores, clientes y aplicaciones que pueden resultar adecuadas para su empresa.

El formato de las figuras que vea dependerá del mecanismo utilizado para visualizar el manual:

- La mayor parte de las figuras de la versión en formato PDF (Portable Document Format) que aparecen en el manual son más sencillas para ahorrar espacio de disco y para facilitar su impresión.
- Las figuras de la versión impresa son más complejas, ocupan más espacio de almacenamiento y tardan más tiempo en imprimirse.

Las figuras de ambas versiones son funcionalmente equivalentes y tienen títulos idénticos y texto alternativo.

A quién va dirigido este manual

Este manual va dirigido a los administradores de sistemas que planifican e integran la seguridad en los sistemas basados en la Web. Debe poseer conocimientos sobre la red y las aplicaciones de e-business.

Cómo está organizado este manual

Este manual contiene las siguientes partes:

- En la Parte 1, “Visión general de FirstSecure” en la página 1 se proporciona una visión general de FirstSecure, sus productos componentes y las ofertas disponibles.
- En la Parte 2, “Planificación de una red de e-business segura” en la página 17 se describen las tareas de planificación de una red de e-business segura.
- En la Parte 3, “Consideraciones sobre la instalación y la integración” en la página 55 se describen los requisitos de instalación y detalles sobre la integración de los productos FirstSecure.
- El Capítulo 16, “Documentación que se proporciona con FirstSecure” en la página 89 describe toda la documentación disponible con FirstSecure.
- El “Glosario” en la página 105 define los términos relacionados con la seguridad que se utilizan en este manual.

El manual también incluye una bibliografía que describe la documentación de cada uno de los productos.

Efecto 2000

A continuación se describe cómo está preparado IBM SecureWay FirstSecure para el efecto 2000.

Productos IBM en IBM SecureWay FirstSecure

Estos productos están preparados para el efecto 2000. Cuando se utilizan según la documentación asociada, pueden procesar, proporcionar y/o recibir correctamente datos de fecha del siglo XX y de fechas comprendidas entre el siglo XX y el siglo XXI, siempre y cuando todos los productos (hardware, software y firmware) que se utilicen con estos productos puedan intercambiar correctamente datos precisos de fechas.

Productos de otros proveedores

Otros productos han declarado a IBM que están preparados para el efecto 2000. Sin embargo, IBM no declara ni ofrece ninguna garantía al respecto de que estos productos estén preparados para el efecto 2000. Póngase en contacto con el fabricante para cualquier consulta relacionada con el efecto 2000 en estos productos. La información relacionada con productos y servicios que no son de IBM son "Reediciones", según el decreto Information and Readiness Disclosure Act, basadas en la información suministrada por otras empresas acerca de los productos y servicios que ofrecen. Estas empresas han declarado a IBM que los productos están preparados para el efecto 2000. Sin embargo, IBM no declara ni ofrece ninguna garantía en cuanto a que estos productos estén preparados para el efecto 2000. Póngase en contacto con el fabricante para cualquier consulta relacionada con el efecto 2000 en estos productos. IBM no ha realizado ninguna comprobación independiente de estas reediciones y no acepta responsabilidad alguna con respecto a que la información contenida en dichas reediciones sea completa y precisa.

Servicio y soporte

Póngase en contacto con IBM para obtener servicio técnico y soporte para todos los productos incluidos en la oferta SecureWay FirstSecure. Algunos de estos productos hacen referencia a soporte que no es de IBM. Si obtiene estos productos como parte de la oferta SecureWay FirstSecure, póngase en contacto con IBM para obtener servicio técnico y soporte.

Convenios

Este manual utiliza los siguientes convenios tipográficos:

- **El texto en negrita** indica el nombre de un elemento que el usuario selecciona, el nombre de un mandato, el texto que escribe el usuario o un ejemplo dentro del cuerpo de texto.
- `El texto en Monoespaciado` indica un ejemplo (como una vía de acceso o un nombre de archivo ficticio) o texto que se muestra en la pantalla.

Información en la Web

La información sobre las actualizaciones de última hora de FirstSecure se puede encontrar en Internet en www.ibm.com/software/security, en las direcciones siguientes:

IBM SecureWay FirstSecure www.ibm.com/software/security/firstsecure

La documentación está disponible en www.ibm.com/software/security/firstsecure/library

IBM SecureWay Policy Director www.ibm.com/software/security/policy

La documentación está disponible en www.ibm.com/software/security/policy/library

IBM SecureWay Boundary Server www.ibm.com/software/boundary

La documentación está disponible en www.ibm.com/software/boundary/library

IBM SecureWay Trust Authority www.ibm.com/software/security/trust

La documentación está disponible en www.ibm.com/software/securitytrust/library

Un libro rojo de la ITSO, *Understanding the IBM SecureWay FirstSecure Framework*, SG24–5498–00 está disponible en Internet en www.ibm.com/redbooks.

Parte 1. Visión general de FirstSecure

Esta parte es una visión general de FirstSecure y de los productos componentes. Contiene una breve descripción de cada producto.

Esta parte describe también IBM Implementation Services.

Capítulo 1. ¿Qué es FirstSecure?

IBM SecureWay FirstSecure forma parte de las soluciones de seguridad integradas de IBM. FirstSecure es un amplio conjunto de componentes esenciales que ayudarán a su empresa a:

- Establecer un entorno e-business seguro.
- Reducir el coste total de la propiedad de la seguridad simplificando las tareas de planificación de la seguridad.
- Implantar políticas de seguridad más fácilmente.
- Crear un entorno e-business más eficaz.

Los componentes de FirstSecure incluyen protección antivirus, detección de intrusismos, control de acceso, control del contenido del tráfico, cifrado, certificados digitales, tecnología de cortafuegos y kits de desarrollo de aplicaciones. Estas funciones las proporciona la familia de productos de seguridad de IBM SecureWay, junto con ofertas de otros proveedores, combinando los mejores componentes de diferentes proveedores de seguridad. Además, se proporcionan los Implementation Services para componentes de FirstSecure seleccionados. Los componentes esenciales de FirstSecure son:

- SecureWay Policy Director
- SecureWay Boundary Server
- Intrusion Immunity
- Public Key Infrastructure, disponible a través de IBM SecureWay Trust Authority
- IBM SecureWay Toolbox

Dado que FirstSecure es un conjunto de productos que se pueden instalar independientemente, podrá planificar las tareas para obtener un entorno seguro. Puede comenzar por un área, comprobar las mejoras y, a continuación, continuar progresando para obtener una mayor seguridad. Esto disminuye la complejidad y el coste, y facilita el empleo de las aplicaciones y recursos de la Web.

¿Por qué necesita FirstSecure?

Sus datos y sus recursos son vitales para su e-business. Juntos, los productos que componen FirstSecure proporcionan:

Autorización Todo el mundo debe seguir las normas. Las funciones de autorización únicamente admiten el acceso de los usuarios autorizados a los sistemas, datos, aplicaciones y redes.

Seguimiento Podrá saber quién hizo qué y cuándo. Podrá determinar quién realizó una acción y qué acciones se han llevado a cabo durante un intervalo de tiempo especificado.

Fiabilidad Puede estar seguro de que el sistema mantiene sus promesas de seguridad. Esta protección le permite demostrar y validar si el nivel de protección de seguridad pretendido está en vigor.

Disponibilidad El sistema estará disponible cuando lo necesite. Esta protección le ayuda a mantener sus sistemas, datos, redes y aplicaciones en uso para sus empleados, asociados y clientes.

Administración Se pueden definir normas. Esta protección le permite definir, mantener, supervisar y modificar la información acerca de la política de seguridad.

Estas protecciones se pueden implantar según la política de toda la empresa y así proporcionar una capa protectora en todo el conjunto de redes, sistemas y aplicaciones de la empresa. La presencia de un enlace vulnerable entre los productos cubiertos bajo esta capa puede hacer que el resto de la infraestructura resulte inútil.

Esta publicación incluye a todos los componentes esenciales de SecureWay en la lista de protecciones suministradas.

¿Cuáles son los componentes esenciales de FirstSecure?

FirstSecure está compuesto por productos que se pueden obtener como un grupo completo de productos, o como productos independientes relacionados. Estos productos, a su vez, pueden tener uno o más productos componentes. Puede comenzar por cualquiera de estos productos y crear una solución completa de seguridad.

Policy Director

Policy Director es el foco central de la planificación de seguridad. Policy Director proporciona funciones de autorización y gestión de la seguridad de uno a otro extremo de los recursos Web a través de intranets o extranets distribuidas geográficamente. Policy Director proporciona funciones de autentificación, autorización, seguridad de datos y gestión de recursos. Utilice Policy Director junto con las aplicaciones estándar basadas en Internet para crear intranets protegidas y con una buena gestión. Policy Director incluye:

- Security Services
- Management Console
- Management Server
- Security Manager (NetSEAL y WebSEAL)
- NetSEAT Client
- Directory Services Broker
- Authorization Server (soporte de aplicaciones de terceros)

Policy Director se ejecuta en Windows NT, AIX y Solaris.

Consulte el Capítulo 5, “Planificación de Policy Director en la red” en la página 33 para obtener una descripción más completa de Policy Director.

SecureWay Boundary Server

Con los productos SecureWay Boundary Server, las aplicaciones e-business en la Web obtienen las características de fiabilidad, administración y seguimiento mencionadas. En todas partes es necesario trazar límites de seguridad—entre departamentos, como por ejemplo, de recursos humanos y técnicos, entre las redes de las sedes centrales y las oficinas remotas, entre la red de la empresa e Internet, entre las aplicaciones Web de la empresas y los clientes y entre la red de la empresa y los socios comerciales. Para trazar los límites de seguridad correctamente es necesario controlar quién puede acceder a la red y qué información entra y sale de la red.

Esta sección describe los componentes esenciales de SecureWay Boundary Server. Consulte el Capítulo 12, “Consideraciones sobre la instalación de SecureWay Boundary Server y requisitos” en la página 61 para obtener información acerca de las consideraciones de planificación e integración.

IBM SecureWay Firewall

IBM SecureWay Firewall, también denominado IBM Firewall, ofrece seguridad en e-business ya que controla todas las comunicaciones con Internet. IBM Firewall contiene las tres funciones principales de cortafuegos— filtrado, proxy y pasarela a nivel de circuito— que proporcionan un alto nivel de seguridad y flexibilidad.

ACE/Server

ACE/Server, de Security Dynamic, incluye señales SecurID (2 licencias de usuario y 2 señales). ACE/Server añade una conexión de administrador y una conexión VPN *(Red privada virtual)* a IBM SecureWay Firewall.

MIMEsweeper para IBM SecureWay Release 2

MIMEsweeper, de Content Technology, incluye componentes para la seguridad en Internet. MAILsweeper comprueba el correo electrónico para asegurarse de que no haya una filtración de información confidencial de su e-business y que no entre ningún correo electrónico no autorizado.

WEBsweeper impide que el material de la Web no deseado entre en su empresa. Busca y acepta los datos únicamente de los applets Java, códigos ejecutables y sitios Web permitidos.

SurfinGate

SurfinGate, de Finjan Software Ltd., es una solución de seguridad de código portátil para e-business. Dado que ahora el código portátil se puede introducir automáticamente y de forma rutinaria en la red de su e-business desde un lugar externo a su intranet, necesita más protección que simplemente cortafuegos. SurfinGate protege la red de los ataques del código Java, ActiveX y JavaScript. Identifica cualquier ataque potencialmente hostil, lejos de los recursos críticos, antes de que pueda entrar en la red. Pone en cuarentena a los datos sospechosos para que pueda inspeccionarlos antes de aceptarlos.

Intrusion Immunity

Intrusion Immunity proporciona Fiabilidad, en forma de productos de detección y protección para la empresa. Consulte el Capítulo 13, “Consideraciones sobre la instalación de Intrusion Immunity y requisitos” en la página 69 para obtener información sobre los requisitos de Intrusion Immunity. Intrusion Immunity incluye Tivoli Cross-Site for Security y Norton AntiVirus.

Tivoli Cross-Site for Security

Tivoli Cross-Site for Security detecta los accesos indebidos en los sistemas con más posibilidades de ser atacados. Con Tivoli Cross-Site for Security puede:

- Instalar Cross-Site for Security Agent en la red para registrar los incidentes sospechosos que puedan ocurrir en Cross-Site for Security Management Server.
- Visualizar los datos sobre accesos indebidos en informes predefinidos y personalizados.
- Detectar y anotar cronológicamente las actividades no autorizadas o sospechosas en tiempo real.
- Ajustar los agentes de seguridad para disminuir el número de falsas alarmas.

Norton AntiVirus

Norton AntiVirus, un producto de Symantec Corporation, es uno de los productos líderes mundiales en software antivirus. Norton AntiVirus se puede ejecutar permanentemente de forma subordinada para mantener sus sistemas protegidos de los virus procedentes de los archivos adjuntos del correo electrónico, de los controles ActiveX, de los applets Java, de los archivos bajados de Internet, de disquetes, software, CD o archivos enviados a través de una red. Con Norton AntiVirus puede poner en cuarentena los archivos afectados. Puede configurar Norton AntiVirus de modo que le informe automáticamente de las actualizaciones y de los virus descubiertos recientemente.

Public Key Infrastructure

IBM FirstSecure da soporte a los estándares PKI (Public Key Infrastructure) para funciones de cifrado y operatividad entre sistemas mediante IBM SecureWay Trust Authority.

SecureWay Trust Authority es una solución de seguridad que permite emitir, renovar y anular certificados digitales. Estos certificados se pueden utilizar en una amplia gama de aplicaciones de internet, lo que proporciona un medio de autentificar a los usuarios y de asegurar comunicaciones fiables. Trust Authority está basado en especificaciones del grupo de trabajo PKI *(Public Key Infrastructure)* del IEFT *(Internet Engineering Task Force)*. Incluye:

- Soporte para servidores IBM AIX y Microsoft Windows NT
- Una autoridad de registro (RA)
- Una autoridad de certificación (CA)
- Interfaces de usuario para solicitar certificados y para administrar los certificados emitidos

- Un *IBM SecureWay Directory* integrado
- Un subsistema de *auditoría*
- Soporte para SecureWay 4758 Cryptographic Coprocessor
- Soporte para *Smart Cards*

Esta infraestructura da soporte a las tareas necesarias para el periodo completo de la duración de los certificados, incluida la inscripción y certificación inicial, la actualización de los pares de claves, la renovación de certificados, la publicación de listas de certificados y de listas de anulación de certificados, y la anulación de certificados. Consulte el Capítulo 14, “Consideraciones sobre la instalación de Public Key Infrastructure y requisitos” en la página 77 para obtener más información.

Toolbox

FirstSecure Toolbox es un conjunto de kits de herramientas de seguridad, y relacionadas con la seguridad, que forman parte de, o son operativas con, los componentes principales de FirstSecure. Estas herramientas le ayudarán a:

- Integrar sus aplicaciones con FirstSecure.
- Personalizar soluciones y aplicaciones con FirstSecure.
- Crear aplicaciones ISV y OEM que utilicen FirstSecure.

Las API de los kits de herramientas de FirstSecure Toolbox dan soporte a las siguientes funciones de seguridad:

- Servicios de autorización
- Servicios de certificado y gestión
- Servicios de directorio
- Servicios de protocolo SSL (Secure Sockets Layer)
- Servicios de cifrado y de gestión de fiabilidad KeyWorks
  - Las API de IBM Key Recovery Service Provider 1.1.3.0. IBM Key Recovery Service Provider permite recuperar la información cifrada.
  - IBM Key Recovery Server 1.1.3.0. IBM Key Recovery Server 1.1.3.0 es una aplicación que, mediante una petición autorizada, puede recuperar la información cifrada cuando las claves no están disponibles o se han perdido o dañado.

    Estos dos kits de herramientas proporcionan interfaces estándar que las aplicaciones pueden utilizar para activar los servicios de seguridad críticos, junto con interfaces estándar que los proveedores de seguridad pueden utilizar para conectarse con el kit de herramientas. Las interfaces estándar están basadas en la arquitectura CDSA (Common Data Security Architecture). Estos kits de herramientas están disponibles en Windows NT, Solaris y AIX.

Implementation Services

Con FirstSecure Implementation Services su e-business tendrá FirstSecure en ejecución rápida y eficazmente. Estos servicios, que se pueden adquirir por separado, los proporciona IBM y los lleva a cabo un equipo experto de consultores. FirstSecure Implementation Services incluye FirstSecure Implementation Workshop y servicios de instalación QuickStart a nivel de producto. IBM también puede proporcionar servicios de integración del sistema FirstSecure personalizados para su entorno individual.

Póngase en contacto con el representante de IBM para obtener información y conocer las opciones de precios.

Capítulo 2. Novedades del Release 2

El Release 2 simplifica la planificación e instalación de los productos IBM SecureWay FirstSecure. Los productos individuales están más integrados, se han añadido productos y las funciones de gestión y control están más centralizadas.

Policy Director

Policy Director presenta las mejoras siguientes:

- Soporte de IBM SecureWay Directory para almacenar la información de credenciales de usuarios y de grupos.
- Las actualizaciones más recientes de la especificación de la API de autorización del Open Group.
- La posibilidad de definir y editar las credenciales de usuarios del proxy IBM Firewall mediante Policy Director Management Console.
- Un servicio CAS (Credentials Acquisition Service) de Policy Director que proporciona soporte para utilizar los servicios de autentificación externos.
- El soporte de funciones de autentificación basadas en certificados en el extremo del cliente mediante el nuevo servicio CAS (Credentials Acquisition Service) de Policy Director.
- La posibilidad de escribir su propio servicio CAS personalizado a través de la interfaz IDL (Interface Definition Language) entre el CAS de Policy Director y WebSEAL. Policy Director también proporciona la infraestructura de servidor general que maneja las funciones de servidor CAS de Policy Director, como por ejemplo, el arranque, el registro de servidores y el manejo de señales.
- Permite utilizar el mecanismo de túnel de SSL (Secure Sockets Layer) además del mecanismo de túnel de GSS (Generic Security Services).
- Management Console de Policy Director, o la interfaz de línea de mandatos, se pueden utilizar para gestionar las políticas de conexión y de contraseñas.
- Management Console de Policy Director, o la interfaz de línea de mandatos, se pueden utilizar para gestionar la conexión de usuarios individuales, grupos y recursos (destinos).
- Una sola herramienta de gestión de contraseñas de destino para conexión, basada en la Web.
- Un proceso de instalación integrado.

SecureWay Boundary Server

SecureWay Boundary Server presenta las mejoras siguientes:

- Una GUI de configuración que agrupa algunas funciones de SecureWay Boundary Server y Policy Director.
- Una nueva TaskGuide de configuración que agrupa algunas de las funciones de SecureWay Boundary Server y Policy Director.

Novedades de IBM SecureWay Firewall para AIX y NT

IBM SecureWay Firewall, conocido también como IBM Firewall, presenta las mejoras siguientes:

Mejoras de Secure Mail Proxy

IBM Firewall Secure Mail Proxy presenta mejoras que incluyen las siguientes nuevas funciones:

- Algoritmos anti-SPAM que incluyen el bloqueo de mensajes procedentes de los remitentes que aparecen en una lista de exclusión SPAM, comprobaciones para verificar la validez y necesidad de respuesta de los mensajes (métodos conocidos de bloquear mensajes no deseados), límites configurables del número de destinatarios por mensajes de correo, límites configurables del tamaño máximo de un mensaje.
- Protección contra usurpación de identidades, incluida la integración de potentes mecanismos de autentificación.
- Soporte de trampas SNMP y soporte de MADMAN MIB
- Seguimiento de mensajes con la posibilidad de seguir de forma transparente los mensajes emitidos entre el cortafuegos y Domino

Mejoras del protocolo Socks de la versión 5

El protocolo Socks de la versión 5 se ha actualizado de forma que incluye la autentificación UNPW (Username-Password Authentication), la autentificación CRAM (Challenge/Response Authentication) y los conectores de autentificación.

Se ha mejorado el registro cronológico para que el usuario posea un mayor control al clasificar los mensajes del registro cronológico y al especificar los niveles de registro cronológico.

Proxy HTTP

IBM SecureWay Firewall proporciona una implantación del proxy HTTP basada en el producto WTE (Web Traffic Express) de IBM. El proxy HTTP maneja de forma eficaz las peticiones del navegador a través de IBM Firewall, por lo que elimina la necesidad de poseer un servidor socks para navegar por la Web. Los usuarios pueden acceder a información útil a través de Internet, sin comprometer la seguridad de sus redes internas y sin alterar su entorno de cliente para implantar el proxy HTTP.

Remote Access Service

RAS (Remote Access Service) de Windows NT proporciona conexiones de red a través de medios de transmisión conmutados, RDSI o X.25 mediante el protocolo PPP (Protocolo punto a punto, Point-to-Point Protocol). NDISWAN es un controlador de red que se proporciona como parte de RAS y convierte los datos PPP subyacentes para que se asemejen a los datos de la LAN Ethernet.

Mejoras de IBM SecureWay Firewall para AIX

IBM SecureWay Firewall para AIX ofrece numerosas extensiones:

Soporte mejorado de IPSec

El soporte mejorado de IPSec incluye soporte para nuevas cabeceras. También da soporte a la interoperatividad con varios servidores y direccionadores IBM, al igual que a muchos productos VPN que no son de IBM que dan soporte a las nuevas cabeceras.

Soporte MP (Multiprocesador)

Los usuarios del cortafuegos pueden beneficiarse de las características de multiprocesador del RS/6000 para obtener mejoras de rendimiento y una mayor posibilidad de ajuste.

Mejoras de los filtros

Un mejor rendimiento y una mayor flexibilidad en la configuración. Puede ajustar el rendimiento de IBM SecureWay Firewall seleccionando el lugar en el que debe ubicar los diferentes tipos de normas de filtrado. Un indicador de frecuencia proporciona el número de veces que se ha utilizado una conexión.

Conversión de direcciones de red

Se da soporte a las correlaciones de direcciones del tipo diversos a uno. Estas correlaciones se realizan desde varias direcciones internas no registradas o privadas a una dirección legal registrada utilizando los números de puerto para crear correlaciones exclusivas.

Asistente para la configuración

Un asistente ayuda al usuario en la configuración inicial de IBM Firewall. Con este asistente para la configuración el usuario que no está familiarizado con IBM Firewall podrá tener una configuración básica en ejecución inmediatamente después de su instalación.

NSA (Network Security Auditor)

NSA (Network Security Auditor) comprueba que en los servidores de red y en IBM Firewall no hayan defectos de seguridad ni errores de configuración. Es más rápido y más potente.

Novedades de MIMEsweeper para IBM SecureWay Release 2

Las mejoras de MAILsweeper son:

- Exploración de palabras clave para bloquear la entrada de correo molesto o difamatorio y para impedir que datos importantes salgan de la empresa.
- Bloqueo de la entrada de correo electrónico basura
- Bloqueo del envío o recepción de tipos de archivos especificados por parte de individuos o grupos
- Bloqueo o retardo de archivos según su tamaño para evitar la contención de la red

Las mejoras de WEBsweeper son:

- Bloqueo a los empleados de sitios especificados que pueden no estar relacionados con el trabajo
- Ayuda para impedir la extracción de documentos a través de una dirección de correo electrónico o HTML, e información del sitio a través de cookies

Novedades de SurfinGate

SurfinGate presenta las siguientes mejoras:

- Inspección de contenido de JavaScript
- Supervisión de rendimiento en misiones críticas
- Mayor gestión de políticas
- Soporte de los protocolos FTP (File Transfer Protocol) y HTTPS
- Integración de conector con el proxy HTTP del cortafuegos
- Posibilidad de impedir que se bajen archivos ejecutables específicos al sistema de un usuario.

Intrusion Immunity

Los productos Intrusion Immunity ahora incluyen Tivoli Cross-Site for Security.

Novedades de Tivoli Cross-Site for Security

Tivoli Cross-Site for Security proporciona la detección de intromisiones. Permite supervisar los ataques a la integridad de su e-business a través de la red.

Novedades en Norton AntiVirus Solution Suite

Norton AntiVirus Solution Suite, Release 3.0.4, incluye las siguientes versiones actualizadas:

- Norton AntiVirus 5.02 para Windows 95/98 y Windows NT Workstation
- Norton AntiVirus 5.02 para Windows NT Server
- Norton AntiVirus para IBM Operating System/2 (OS/2) 5.02
- Norton AntiVirus OS/2 para Lotus Notes 2.0
- Norton AntiVirus para Lotus Notes 2.0
- Norton AntiVirus para Microsoft Exchange 1.5.2

Public Key Infrastructure

El componente Public Key Infrastructure ahora incluye Trust Authority. Trust Authority contiene:

- Un asistente para la instalación que guía al usuario para la instalación sencilla en Windows NT.
- Una configuración predeterminada para la tarjeta de cifrado 4758 Cryptographic Card. Esta información se puede cambiar.
- Un asistente para la configuración que comprueba la validez de los datos antes de que el programa de configuración subordinado se inicie.
- Mensajes de error y generación de informes.

- Documentación en línea, incluida la ayuda según contexto para los asistentes para la configuración, Registration Authority Desktop, y una aplicación cliente de entidad final.

IBM SecureWay Toolbox

Toolbox presenta las mejoras siguientes:

- Las API de Policy Director junto con la documentación.
- Las API del servicio de directorio.
- Las API PKIX (Public Key Infrastructure) junto con la documentación.
- Ahora IBM Key Recovery Server 1.1.3.0 se incluye en Toolbox. Únicamente está disponible en inglés.

Parte 2. Planificación de una red de e-business segura

La Parte 2 trata los temas de planificación de una red de e-business segura.

En los capítulos siguientes se describe un tráfico típico de Internet y los temas de seguridad y, a continuación, describen cómo funcionan los productos FirstSecure en la red de e-business.

Esta sección contiene los capítulos siguientes:

- El Capítulo 3, “Visión general de una red de e-business” en la página 19 describe una red de e-business típica y los tipos de usuarios, recursos e interacciones que existen en una red. Es posible que su red tenga más o menos características, pero los temas de seguridad serán los mismos y se necesitará la misma protección de seguridad.
- El Capítulo 4, “Planificación de FirstSecure en la red de e-business” en la página 31 agrupa los productos FirstSecure en la red.
- Capítulo 5, “Planificación de Policy Director en la red” en la página 33
- Capítulo 6, “Planificación de SecureWay Boundary Server en la red” en la página 37
- Capítulo 7, “Planificación de Intrusion Immunity en la red” en la página 43
- Capítulo 8, “Planificación de Public Key Infrastructure en la red” en la página 49

Capítulo 3. Visión general de una red de e-business

La red de e-business está compuesta por recursos: datos y bases de datos, usuarios, clientes, suministradores, programadores, hardware, información de la empresa, etc. Se analizarán algunas de estas áreas para que pueda ver donde necesita seguridad.

Internet es una creación compleja. Los datos se trasladan por ésta de servidor a servidor y de usuario a usuario, por vías de acceso no definidas que varían de transmisión a transmisión.

Las transmisiones de datos de la empresa a través de Internet se mezclan con el resto del tráfico que fluye por Internet. Por el camino, es posible que algunos datos críticos de su empresa hayan pasado a través de cualquier servidor que puede estar situado en cualquier lugar. Y cualquier usuario de Internet puede intentar acceder a sus recursos, empleados y datos. Desafortunadamente, además del tráfico legítimo para fines educativos, empresariales y de ocio, Internet también transporta un tráfico malévolo, que puede ser tanto no intencionado como deliberado. La Figura 1 en la página 20 es una visión general de Internet con las transmisiones de datos de la empresa fluyendo por Internet que aparece cargada con el tráfico del resto de los usuarios.

FirstSecure le ayuda a separar y proteger sus transmisiones del resto del tráfico.

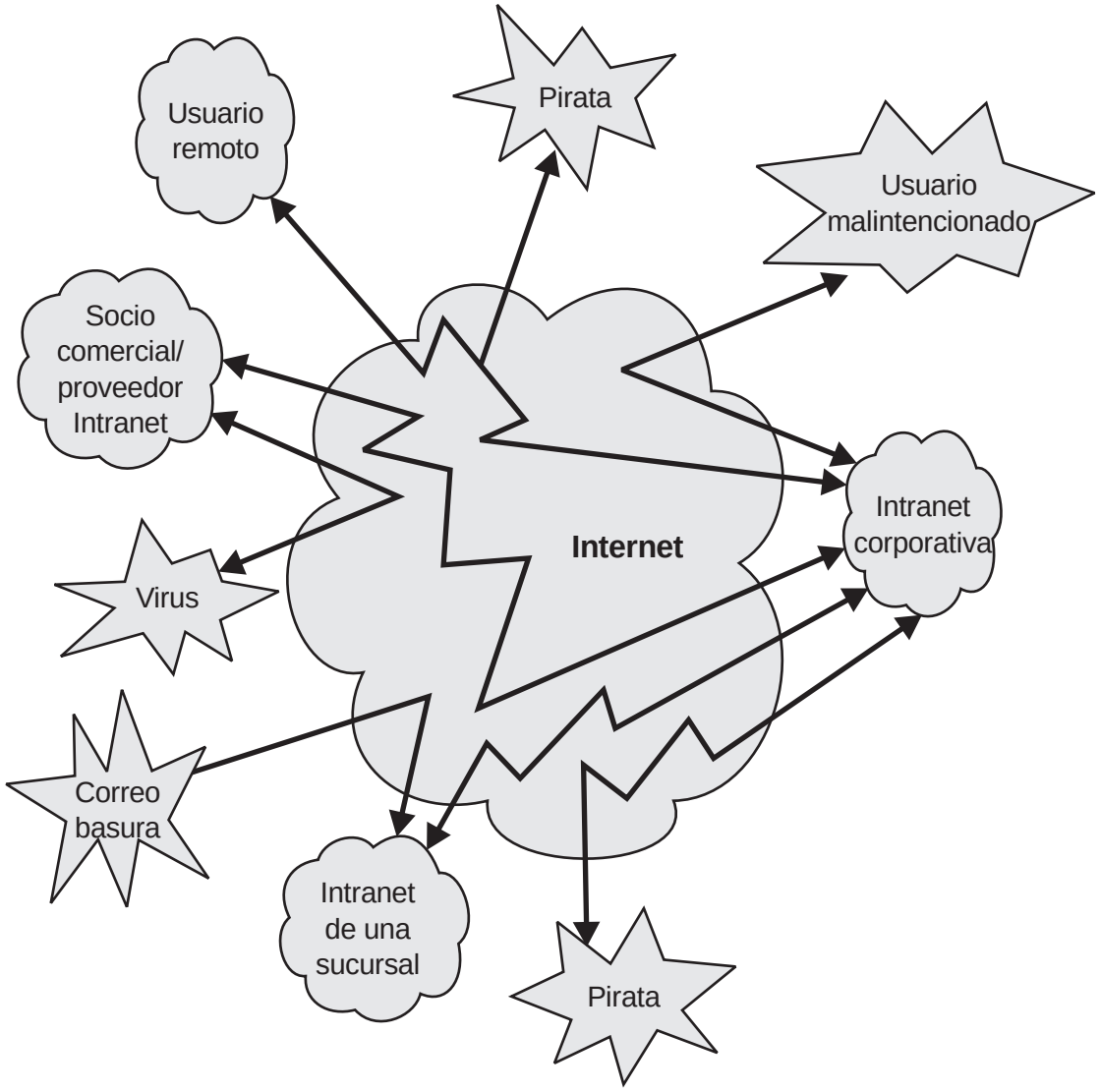


Figura 1. Visión general de Internet ocupada con actividades no relacionadas

Esta visión de Internet no es la que desea para sus operaciones. La visión que desea es la que aparece en la Figura 2 en la página 21, con Internet protegido mediante FirstSecure.

La Internet ideal protegida por FirstSecure

La mayor parte del tráfico de sus operaciones de e-business fluye a través de Internet. Pero para sus operaciones no desea la vista típica de Internet como una agrupación de datos aleatorios que prácticamente todo el mundo puede ver desde su hogar. La Figura 2 muestra Internet tal y como la desea.

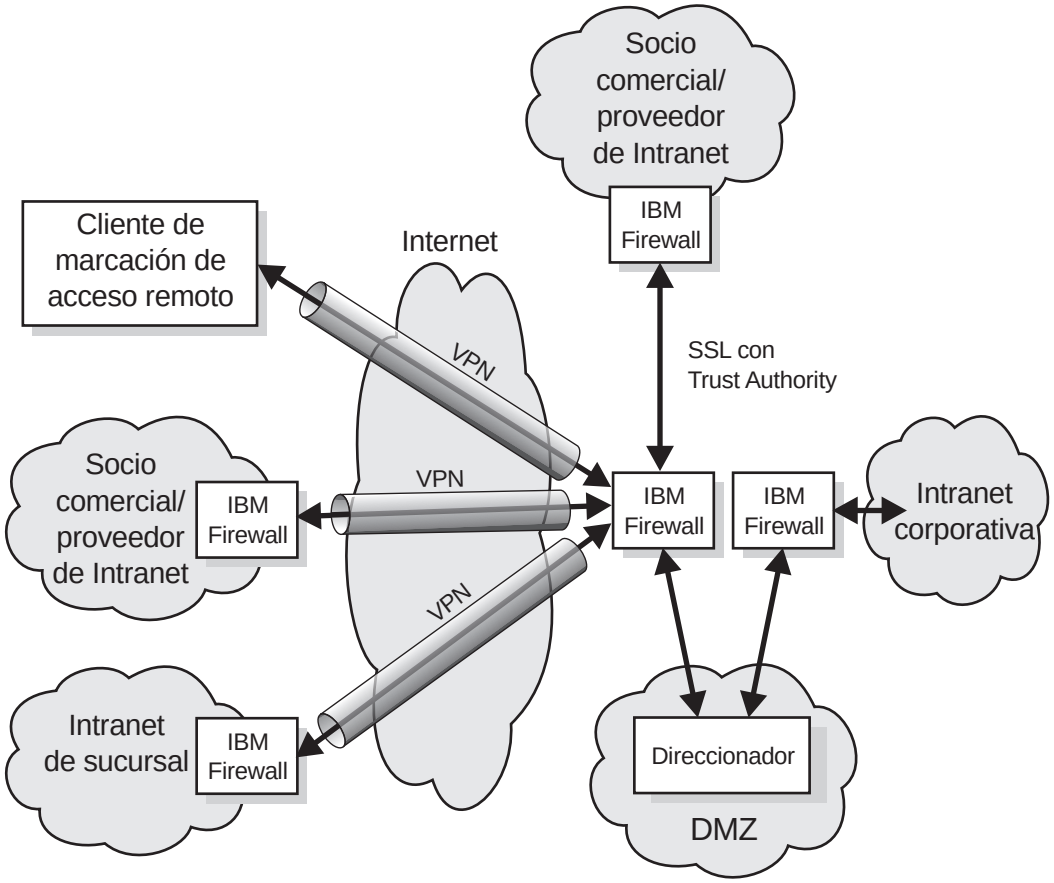


Figura 2. Internet tal y como la desea

Aunque hay mucha y buena información disponible a través de Internet, hay aplicaciones, datos y accesos contra los que deberá proteger a su empresa. Deberá asegurarse de que

- Los empleados no se distraigan de las tareas asignadas.
- Los empleados estén protegidos del correo electrónico inadecuado.

- La información confidencial de la empresa permanece en la empresa.

Red privada virtual

Una VPN (Red privada virtual) es una conexión privada a través de Internet inaccesible para otros. La Figura 3 muestra una VPN típica. La conexión está, para los usuarios de cada extremo, protegida del intrusismo de usuarios o aplicaciones no deseados. Los productos FirstSecure, como por ejemplo IBM SecureWay Firewall, le ayudan a configurar y dar soporte a las VPN.

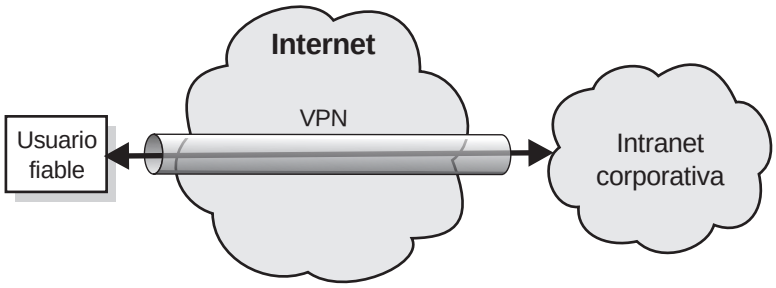


Figura 3. Una Red privada virtual típica.

La DMZ (zona intermedia)

La DMZ (*zona intermedia*) es el conjunto de recursos al que permite que accedan los usuarios externos. Los productos IBM Firewall, MIMEsweeper, y otros productos FirstSecure los utilizará para asegurarse de que únicamente los usuarios que desee puedan acceder a la DMZ, y que éstos tengan acceso únicamente a los recursos especificados. El tráfico de entrada y salida de la DMZ se deberá supervisar para decidir si es apropiado.

El catálogo de la empresa puede estar en la DMZ para que cualquier cliente en potencia pueda navegar por él. O también puede tener folletos informativos que describan su empresa. Los componentes de FirstSecure sólo permiten a los usuarios autorizados acceder a la información que se encuentra fuera de la DMZ.

La Figura 4 en la página 23 muestra una DMZ típica.

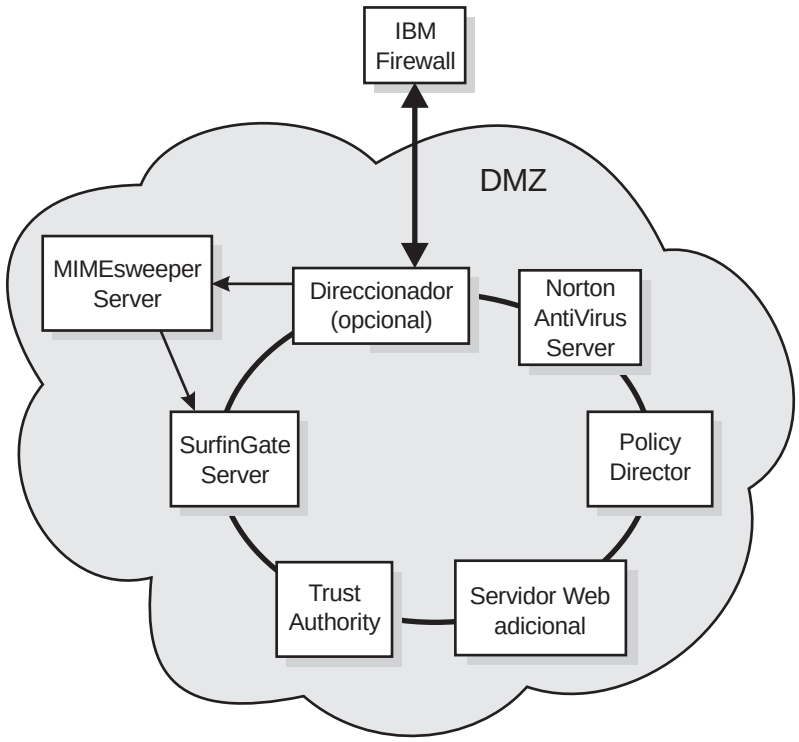


Figura 4. Una DMZ típica con recursos del sistema

A medida que desarrolla aplicaciones seguras, puede utilizar la DMZ como un lugar donde realizar pruebas para la intranet antes de otorgar acceso público a estas aplicaciones.

Ahora analizaremos los tipos de información para los que se utiliza Internet y la intranet.

Una intranet corporativa típica

La intranet corporativa es el lugar donde se realizan las comunicaciones internas de la empresa. Contiene información y recursos que no se desean compartir con Internet. Los empleados comparten datos, se envían correo electrónico entre sí, acceden a los recursos de la empresa, como por ejemplo bases de datos, impresoras y escáneres. La Figura 5 en la página 24 muestra una intranet corporativa.

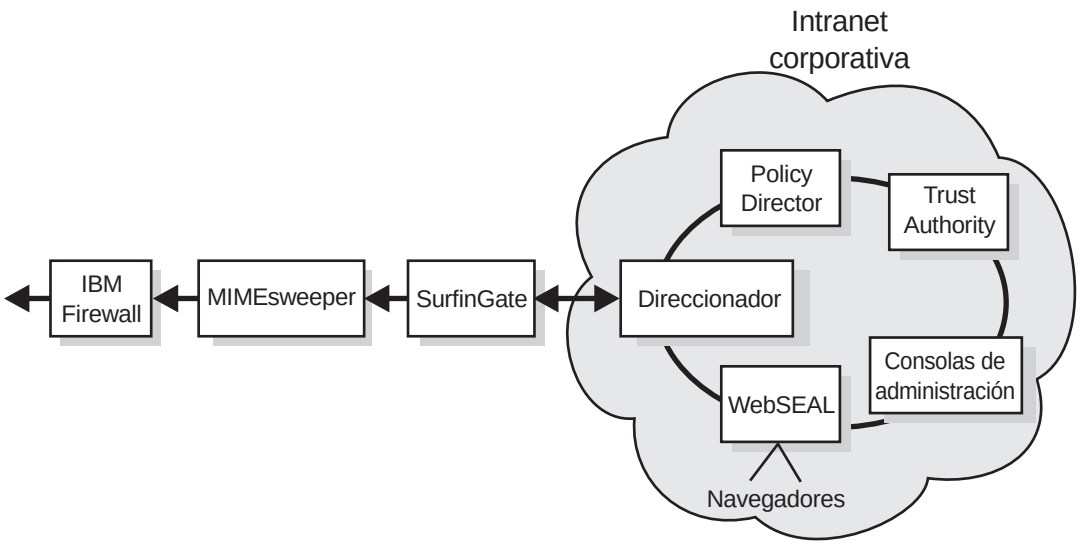


Figura 5. Visión general de una intranet corporativa típica

Debe asegurarse de que la información confidencial de la empresa permanezca en su empresa y que sólo aquellos usuarios autorizados puedan acceder a estos datos. Sin embargo, hay algunos datos a los que sí desea que sus clientes puedan acceder y utilizar. Por ejemplo, desea que un depositante de su banco pueda comprobar el saldo de una cuenta, pero no desea que este depositante pueda acceder a los registros de empleados. Con IBM Firewall su información confidencial continuará siendo confidencial.

Los productos IBM FirstSecure le ayudan a mantener su intranet protegida. Policy Director le permite definir las normas de acceso. IBM SecureWay Trust Authority se asegura de que los usuarios sean quienes pretenden ser. Tivoli Cross-Site for Security le permite saber si hay algún intento no autorizado de acceder a sus recursos de intranet.

Una intranet de una sucursal corporativa típica

Los empleados remotos de sus sucursales necesitan acceder a los mismos datos y a otros recursos del mismo modo que los empleados de la sede central. Pero las conexiones telefónicas para enviar y recibir información son lentas y no están protegidas de interferencias malintencionadas. Y usted desea utilizar Internet como un medio de ahorrar costes y de añadir protección a sus transacciones. La Figura 6 en la

página 25 muestra una sucursal típica en comunicación a través de Internet con una oficina central.

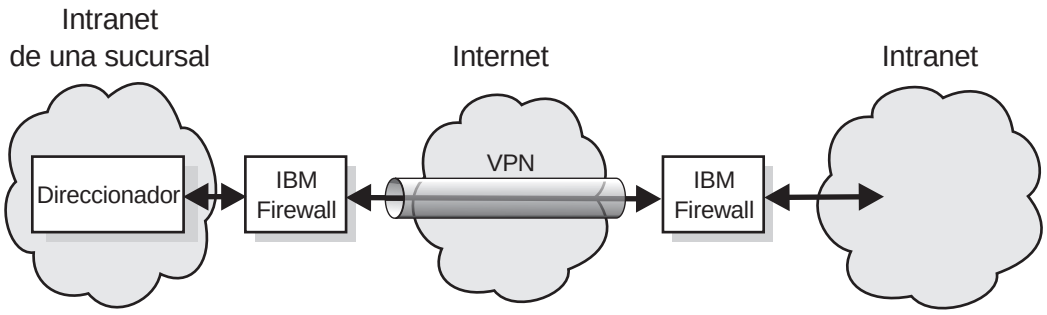


Figura 6. Sucursal conectada a la oficina central a través de una Red privada virtual

Desea que sus transmisiones y sus datos estén tan protegidos como cuando permanecen en un lugar de la empresa. La VPN *(Red privada virtual)* es su túnel a través de Internet. Internet se utiliza como si fuera su red intranet privada.

Un empleado típico con acceso remoto

Es posible que algunos de sus empleados trabajen lejos de la sede central, ya sea de forma permanente u ocasional. Un empleado puede acceder a su red a través de Internet con una conexión conmutada o de línea alquilada.

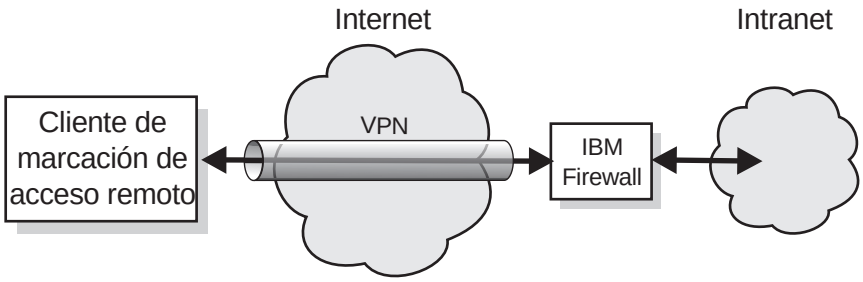


Figura 7. El cliente de acceso remoto con marcación conectado a una oficina central a través de una Red privada virtual

IBM Firewall protege las transmisiones de los empleados.

Una intranet típica de proveedores o socios comerciales

La empresa funciona de forma más eficaz cuando los proveedores y socios comerciales pueden acceder directamente a algunos de sus datos. Un proveedor puede tener autorización para comprobar los niveles de inventario y para enviar nuevas existencias a niveles especificados. Otro socio comercial puede acceder a registros seleccionados. Una empresa de contabilidad puede necesitar acceder a otros registros de impuestos pero no a los registros del socio comercial. La Figura 8 y la Figura 9 en la página 27 muestran un proveedor o socio comercial típicos. Lo deseable es que las transacciones de la empresa viajen por Internet como si viajaran por una conexión privada.

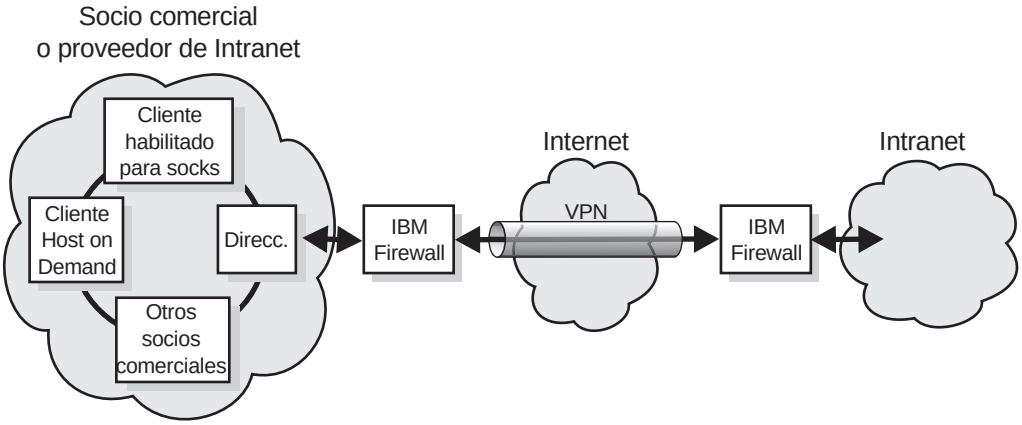


Figura 8. Una intranet de proveedores o socios comerciales típica mediante VPN (Red privada virtual)

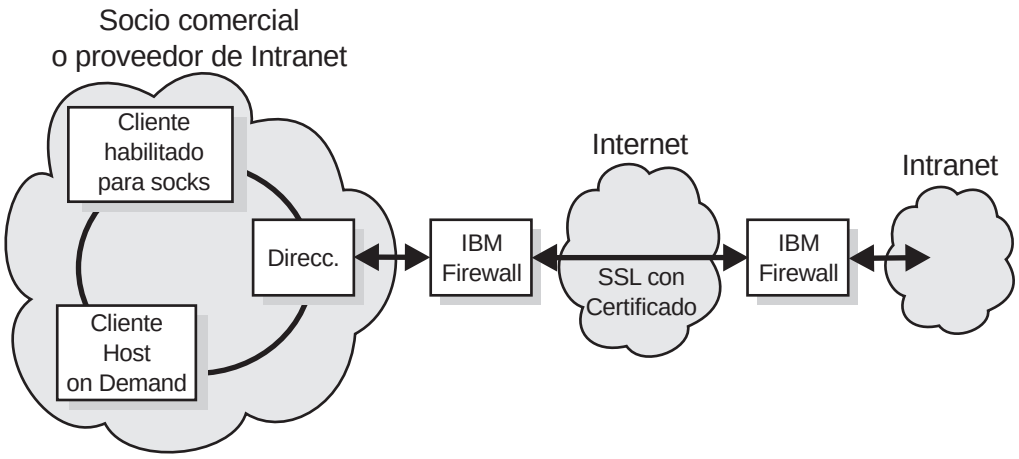


Figura 9. Una intranet de proveedores o socios comerciales típica que utiliza el protocolo de transmisión SSL (Secure Sockets Layer).

Este socio comercial utiliza SSL (Secure Sockets Layer) en lugar de una VPN porque las transmisiones están cifradas de uno a otro extremo. (El usuario también puede utilizar una VPN para obtener una capa adicional de seguridad.)

Necesita proteger a estos usuarios entre sí, de interferencias malintencionadas y de intrusismos. Deberá proteger sus transmisiones de datos de escuchas no autorizadas y de remitentes no autorizados. También deberá asegurarse de que estos usuarios accedan únicamente a los datos que desea que estén accesibles. Y desea asegurarse de que cada uno de estos usuarios sea el usuario que espera.

Datos y bases de datos

Los datos es uno de los recursos más valiosos que posee una empresa. Algunos de los datos de e-business están diseñados para que estén a disposición de todos los usuarios de Internet. Por ejemplo, un distribuidor de hardware puede tener su inventario y su lista de precios disponible para compras en línea. Un minorista de ropa puede tener un catálogo en línea ilustrado de estilos, colores y tamaños para las compras en línea.

Antes de otorgar acceso a los datos, debe saber quién es el que los solicita y por qué desea los datos. Utilice Trust Authority para emitir certificados a los usuarios certificados.

Otras áreas que se han de proteger

Este manual no cubre ningún tipo de contramedidas para otras áreas de seguridad. También tiene que planificar:

- La seguridad del local, el acceso y la salida, y la división en departamentos
- La seguridad física de los portátiles, de los sistemas personales y estaciones de trabajo, y demás contenedores
- La realización de comprobaciones de la historia de seguridad personal
- Las renuncias legales a responsabilidades, contratos, etc.
- La puesta en práctica de medidas operativas como la gestión de claves, el control de información, y la formación y aceptación de los temas de seguridad.

El sistema operativo

Muchos sistemas operativos están configurados para ofrecer una alta disponibilidad y para una gran gama de funciones. Un método de seguridad efectivo es poseer únicamente las funciones mínimas necesarias para realizar una tarea determinada. Debe pensar en desinstalar o inhabilitar todas las características del sistema operativo a las que no desea que acceda un intruso.

Usuarios típicos

Internet tiene muchas clases de usuarios diferentes, algunos convenientes y otros no. En e-business se desean usuarios que sean clientes que realizan búsquedas y compras en línea. Y en e-business también se desea que los socios comerciales puedan acceder a datos específicos para comprobar el inventario, efectuar decisiones de fabricación o para realizar comentarios acerca de los planes y de las actividades de la empresa. En e-business también se desea que los empleados puedan acceder a los datos que necesitan para realizar las tareas asignadas.

Internet también tiene usuarios que un e-business no desea: los piratas informáticos y los intrusos, los que distribuyen virus y los que desean acceder a su datos confidenciales. Estos usuarios incluso pueden encontrarse en su e-business.

Antes de otorgar acceso a cualquier recurso, deberá saber quién es el usuario que lo solicita, qué acceso debe tener este usuario a los datos y aplicaciones y qué registros de acceso de usuario se deben mantener.

Aplicaciones y creación de aplicaciones

Se pueden diseñar aplicaciones que incluyan seguridad. Puede beneficiarse del cifrado de los datos a transmitir, de las funciones de certificación de los usuarios que solicitan acceso y de los registros cronológicos de auditoría de usuarios y transacciones.

Las API de Toolbox permiten añadir seguridad a las aplicaciones.

Seguridad del hardware

Los servidores y los bancos de datos forman parte de un sistema seguro. Aunque este manual no cubre los temas de hardware, deberá planificar la seguridad física de los servidores y estaciones de trabajo utilizados para gestionar la seguridad.

Seguridad del hardware de Trust Authority

Aunque esta sección cubre específicamente el componente Trust Authority, las consideraciones se pueden aplicar a todos los componentes de FirstSecure.

Aislamiento del área Configure el servidor en una sala aislada dedicada a la actividad de CA. A ser posible, la sala debe tener paredes reforzadas, una sola puerta de acero o de madera maciza y un techo de buena construcción sin paneles inclinados. La sala también debe tener un suelo elevado que la proteja de descargas eléctricas en caso de incendio.

Mantenimiento del área La sala debe proporcionar una fuente ininterrumpida de alimentación para los sistemas, puntos de luz, detectores de movimientos y sistemas de calefacción y refrigeración. También debe comprobar que la ventilación de la sala sea correcta para que el calor que genera el equipo no cargue el ambiente.

Control del acceso al área Puede proporcionar acceso a un área física de diferentes formas, como por ejemplo, utilizando identificadores o cerraduras controladas por mando a distancia. Para impedir las intromisiones de una sola persona, debe instalar controles que requieran la presentación de las credenciales correspondientes a como mínimo dos individuos certificados.

También debe supervisar la sala para poder realizar un seguimiento de en qué momento se accede a la sala y quién accede. Para una máxima seguridad, instale detectores de movimientos tanto en el interior como en el exterior de la puerta.

Control de las comunicaciones No debe haber ningún puerto abierto adicional en el servidor Trust Authority. Debe configurar el sistema de modo que escuche únicamente las peticiones en los puertos asignados explícitamente a las aplicaciones Trust Authority.

Siga los procedimientos y los requisitos de la empresa para proteger el hardware que se utiliza en su e-business.

Capítulo 4. Planificación de FirstSecure en la red de e-business

Los capítulos siguientes de esta parte unen los productos incluidos en FirstSecure a su e-business. Los capítulos están basados en las ilustraciones del Capítulo 3, “Visión general de una red de e-business” en la página 19. Todos los productos se describen detalladamente. Para obtener una información más completa acerca de un producto, consulte la documentación que acompaña al producto. Los marcos hipotéticos que se presentan no son más que sugerencias.

En cada marco hipotético, siga los mismos pasos básicos:

1. Haga que todas los componentes de su red utilicen una referencia horaria común para que los registros cronológicos de auditoría resulten más sencillos y precisos.
2. Comience desde su intranet a instalar y comprobar los componentes.
3. Una vez se sienta cómodo en su intranet, comience a crear aplicaciones en su DMZ (zona intermedia).
4. El tráfico entre la intranet y la DMZ debe pasar a través de un cortafuegos.
5. Cree sus aplicaciones de Internet externas y compruébelas con los datos de las pruebas.
6. Instale un cortafuegos para proteger el tráfico entre Internet y su DMZ.
7. Otorgue acceso a los usuarios de su red.

Planificación de un sistema FirstSecure completo

El siguiente es el orden que se sugiere para desplegar los productos FirstSecure en la red. Se ha simplificado enormemente. Consulte la Parte 3, “Consideraciones sobre la instalación y la integración” en la página 55 para obtener los requisitos detallados de hardware y software para cada producto y para obtener información sobre los puntos a tener en cuenta en relación con la integración. También lea los requisitos de instalación y las instrucciones que acompañan a cada producto. Muchos productos también tienen información actualizada en Internet. El apartado “Información en la Web” en la página xii lista los sitios Web con información sobre FirstSecure. El libro rojo, *Understanding the IBM SecureWay FirstSecure Framework*, SG24–5498 contiene varios marcos hipotéticos más detallados.

1. Planifique los requisitos de seguridad que necesitará.
2. Instale Policy Director para satisfacer estos requisitos.
3. Cree y compruebe su aplicación de servidor del cliente. Manténgala en su intranet corporativa de momento, todavía no permita que esté disponible en Internet.
4. Instale IBM Firewall, que protegerá la aplicación de servidor del cliente.
5. Añada SurfinGate a la DMZ.
6. En su DMZ (zona intermedia), añada MIMEsweeper y Norton AntiVirus para proteger las aplicaciones cuando permita que estén disponibles en Internet. Cuando estén disponibles para el tráfico externo, configúrelas de modo que apunten a sus servidores.
7. Instale el producto Tivoli Cross-Site for Security para detección e inmunidad contra intromisiones.
8. En su DMZ añada:
   - Servidores Web
   - Servidor Web de catálogos
   - Servidor Web de inventarios
   - Aplicaciones cliente para compradores
   - Aplicaciones cliente para compradores seguras
   - Un Cross-Site for Security Agent o más

   Compruebe todas sus aplicaciones detrás del cortafuegos antes de abrirlas al tráfico. Utilice la herramienta Network Security Auditor de SecureWay Boundary Server para comprobar las normas que ha establecido.
9. Instale una instancia de IBM SecureWay Firewall para proteger el software dentro de la DMZ. La configuración por omisión deberá ser “Sin tráfico”, para que pueda comprobar la instalación antes de abrirla al público.
10. Instale Trust Authority y emita certificados a usuarios certificados.
11. Abra su aplicación a Internet una vez haya finalizado la comprobación.
12. Ejecute Network Security Auditor desde fuera del sistema para comprobar las normas antes de anunciar el acceso al público.
13. Compruebe los registros cronológicos creados por los programas componentes de FirstSecure para asegurarse de que no ha ocurrido ningún incidente adverso.
14. Continúe comprobando los registros cronológicos de auditoría y vaya añadiendo Cross-Site for Security Agent a medida que añade aplicaciones a la red.

Capítulo 5. Planificación de Policy Director en la red

FirstSecure proporciona un punto de control consolidado dirigido por políticas, para entornos Web heterogéneos. En entornos en los que los usuarios acceden a varios servidores Web subordinados a través de navegadores, Policy Director proporciona:

- Un solo inicio de sesión para cada usuario de la Web
- Verificación de la identificación
- Comprobación de las autorizaciones de los usuarios que solicitan acceso a las páginas Web protegidas

Con este soporte, puede autorizar y asegurar:

- Intercambios de TCP/IP, como por ejemplo HTML, Telnet y POP3
- Aplicaciones de terceros, tales como sistemas de bases de datos
- Herramientas de gestión de redes
- Aplicaciones desarrolladas en la empresa

Con FirstSecure, los usuarios pueden autentificarse a Policy Director mediante los siguientes mecanismos:

- Autentificación básica sobre SSL (Secure Sockets Layer)
- Inicio de sesión basado en formularios sobre SSL
- SSL mediante certificados de cliente
- Inicio de sesión Kerberos

FirstSecure controla el acceso de los usuarios autentificados a servicios de red y objetos de tipo Web individuales y puede limitar los usuarios no autorizados a un subconjunto de dichos recursos.

Despliegue de Policy Director

Policy Director gestiona la correlación entre usuarios y grupos y los recursos. La consola de gestión de Policy Director se utiliza para:

- Definir usuarios y grupos que utilizarán los recursos.
- Definir los objetos que necesitan protección. Los objetos pueden ser la Web, los puertos TCP, los métodos y las interfaces.

- Definir cómo accederán los usuarios a los recursos y qué normas protegerán los recursos, como por ejemplo, para lectura, modificación, administración, ejecución o supresión.

La tabla siguiente describe las configuraciones de los componentes de Policy Director más comunes. Determine la configuración adecuada para su red. A continuación, seleccione dichos componentes durante la instalación.

Consulte la publicación *IBM SecureWay Policy Director Up and Running* para obtener una información más detallada.

Ejemplo de configuración	**Componentes instalados**
Un servidor que ejecute una sola instancia del servidor Management Server para el dominio seguro. En este marco hipotético, Management Server reside sólo en su propio sistema. Management Server mantiene la base de datos de autorizaciones maestra del dominio seguro, efectúa una réplica de estos datos en todo el dominio seguro, y mantiene la información sobre la ubicación de otras máquinas servidor de Policy Director en el dominio seguro.	Sólo para Management Server
Un servidor WebSEAL. Este marco hipotético representa la solución para proteger un espacio Web. WebSEAL da soporte a servidores subordinados, lo que ofrece una elevada disponibilidad y tolerancia ante anomalías.	Security Manager con WebSEAL
Un servidor NetSEAL. Este marco hipotético representa la solución para proteger una red VPN (Red privada virtual) y proporciona control de acceso para los servicios de red de terceros y propios.	Security Manager con NetSEAL
Una combinación de servidor WebSEAL y NetSEAL.	Security Manager con WebSEAL y NetSEAL
Un servidor que proporciona acceso al servicio Authorization Service de Policy Director para aplicaciones de terceros.	Authorization Server
Un servidor que proporciona un entorno de desarrollo para los desarrolladores que deseen crear aplicaciones de terceros que utilicen la API de autorizaciones.	Authorization Server y ADK
Un servidor que proporciona los servicios combinados de todas las configuraciones mencionadas.	Todos los componentes

Policy Director es un sistema de seguridad con un alto nivel de distribución que puede desplegar componentes de una gran variedad de configuraciones en una o más máquinas. La siguiente es una visión general de cómo utilizar Policy Director en la red.

En la publicación *IBM SecureWay Policy Director Up and Running* encontrará las instrucciones de instalación completas.

1. Instale el servidor de seguridad de Policy Director.

   Como mínimo un sistema del dominio seguro debe contener el servidor de seguridad de Policy Director para configurar un dominio seguro para Policy Director. Consulte los manuales de instalación y administración y los recursos de soporte técnico para las plataformas deseadas.

   Los servidores restantes pueden funcionar sólo con las instalaciones clientes DCE (o con NetSEAT en sistemas Windows NT).

2. Instale el servidor SecureWay Directory (LDAP).
3. Instale Policy Director.
   - El servidor de seguridad de Policy Director debe desplegarse en primer lugar (consulte el paso 1).
   - Todas las instalaciones de servidores de Policy Director requieren Policy Director Base.
   - Si esta es la *primera* o la *única* máquina del dominio seguro, debe instalar Management Server.

     Si esta es una máquina *adicional* en un dominio seguro existente donde ya hay un Management Server, no instale otro Management Server. Únicamente debe haber una instancia de Management Server en cualquier dominio seguro.
   - WebSEAL, NetSEAL y los componentes de servidor de autorizaciones de terceros son opcionales.
   - Security Manager se combina junto con WebSEAL para proporcionar el componente servidor HTTP de WebSEAL y el control de acceso HTTP con un riguroso nivel de filtrado, y junto con NetSEAL para proporcionar el componente de control de acceso TCP/IP NetSEAL con un nivel de filtrado más amplio.
4. Instale Management Console.

   Management Console requiere que instale un cliente DCE (o NetSEAT para Windows NT) en el sistema operativo (consulte el paso 1).

5. Las siguientes dependencias son aplicables a las aplicaciones que se desarrollan con el componente Authorization ADK:
   - Necesitará el paquete Policy Director.
   - Instale IVAuthADK en la máquina de la aplicación.
   - El sistema operativo en el que se ejecuta la aplicación debe tener un cliente DCE o NetSEAT para sistemas Windows NT.
   - El dominio seguro que ejecuta una aplicación debe tener instalado como mínimo un componente Authorization Server en un sistema del dominio seguro. Un entorno de desarrollo típico requiere que el componente

Authorization Server esté en el mismo sistema operativo que Authorization ADK.

Capítulo 6. Planificación de SecureWay Boundary Server en la red

FirstSecure proporciona seguridad para las aplicaciones basadas en la Web que se benefician de los estándares de seguridad actuales, como por ejemplo, SSL (Secure Sockets Layer), SOCKS e IPSec.

Si su entorno operativo incluye conexiones entre dos partes de la red con diferentes características de fiabilidad, el componente SecureWay Boundary Server de FirstSecure le será útil para conseguir los requisitos siguientes:

- Conexiones seguras a Internet, minimizando la posibilidad de accesos no autorizados a su red privada
- Infraestructuras extranet a gran escala para compartir datos de forma selectiva con los socios comerciales y los proveedores
- Utilización de Internet u otros segmentos de red relativamente poco fiables como una VPN (Red privada virtual), manteniendo los mensajes como confidenciales cuando cruzan la infraestructura de red con poca fiabilidad.

SecureWay Boundary Server de FirstSecure utiliza tecnologías de filtrado de direcciones de red, filtrado de contenido, proxy y las tecnologías de pasarela a nivel de circuito. Mediante la combinación de estas tecnologías, SecureWay Boundary Server permite que las operaciones de e-business sean seguras y estén dirigidas por políticas, ya que controla las comunicaciones entre las redes con diferentes características de fiabilidad.

SecureWay Boundary Server incluye:

- IBM SecureWay Firewall, incluido ACE/Server
- MIMEsweeper para IBM SecureWay Release 2
- SurfinGate 4.05 para Windows NT
- Mejoras en las gestión de políticas

Consulte la Figura 10 en la página 38 para obtener una visión general del flujo de datos en una instalación SecureWay Boundary Server completa.

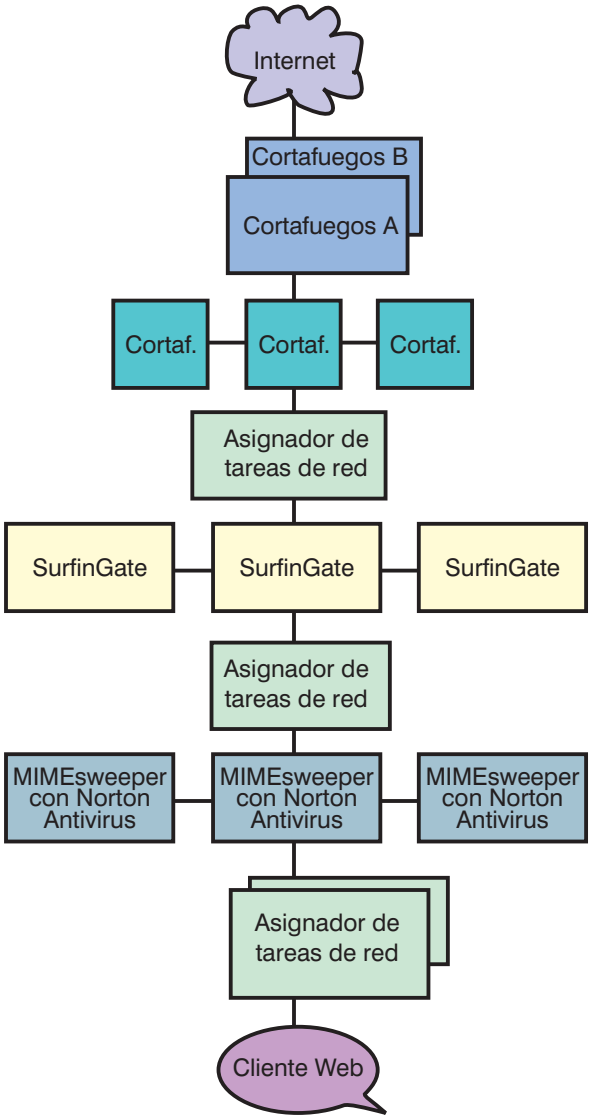


Figura 10. Visión general de un flujo de datos en productos SecureWay Boundary Server

Despliegue de IBM SecureWay Firewall

IBM SecureWay Firewall, también denominado IBM Firewall, controla las comunicaciones hacia y desde Internet. Esta tecnología de cortafuegos protege los propios activos de IBM.

Consulte el apartado “Consideraciones sobre el componente SecureWay Boundary Server” en la página 64 para obtener las consideraciones de instalación.

Entre los temas de conectividad que ha de tener en cuenta se encuentran:

- La necesidad de conectarse a Internet pero de impedir el acceso no autorizado a la red, las aplicaciones o los datos de la empresa
- El uso abusivo de las infraestructuras de red por parte de los usuarios internos
- Las formas de planificar una infraestructura extranet a gran escala para socios comerciales y proveedores, a pesar del alto coste de la gestión de la configuración
- El alto coste de las líneas alquiladas que conectan a las diferentes sucursales
- La baja productividad en la empresa como consecuencia de una comunicación ineficaz, tardía o confusa entre los socios comerciales y los proveedores
- El alto coste administrativo que representa gestionar software en idiomas no nativos

IBM Firewall da respuesta a todas estos temas. Como el cortafuegos sólo admite el tráfico explícitamente permitido, IBM Firewall protege su red de intrusos. Para tener una protección aún mayor, el software de comprobación de la vulnerabilidad incluido con IBM Firewall puede *fortalecer* el servidor en el que se ejecuta IBM Firewall para garantizar que los piratas informáticos no puedan burlar el cortafuegos. Las direcciones IP y la configuración de la red interna están ocultas para la red no fiable. Todo el tráfico que pasa por el cortafuegos queda registrado y puede utilizarse para generar informes de actividad de usuario.

IBM Firewall y su aplicación de configuración de VPN permiten utilizar y gestionar, sin grandes costes, infraestructuras VPN a gran escala. Los estudios de redes han mostrado que los clientes pueden utilizar las VPN para beneficiarse de un ahorro significativo en el coste de las soluciones de líneas alquiladas.

Con IBM Firewall, puede interconectar sus sucursales a través de Internet, desplegando cortafuegos en cada sucursal y utilizando un túnel basado en IPSec.

Junto con IBM Firewall se proporciona ACE/Server, un producto de Security Dynamics Technologies, Inc. ACE/Server, que proporciona potentes servicios de autentificación centralizados para redes de empresas, de modo que sólo los usuarios autorizados pueden acceder a comunicaciones, aplicaciones y archivos de red. Junto con la tecnología de señales SecurID, patentada por Security Dynamics Technologies Inc.,

ACE/Server crea una barrera que impide el acceso no autorizado. La autentificación está basada en dos factores: los usuarios deberán *tener* algo (una tarjeta de SecurID) y *saber* algo (un PIN) que los autentificará.

Despliegue de MIMEsweeper

MIMEsweeper es un producto de Content Technologies Ltd. que realiza un análisis basado en el contenido de los datos de Internet y de la intranet a fin de identificar los posibles riesgos o amenazas y proteger a los usuarios de la red ante estos riesgos.

Consulte el apartado “Consideraciones sobre el componente SecureWay Boundary Server” en la página 64 para conocer las consideraciones sobre la instalación.

MIMEsweeper contiene dos módulos básicos, MAILsweeper y WEBsweeper, que protegen a los usuarios de maneras diferentes. Cuando MIMEsweeper recibe correo u otros datos de tipo Web, MIMEsweeper verifica las direcciones del remitente y del receptor y después descompone repetidamente el archivo en las partes que lo componen. A continuación MAILsweeper y WEBsweeper analizan estas partes para minimizar el riesgo de que los posibles problemas o amenazas puedan entrar en su red privada.

FirstSecure incluye tanto MAILsweeper 4.0 como WEBsweeper 3.2_5. Cada uno de ellos se puede instalar, configurar y utilizar por separado.

MAILsweeper puede:

- Trabajar con exploradores de virus seleccionados por usted a fin de verificar que los archivos que se han fragmentado no contienen virus
- Detectar y bloquear macros "bomba"
- Explorar las palabras clave para:
  - Evitar expresiones políticamente incorrectas en los mensajes de correo electrónico
  - Evitar que información importante o valiosa salga de la empresa
- Bloquear el correo electrónico basura entrante, descongestionando así la red y minimizando la pérdida de productividad de los empleados.
- Evitar que usuarios o grupos envíen o reciban determinados tipos de archivos como, por ejemplo, AVI o MPEG
- Bloquear o retrasar archivos según el tamaño hasta que la red pueda acomodar mejor el tráfico

WEBsweeper puede:

- Impedir que determinados usuarios puedan acceder a ciertas direcciones que seguramente no están relacionadas con el trabajo
- Evitar la pérdida accidental de documentos importantes o confidenciales

Además, MIMEsweeper contiene una API (interfaz de programación de aplicaciones) que puede utilizar para integrar bloqueadores de URL de otras empresas.

MIMEsweeper puede ser una herramienta fundamental para proteger a la empresa y a los usuarios frente a amenazas de seguridad de Internet.

Nota: Aunque la documentación de MIMEsweeper puede proporcionarle la manera de contactar con Content Technologies para obtener servicio técnico y soporte, si obtiene MIMEsweeper para IBM SecureWay Release 2 como parte de la oferta de SecureWay FirstSecure o de la oferta de SecureWay Boundary Server, deberá ponerse en contacto con IBM para solicitar servicio técnico y soporte.

Despliegue de SurfinGate

SurfinGate es un producto de Finjan Software Ltd. que examina el código móvil, como por ejemplo, el código JavaScript, los applets Java o los controles ActiveX para proteger su red de daños, como pueden ser la modificación de datos, la supresión de información o la recopilación ilícita de datos. SurfinGate inspecciona el código móvil a nivel de pasarela e identifica el código que supone algún tipo de amenaza antes de que éste pueda entrar en la red. El código móvil puede bloquearse de manera selectiva o bien puede admitirse en función de cada usuario o de cada departamento, y puede admitirse o denegarse el acceso del código a la red de la empresa según su función teórica. Con SurfinGate, los administradores pueden habilitar el código móvil y gestionar, controlar y reforzar las políticas de seguridad de la empresa para ActiveX, Java, JavaScript, Visual Basic Script, complementos y cookies.

SurfinGate incluye los componentes siguientes:

- SurfinGate Server
- SurfinConsole
- Base de datos de SurfinGate
- Componentes para integración WTE

SurfinGate Server actúa como servidor proxy HTTP o como servicio para el cortafuegos o el proxy. SurfinGate Server puede colocarse después del cortafuegos de la empresa y otros servidores proxy existentes, y además actúa como servidor HTTP. Esta arquitectura permite detener el código móvil e inspeccionarlo antes de que se produzca un ataque.

Un administrador de la red puede utilizar SurfinConsole para gestionar y definir una política de seguridad central de la empresa para el código móvil. SurfinConsole puede controlar varios servidores SurfinGate Server de la red y aplicar normas de la empresa

para código móvil, o bien por usuario o bien por grupo, o mediante listas de los códigos considerados inaceptables o aceptables.

La base de datos de SurfinGate almacena información detallada de ASP (Applet Security Profiles), incluidas la información sobre usuarios y grupos y las políticas de seguridad correspondientes. Como SurfinGate examina dinámicamente el contenido de todo el código móvil, la base de datos no es necesaria de cara a la seguridad, pero ayuda a mejorar el rendimiento en operaciones a gran escala.

Nota: Aunque la documentación de SurfinGate puede proporcionarle un contacto con Finjan para obtener servicio técnico y soporte, si obtiene SurfinGate para Windows NT como parte de la oferta de SecureWay FirstSecure o de la oferta de SecureWay Boundary Server, deberá ponerse en contacto con IBM para solicitar servicio técnico y soporte.

Capítulo 7. Planificación de Intrusion Immunity en la red

Las tecnologías de seguridad que se han descrito hasta este momento ponen el énfasis en las amenazas a la seguridad. Otro aspecto de la seguridad de similar importancia es la detección de estas amenazas. Los productos que ofrecen inmunidad ante posibles intrusismos en FirstSecure proporcionan la detección de intromisiones y posibilidades antivirus que permiten a la empresa detectar las amenazas de seguridad.

El software antivirus proporciona protección contra todo tipo de código peligroso, incluidos los caballos de Troya, gusanos, virus en macros o controles ActiveX y applets Java dañinos. La protección contra virus es una parte fundamental de toda solución de seguridad. Los productos antivirus de FirstSecure dan respuesta a estos requisitos clave de protección ante los virus:

- Se cubre una amplia gama de clientes para proporcionar un método amplio y coherente que satisfaga las necesidades antivirus de los clientes fijos o con movilidad geográfica.
- Se ofrece un servicio de suscripción para signaturas de virus. La actualización periódica de las signaturas de virus es fundamental para mantener de forma eficaz la protección contra las últimas formas de código peligroso.
- Las actualizaciones de antivirus se distribuyen, según las políticas de la empresa, desde los servidores a los clientes para de este modo asegurar que las políticas antivirus entren en vigor.

Despliegue de Tivoli Cross-Site for Security

Tivoli Cross-Site for Security proporciona detección de los accesos indebidos en la red en aquellos sistemas que presentan más posibilidades de ser atacados. Se pueden desplegar los agentes de Tivoli Cross-Site for Security dondequiera que su dominio de administración se conecte con Internet. Tivoli Cross-Site for Security supervisa las redes para detectar los ataques internos y externos. Presenta los beneficios siguientes:

- Detección de intrusismos en tiempo real que alerta al administrador de Cross-Site for Security sobre posibles ataques
- Políticas configurables que permiten establecer diferentes políticas para los agentes de su DMZ y para los agentes de su intranet
- Modificación en línea de la política de Security Agent que le permite responder rápidamente a los cambios de entorno

- Integración con las aplicaciones para la empresa de Tivoli Enterprise para que pueda aumentar su sistema de gestión de empresa Tivoli.

Tivoli Cross-Site for Security puede:

- Detectar exploraciones y ataques masivos
- Supervisar el tráfico IP
- Supervisar los servicios de puertos
- Detectar peticiones y respuestas del sistema de archivos de la red, DNS y del servicio de montaje
- Detectar las peticiones de servicio de correlación de puertos y responder a los vuelcos
- Detectar las llamadas RStatd
- Detectar las peticiones de nombres de correlaciones y nombres de archivos específicos
- Detectar los ataques basados en SMB en los servidores de archivos de PC
- Detectar el protocolo de mensajes de control de Internet

Cross-Site for Security le permite supervisar el tráfico de red y detectar los ataques y los intentos de intrusismo. Supervisa el tráfico en la DMZ, que aísla su intranet de Internet, y en la red interna.

Los tipos de intrusismos que Cross-Site for Security puede detectar son:

- Detección de signaturas o patrones
- Detección de ataques masivos
- Ataques basados en la red
- Ataques en la red Windows
- Ataques de procedimientos remotos
- Explotaciones del servicio
- Tráfico de red no autorizado
- Actividades sospechosas

Cross-Site for Security protege la red utilizando Cross-Site for Security Agent y Cross-Site for Security Management Server. Cuando un agente detecta un ataque crítico, envía un suceso cifrado a Cross-Site for Security Management Server, el cual inmediatamente anota cronológicamente la información y responde. Puede configurar Cross-Site for Security Management Server de modo que envíe una alerta a la consola, que envíe un correo electrónico a un administrador o que busque a un administrador que esté disponible.

Obtención de una clave de licencia Tivoli Cross-Site for Security

Para habilitar el producto Tivoli Cross-Site for Security, necesita una clave de licencia personalizada.

Puede recibir la clave de licencia desde el sitio Web de Tivoli Cross-Site y realizar los pasos siguientes:

1. Busque el documento de titularidad Passport Advantage Proof of Entitlement que ha recibido con los productos FirstSecure, incluido el CD-ROM de Tivoli Cross-Site for Security y también la publicación *Tivoli Cross-Site for Security Installation*.
2. Localice en su documento de titularidad Passport Advantage Proof of Entitlement el número de pedido, un número de ocho dígitos que comienza por 5, y el número de cliente (local), un número de siete dígitos que comienza por 7. Utilice estos números para acceder al sitio Web Tivoli Cross-Site por primera vez.
3. Conéctese al sitio Web Tivoli Cross-Site utilizando un navegador Web en un sistema con acceso a Internet. El URL del sitio Web es `www.cross-site.com/support/licensing/`.
4. Especifique su número de pedido, su número de cliente y la información de contacto. También debe suministrar el nombre de dominio del servidor en el que piensa instalar Tivoli Cross-Site for Security.
5. Siga las instrucciones adicionales que encontrará en la Web.
6. Si tiene problemas para acceder al sitio Web de claves de licencia Tivoli Cross-Site, póngase en contacto con el servicio de soporte de Tivoli Cross-Site en el número 1–800–2–TIVOLI, extensión 9396 (en los EE.UU.) o mediante un correo electrónico a licensing@cross-site.com.

Productos Tivoli Cross-Site relacionados

La familia de productos Tivoli Cross-Site incluye otros componentes que no forman parte de la familia FirstSecure:

- Tivoli Cross-Site for Availability supervisa y genera informes sobre si los usuarios finales pueden acceder satisfactoriamente a su sitio Web.
- Tivoli Cross-Sitefor Deployment amplía el alcance de la empresa, ya que permite distribuir y gestionar las aplicaciones y la información críticas a través de Internet.

Aunque es posible que estos productos se mencionen en la documentación de Tivoli Cross-Site for Security, deben adquirirse por separado.

Supervisión del tráfico con Tivoli Cross-Site for Security

Cross-Site for Security Agent es un detector inteligente de la red. Supervisa de forma continuada los paquetes de la red. Cross-Site for Security Agent filtra los paquetes en busca de diferentes signaturas que puedan representar actividades sospechosas. Estas signaturas pueden indicar ataques en la red.

Cross-Site for Security Agent se ejecuta como un *daemon* en UNIX, y como un servicio NT en Windows NT. Cross-Site for Security está configurado de forma que pueda iniciarse automáticamente cuando se arranca el sistema. Reside y se ejecuta de forma subordinada en el sistema haya o no un usuario conectado.

Cuando se detecta un posible ataque, el agente determina la gravedad y si debe notificarlo inmediatamente al servidor de gestión, o si debe anotar cronológicamente la alerta en un archivo local. Los registros cronológicos se suben periódicamente al servidor de gestión.

El agente también se pone en contacto regularmente con Cross-Site for Security Management Server para hacerle saber que el agente está activo y en ejecución. Este tipo de comunicación se llama una *pulsación*. El usuario puede configurar los intervalos de las pulsaciones.

Cuando el servidor de gestión recibe una pulsación del agente, el servidor de gestión notifica al agente si hay información de configuración actualizada, nuevas signaturas y si se han subido planificaciones. Automáticamente el agente baja e instala estas actualizaciones.

Tivoli Cross-Site for Security en la red

Puede configurar Cross-Site for Security de modo que se ajuste a los requisitos de su empresa. Las decisiones principales son:

- ¿Dónde se ha de instalar Cross-Site for Security Management Server?
- ¿Cuántos Cross-Site for Security Agent necesita?
- ¿Dónde debe instalar Cross-Site for Security Agent?

Estas consideraciones, además del tamaño, la topología y la anchura de banda y el tráfico de la red, son críticas para determinar el número de servidores de gestión y de agentes. Consulte el apartado “Requisitos de hardware y software de Intrusion Immunity” en la página 69 para obtener las consideraciones sobre la instalación de Tivoli Cross-Site for Security.

Nota: Aunque la documentación de Tivoli Cross-Site for Security puede proporcionarle la manera de obtener servicio técnico y soporte, cuando adquiera Tivoli

Cross-Site for Security como parte de la oferta SecureWay FirstSecure, deberá ponerse en contacto con IBM para obtener servicio técnico y soporte.

Despliegue de Norton AntiVirus

Norton AntiVirus, de Symantec Corporation, es uno de los productos de software antivirus líderes del mundo. Norton AntiVirus puede:

- Poner en cuarentena los archivos infectados
- Ofrecer protección contra virus y controles ActiveX y applets Java maliciosos.
- Ofrecer protección contra virus procedentes de archivos adjuntos al correo electrónico, archivos bajados de Internet, disquetes flexibles, CD de software o desde una red.

Puede planificar Norton AntiVirus de modo que se ejecute permanentemente de forma subordinada para ayudarle a mantener la seguridad del sistema. Los investigadores de Symantec continúan añadiendo virus a la lista de los que Norton AntiVirus puede detectar. Puede utilizar la característica LiveUpdate para recuperar de forma automática nuevas definiciones de antivirus de Symantec una vez a la semana.

La función de cuarentena de Norton AntiVirus aísla archivos infectados o sospechosos en una ubicación segura del sistema, separados del resto de los archivos para impedir que se distribuya el virus mientras arregla el archivo.

El asistente Scan and Deliver permite enviar fácilmente archivos sospechosos a Symantec para su evaluación. El centro SRAC (Symantec AntiVirus Research Center) acudirá rápidamente a solucionar el problema.

El explorador Norton AntiVirus, *Bloodhound*, se ejecuta subordinado, para examinar y clasificar el comportamiento de las aplicaciones que pueden estar infectadas con nuevos virus. Si una aplicación se comporta como un virus e intenta infectar a otros programas, Bloodhound puede detener el programa, evitando que los demás archivos se infecten, hasta que usted reciba nuevas actualizaciones de antivirus.

Los productos de Norton AntiVirus Solution Release 3.04 proporcionados en FirstSecure son:

- Soluciones de escritorio:
  - Norton AntiVirus 4.08 para DOS
  - Norton AntiVirus 4.08 para Windows 3.51
  - Norton AntiVirus 5.02 para Windows 95/98
  - Norton AntiVirus 4.08 para Windows NT 3.51
  - Norton AntiVirus 5.02 para Windows NT 4.0
  - Norton AntiVirus 5.03 para Macintosh
  - Norton AntiVirus 5.02 para OS/2

- Soluciones de servidor:
  - Norton AntiVirus 4.08 para Windows NT 3.51
  - Norton AntiVirus 5.02 para Windows NT 4.0
  - Norton AntiVirus 4.04 para NetWare
  - Norton AntiVirus 2.0 para Lotus Notes™ y OS/2
  - Norton AntiVirus 1.52 para Microsoft Exchange
- Soluciones de pasarela:
  - Norton AntiVirus 1.02A para pasarelas de correo electrónico de Internet para NT
  - Norton AntiVirus 1.04 para cortafuegos
- Administración:
  - Norton System Center 3.1
  - Norton AntiVirus 5.03 para Macintosh Administrator
  - Norton AntiVirus Plus 5.0 para Tivoli Enterprise
  - Norton AntiVirus Plus 5.0 para Tivoli IT Director
  - Otras herramientas de administración, incluido Norton AntiVirus Network Manager (NAV32/NAVNETW) v3.01

Para obtener más información acerca de Norton AntiVirus, consulte el archivo contents.txt del directorio raíz del CD de Norton AntiVirus.

Nota: Aunque la documentación de Norton AntiVirus puede proporcionarle la manera de contactar con Symantec para obtener servicio técnico y soporte, si obtiene Norton AntiVirus Solution Release 3.04 como parte de SecureWay FirstSecure, deberá ponerse en contacto con IBM para obtener servicio técnico y soporte.

Para obtener los pasos de instalación detallados, consulte la documentación que acompaña a los productos específicos y los requisitos de hardware y software que encontrará en el Capítulo 13, “Consideraciones sobre la instalación de Intrusion Immunity y requisitos” en la página 69.

Capítulo 8. Planificación de Public Key Infrastructure en la red

El componente Trust Authority de Public Key Infrastructure proporciona a las aplicaciones de Internet un medio para autentificar a los usuarios y asegurar que las comunicaciones sean confidenciales. Basado en los estándares PKI (Public Key Infrastructure) para funciones de cifrado e interoperatividad, un sistema Trust Authority proporciona la infraestructura necesaria para emitir, publicar y administrar certificados digitales. Incluye:

- Soporte para plataformas de servidores IBM AIX y Microsoft Windows NT
- Una autoridad de registro, RA (Registration Authority), que maneja las tareas administrativas que requiere el registro de usuarios. Los siguientes son algunos de los tipos de tareas administrativas, las cuales se pueden implantar mediante procesos automatizados o mediante la toma de decisiones por parte de individuos:
  - Confirmar la identidad del usuario
  - Aprobar o rechazar las peticiones para obtener, renovar o revocar certificados
  - Validar que el usuario posea la clave privada asociada a la clave pública en un certificado
  - De acorde con las normas de un proceso de la empresa o de un perfil de certificado determinados, emitir determinados tipos de certificados para determinados tipos de usuarios

  La RA también edita información acerca de los certificados en un directorio integrado de claves públicas: el directorio IBM SecureWay LDAP.
- Una autoridad de certificación homologada, CA, (Certificate Authority). La CA:
  - Emite certificados digitales y genera pares de claves digitales que permiten autentificar los certificados
  - Soporta la duración completa del certificado, esto es, desde la emisión inicial hasta la renovación y anulación del certificado
  - La RA actualiza el directorio inmediatamente después de que se anule un certificado
  - Puede utilizar hardware de cifrado, como por ejemplo IBM SecureWay 4758 PCI Cryptographic Coprocessor y Smart Cards, para aumentar su posibilidad de protección de claves.
- Credential Central es una interfaz de registro basada en la Web que facilita la obtención de certificados del navegador, certificados del servidor y certificados para obtener determinados dispositivos, como por ejemplo, Smart Cards. Los administradores también pueden utilizar estos formularios de registro para realizar un registro previo de los usuarios finales de un certificado PKIX.

- El cliente Trust Authority, una interfaz Windows autónoma que permite que los usuarios obtengan, renueven y anulen los certificados PKIX sin utilizar un navegador Web.
- RA Desktop, una interfaz de administración basada en la Web que permite que el administrador responsable apruebe o rechace las peticiones de obtener, renovar o anular certificados.
- Un subsistema Audit que utiliza los códigos de autentificación de mensajes, los MAC, para asegurarse de que los sucesos que recibe de la RA y la CA de Trust Authority se puedan autentificar. Una opción configurable permite que la integridad de los registros de auditoría esté protegida cuando éstos se registren cronológicamente.
- Varias interfaces de administración para configurar el sistema, cambiar las contraseñas protegidas, las CA de certificados cruzados, comprobar la integridad de los registros cronológicos e iniciar y detener los componentes del sistema de forma segura.
- Una interfaz de programación de aplicaciones, API, que permite a los desarrolladores de aplicaciones escribir aplicaciones PKI personalizadas.
- Soporte de tiempo de ejecución integrado para IBM DB2 Universal Database. Existen diferentes bases de datos para los componentes IBM SecureWay Directory y RA, CA y Audit.

Despliegue de Trust Authority

Consulte la publicación *IBM SecureWay Trust Authority Up and Running* para obtener información detallada sobre planificación e instalación. Este manual contiene marcos hipotéticos y los pasos para la instalación en servidores Windows NT y en AIX.

Capítulo 9. Planificación de SecureWay Toolbox en la empresa

Deberá planificar la instalación de FirstSecure Toolbox en un entorno de desarrollo, no en la red. Compruebe las aplicaciones en su entorno de desarrollo antes de ponerlas a disposición de los usuarios externos.

Servicios de autorización

Los Servicios de autorización le permiten supervisar quién tiene autorización para acceder a su sitio Web. La autentificación está basada en contraseñas o claves públicas. Estas medidas protegen la integridad y la confidencialidad de los datos en su sitio. Los servicios de autorización crean listas de control de acceso, ACL, que definen quién puede acceder a objetos del sitio y cómo pueden acceder a dichos objetos. Los servicios de autorización también permiten definir objetos protegidos y crear contraseñas para inicios de sesión individuales. Todas estas herramientas de seguridad están centralizadas para facilitar la gestión de las políticas de seguridad. Los servicios de autorización están soportados por las API de autorización de IBM SecureWay Policy Director.

Servicios de autorización de certificados

Los servicios de autorización de certificados están soportados por X.509 Public Key Infrastructure para múltiples plataformas y IBM KeyWorks Toolkit.

Los servicios de autorización de certificados le permiten asegurar la seguridad a través de la gestión de certificados digitales. Estos servicios incluyen las API para la duración completa de estos certificados, esto es, emisión, renovación y anulación. También publican listas de anulación de certificados. Las API utilizan la tecnología de cifrado de claves públicas y Smart Card como un medio de autentificar a los usuarios de certificados.

X.509 Public Key Infrastructure para múltiples plataformas, conocido también como PKIX, se proporciona a través de las API de PKIX. Estas API permiten crear, gestionar, almacenar, distribuir y anular certificados a través de los componentes de entidad final, EE (End Entity), autoridad de certificación, CA (Certificate Authority), y de autoridad de

registro, RA (Registration Authority). Las API están habilitadas como interfaz con IBM SecureWay Trust Authority, y están basadas en IBMKeyWorks.

Para obtener información acerca de las API PKIX, consulte la publicación *IBM SecureWay X.509 Public Key Infrastructure for Multiplatforms Programming Guide and Reference*. Para obtener más información acerca de IBM KeyWorks, consulte el Capítulo 16, “Documentación que se proporciona con FirstSecure” en la página 89 donde encontrará una lista de la documentación que se proporciona con Toolbox.

Servicios de directorio

IBM SecureWay Directory Client da soporte a los servicios de directorio.

Los servicios de directorio utilizan Lightweight Directory Access Protocol (LDAP) para organizar, controlar y acceder a los directorios. Estos servicios están basados en un modelo cliente/servidor que proporciona a los clientes acceso a un servidor LDAP. Los servicios de directorio proporcionan un medio de mantener la información sobre directorios en una ubicación central para su almacenamiento, actualización, recuperación e intercambio. Los servicios de directorio utilizan SSL (Secure Sockets Layer) para cifrar la información.

Para obtener más información acerca de los servicios de directorio, consulte el Capítulo 16, “Documentación que se proporciona con FirstSecure” en la página 89 para obtener una lista completa de la documentación de IBM SecureWay Directory Client que se proporciona con Toolbox.

Servicios de cifrado y de gestión de fiabilidad KeyWorks

IBM KeyWorks Toolkit, al que también se hace referencia como KeyWorks, da soporte a los servicios de cifrado y de gestión de fiabilidad.

Los servicios de cifrado y de gestión de fiabilidad KeyWorks cifran y descifran la información para controlar quién tiene acceso a dicha información. Estos servicios crean y verifican las signaturas digitales para autentificar las identidades de los individuos y sistemas en la red. En IBM Key Recovery Service Provider se ha incorporado un sistema de recuperación de claves que permite recuperar la información cifrada, sin distribuir la clave.

KeyWorks es un kit de herramientas de servicios de cifrado y de gestión de fiabilidad. Está compuesto por un conjunto de capas de servicios de seguridad y de interfaces de programación asociadas que forman un conjunto integrado de posibilidades de seguridad para la información y las comunicaciones. Cada capa presenta servicios más fundamentales que los que posee la capa inmediatamente inferior. Estas capas comienzan por contener componentes fundamentales, como por ejemplo, algoritmos de cifrado, números aleatorios e información de identificación exclusiva en las capas inferiores, y va aumentando sus componentes a certificados digitales, mecanismos de gestión de claves y recuperación y protocolos de transacción protegidos.

KeyWorks está habilitado para el Soporte del idioma nacional (NLS), lo cual significa que el producto no depende de ningún idioma, script, cultura ni juego de caracteres codificados.

Para obtener más información acerca de las API de KeyWorksC, consulte el Capítulo 16, “Documentación que se proporciona con FirstSecure” en la página 89 para obtener una lista de la documentación de KeyWorks que se proporciona con Toolbox.

Servicios de protocolo SSL

Los servicios de protocolo SSL (Secure Sockets Layer) están soportados por IBMSecure Sockets Layer (SSL) Toolkit.

Los servicios de protocolo SSL le permiten decidir quién tiene acceso a sus datos. Estos servicios cifran datos mediante claves públicas y privadas para diferentes fines, incluida la autentificación de usuarios, la prevención de accesos de clientes no autorizados y la prevención de la manipulación de los datos. Se puede controlar a quién se le emiten certificados, por lo tanto, se puede controlar a quién se le permite el acceso a los datos. La tecnología SSL está incorporada en otras API para cifrado de datos y creación de contraseñas.

Parte 3. Consideraciones sobre la instalación y la integración

Esta sección describe de qué modo se ajustan entre sí los diferentes componentes. Lista los requisitos de hardware y software para cada producto y cualquier aplicación o producto de base de datos que sea necesario.

Capítulo 10. Planificación de la instalación de FirstSecure

Antes de instalar los productos componentes de FirstSecure, lea los siguientes apartados para asegurarse de que tiene el hardware y software necesarios. Puede encontrar información sobre las actualizaciones más recientes de FirstSecure en www.ibm.com/software/security/firstsecure . Antes de instalar los productos consulte en el sitio Web las últimas actualizaciones.

Las instrucciones detalladas para instalar y configurar los productos integrantes de FirstSecure se proporcionan con la documentación del producto que acompaña a cada producto integrante.

Requisitos generales del sistema

Esta sección describe los requisitos globales del sistema para los productos FirstSecure. Para obtener los requisitos de hardware y software de cada uno de los productos integrantes, consulte la información referente al producto específico.

Para instalar los componentes de FirstSecure, necesitará un hardware que pueda ejecutar uno de los siguientes sistemas operativos de servidor:

- Microsoft Windows NT Versión 4 con Service Pack 5.
- AIX Versión 4.3.1 o superior.
- Sun Solaris Versión 2.6 o superior.

  Nota: En Solaris, Toolbox requiere Sun Solaris Versión 2.6 con el Fix Pack de Mayo de 1999.

Cada uno de los productos componentes de FirstSecure se ejecuta en, como mínimo, uno de estos sistemas operativos. El apartado correspondiente a cada producto componente muestra las plataformas de sistema operativo soportadas y otros prerrequisitos de software para cada producto componente. Para dichos sistemas operativos necesitará servidores, consolas de gestión y sistemas cliente. Los siguientes apartados ofrecen una visión general de dichos requisitos.

Requisitos del sistema operativo para servidores y clientes

Consulte en la Tabla 1 los requisitos del sistema operativo para los productos SecureWay.

Tabla 1. Requisitos del sistema operativo para servidores y clientes

Sistema operativo	Nivel mínimo de servidor	Nivel mínimo de cliente
Windows NT	Versión 4.0, Service Pack 5	Versión 4.0, Service Pack 5
IBM AIX	Versión 4.3.1	Versión 4.3.1
Sun Solaris	Versión 2.6	Versión 2.6
Windows 95	N/A	Se da soporte a todas las versiones
Windows 98	N/A	Se da soporte a todas las versiones
Windows 3.1 (sólo Norton AntiVirus)	N/A	Se da soporte a todas las versiones
IBM OS/2 (sólo Norton AntiVirus)	N/A	Versión 4.0, FixPak 6 o superior

Detalles y requisitos de los productos integrantes

En los apartados siguientes se indican los requisitos de hardware y software para los productos componentes de FirstSecure. Los capítulos siguientes describen detalladamente cada uno de los componentes y listan los requisitos de hardware y software de cada uno de éstos. Los capítulos también ofrecen una visión general de la instalación y configuración de cada producto, incluidos los temas relacionados con la integración con los demás componentes.

- Capítulo 11, “Consideraciones sobre la instalación de Policy Director y requisitos” en la página 59
- Capítulo 12, “Consideraciones sobre la instalación de SecureWay Boundary Server y requisitos” en la página 61
- Capítulo 13, “Consideraciones sobre la instalación de Intrusion Immunity y requisitos” en la página 69
- Capítulo 14, “Consideraciones sobre la instalación de Public Key Infrastructure y requisitos” en la página 77
- Capítulo 15, “Consideraciones sobre la instalación de Toolbox y requisitos” en la página 83

Capítulo 11. Consideraciones sobre la instalación de Policy Director y requisitos

Este capítulo lista los requisitos de hardware y software para Policy Director. También ofrece las consideraciones sobre la instalación relacionadas con la integración con otros productos FirstSecure.

Requisitos de hardware y software de Policy Director

La Tabla 2 lista los requisitos de hardware de Policy Director.

Tabla 2. Requisitos de hardware de Policy Director

Plataforma	Espacio mínimo en disco	Memoria mínima
Windows NT Server: Intel 80486 o compatible a 133 MHZ o superior	16 MB	64 MB
Servidor AIX: hardware que ejecute AIX 4.3.1	16 MB	64 MB
Servidor Solaris: hardware que ejecute Solaris 2.6	16 MB	64 MB

Los requisitos de software para los componentes de Policy Director son:

Servidores Policy Director

- Windows NTServer Versión 4.0, Service Pack 5
- AIX Versión 4.3.1
- Sun Solaris, Versión 2.6

Clientes NetSEAT

- Windows NT Server Versión 4.0, Service Pack 5
- Windows 95
- Windows 98

Management Console

- Windows NT Workstation
- Windows NT Server Client
- AIX Versión 4.3.1 Client

- Sun Solaris, Versión 2.6 Client

Policy Director requiere otro software, el cual se incluye en el paquete. Siga las indicaciones de la publicación *IBM SecureWay Policy Director Up and Running* para instalar el software que necesita para el despliegue de Policy Director.

Consideraciones acerca de la instalación de Policy Director

En www.ibm.com/software/security/policy se listan las actualizaciones de los prerrequisitos de software actuales para Policy Director.

Integración de Policy Director y Trust Authority

IBM SecureWay Trust Authority proporciona funciones de autentificación comprobando que cada usuario es quien pretende ser. Trust Authority emite certificados a los usuarios basándose en la información de IBM SecureWay Directory, denominado a veces Lightweight Directory Access Protocol o LDAP.

Policy Director, a su vez, utiliza estos certificados y otorga autorización comprobando que cada uno de los usuarios únicamente tenga acceso a los recursos permitidos. Policy Director almacena la información del mismo modo que IBM SecureWay Directory.

Su entorno e-business puede tener una sola definición de usuario con todos los permisos de Policy Director y toda la información de Trust Authority. Si también almacena información de SecureWay Boundary Server en IBM SecureWay Directory, Policy Director también puede gestionarla.

Capítulo 12. Consideraciones sobre la instalación de SecureWay Boundary Server y requisitos

Este capítulo lista los requisitos de hardware y software para SecureWay Boundary Server. También ofrece las consideraciones sobre la instalación relacionadas con la integración con otros productos SecureWay Boundary Server.

Requisitos de hardware y software de SecureWay Boundary Server

Los requisitos de hardware de los productos que componen SecureWay Boundary Server se muestran en la Tabla 3 en la página 62 y en la Tabla 4 en la página 63.

Tabla 3. Requisitos de hardware para los productos que componen SecureWay Boundary Server

Componente de SecureWay Boundary Server	**Tipo de máquina**	**Espacio en disco**	**Memoria**	**Otros**
IBM SecureWay Firewall[1]	NT: Pentium® 133 MHz o superior AIX: Máquina RS/6000 que soporte AIX 4.3.2	NT: 24 MB[2] AIX: 307 MB	NT: 64 MB AIX: 64 MB	2 tarjetas de interfaz de red
ACE/Server	NT: Pentium 166 MHz o superior (solamente los de un solo procesador) AIX: Máquina que soporte AIX 4.2	Software de servidor principal: 50 MB Servidor de reserva: 22 MB Base de datos de usuario inicial: 4 MB Instalación: 240 MB	Mínimo: 32 MB	Los requisitos reales de almacenamiento están basados en el número de usuarios
SurfinGate				
Servidor	Pentium 233 MHz o superior	20 MB	Mínimo: 128 MB Recomendado: 256 MB	
Consola	Pentium 233 MHz o superior	15 MB	Mínimo: 32 MB Recomendado: 64 MB	
MIMEsweeper para IBM SecureWay Release 2				
MAILsweeper	Pentium 200 MHz o superior	1 GB	64 MB	1 tarjeta de interfaz de red
WEBsweeper	Pentium 400 MHz o superior	1 GB	128 MB + 1 MB para cada conexión Web simultánea	1 tarjeta de interfaz de red

Notas:

1. Consulte la documentación que se incluye en IBM Firewall para obtener una información más detallada.
2. También se requieren 13 MB de espacio de disco para el navegador Netscape.

Tabla 4. Requisitos de software para los productos que componen SecureWay Boundary Server

Componente SecureWay Boundary Server	**Plataformas Microsoft Windows**		**AIX**	**Solaris**
	Cliente	**Servidor**	**Servidor**	**Servidor**
IBM SecureWay Firewall	Windows 95, cliente IPSec	Windows NT Server Versión 4.0, Service Pack 5[1]	AIX 4.3.2	No disponible
ACE/Server	Windows NT Workstation 4.0, Service Pack 2 o superior	Windows NT Server Versión 4.0, Service Pack 5 o superior	AIX 4.2	Solaris 2.5.1
SurfinGate 4.05				
Servidor	No disponible	Windows NT 4.0[2]	No disponible	No disponible
Consola	Windows NT 4.0 o superior [2] Windows 95, Windows 98	No disponible	No disponible	No disponible
MIMEsweeper para IBM SecureWay Release 2				
MAILsweeper	No disponible	Windows NT 4.0[3]	No disponible	No disponible
WEBsweeper	Windows NT Workstation 4.0, Service Pack 3 o superior	Windows NT 4.0[4]	No disponible	No disponible

Notas:

1. Consulte la documentación que se proporciona con IBM Firewall para Windows NT para obtener información acerca de los arreglos necesarios.
2. Además:
   - Se requiere el cliente de red Windows para Microsoft Windows.
   - No se da soporte a Windows NT Workstation.
3. Además:
   - No se da soporte a NT 3.5.1 ni Windows NT Workstation.
   - Se requiere uno de los siguientes entornos:
     - Microsoft Exchange
     - SMTP
     - cc:Mail™
     - Groupwise
     - Lotus Notes
4. Consulte el apartado “Consideraciones acerca de MIMEsweeper” en la página 67 para obtener las recomendaciones para MIMEsweeper.

Consideraciones sobre el componente SecureWay Boundary Server

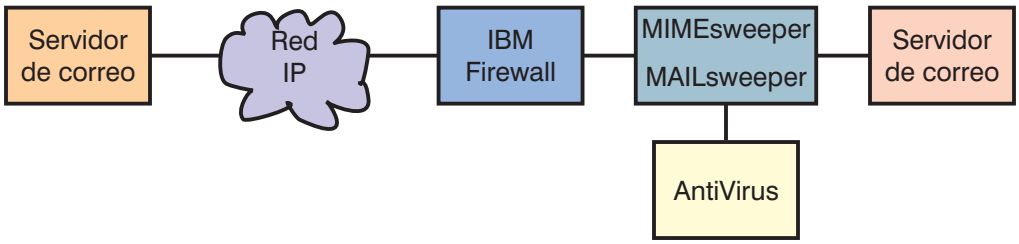
Las secciones siguientes describen las consideraciones sobre la instalación y configuración de los productos del componente SecureWay Boundary Server.

Consideraciones acerca de IBM Firewall

Las consideraciones para IBM Firewall principalmente requieren conocer en qué lugar de la corriente de tráfico en relación con los demás productos SecureWay Boundary Server piensa instalarlo.

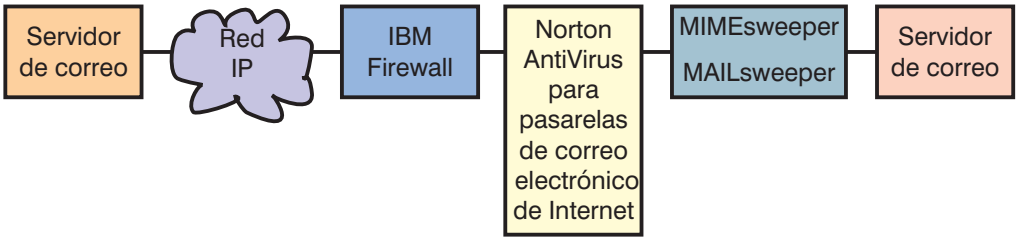
Configuraciones de ejemplo

Configuración de ejemplo de IBM Firewall y MAILsweeper: Cuando instala IBM Firewall y MIMEsweeper, puede utilizar la configuración que se describe en esta sección.



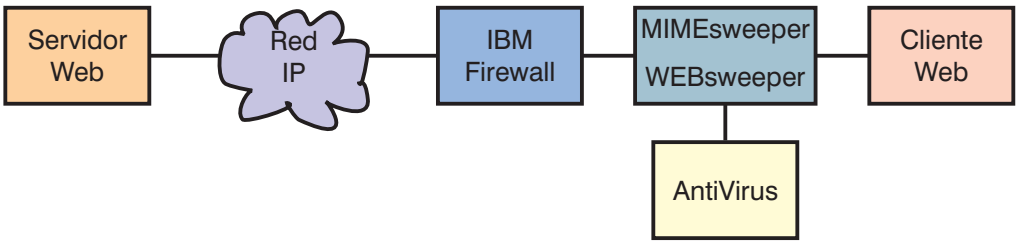
- MAILsweeper es la parte de MIMEsweeper que comprueba el contenido de los mensajes de correo. MAILsweeper tiene una función para habilitar las comprobaciones antivirus.
- MAILsweeper se ubica entre IBM Firewall y los servidores SMTP seguros.
- IBM Firewall utiliza MAILsweeper como sistema principal de correo para reenviar el correo.
  - IBM Firewall requiere que se hayan establecido las reglas de correo predefinidas para poder permitir el flujo del tráfico.
- Los servidores SMTP también deben indicar que MAILsweeper es el sistema principal de correo para el reenvío de correo.
- MAILsweeper comprueba el contenido de los mensajes de correo reenviados que fluyen en ambas direcciones.

Configuración de ejemplo de IBM Firewall, Norton AntiVirus para pasarelas de correo electrónico de Internet y MIMEsweeper: Si va a instalar IBM Firewall, Norton AntiVirus para pasarelas de correo electrónico de Internet y MIMEsweeper, puede utilizar la configuración que se describe en este apartado. En este caso hipotético se combina IBM Firewall, Norton AntiVirus para pasarelas de correo electrónico de Internet y MAILsweeper en una cadena para comprobar los virus y el contenido del correo, tal como se ilustra en el siguiente diagrama.



- El cortafuegos utiliza Norton AntiVirus para pasarelas de correo electrónico de Internet como servidor seguro de correo. Para permitir este tráfico específico, deben haberse establecido las reglas correctas de cortafuegos.
- Norton AntiVirus para pasarelas de correo electrónico de Internet apunta a MAILsweeper como sistema de reenvío de correo para el correo seguro y el cortafuegos para el correo destinado al exterior.
- MAILsweeper recibe y comprueba el correo que ha recibido. A continuación, lo envía al servidor correspondiente, en función de sus tablas de direccionamiento o de las búsquedas de registro MX. Si MAILsweeper y Norton AntiVirus para pasarelas de correo electrónico de Internet se encuentran en la misma máquina, debe cambiar el puerto receptor para MAILsweeper a fin de evitar conflictos con Norton AntiVirus para pasarelas de correo electrónico de Internet.

Configuración de ejemplo de IBM Firewall y WEBsweeper: Si instala IBM Firewall y MIMEsweeper, puede utilizar la configuración que se describe en este apartado.



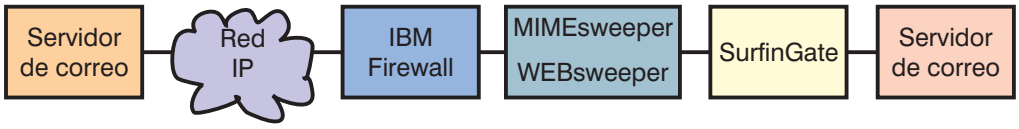
- WEBsweeper es la parte de MIMEsweeper que comprueba el tráfico de tipo Web. WEBsweeper tiene una función para habilitar las comprobaciones antivirus.
- WEBsweeper actúa como un proxy intermedio. Los clientes utilizan WEBsweeper como su proxy. A continuación, WEBsweeper se define para reenviar el tráfico al proxy del cortafuegos.

- Deben haberse configurado reglas en el cortafuegos para permitir el tráfico del proxy.
- La peticiones de proxy sólo pueden provenir de la red segura que se encuentra detrás del cortafuegos.
- WEBsweeper no maneja HTTPS. Para utilizar HTTPS, debe eludir WEBsweeper a fin de evitar problemas con el cortafuegos y garantizar que se comprueba todo el tráfico de tipo Web. Debe apuntar directamente al proxy del cortafuegos. El tráfico tipo Web sigue siendo seguro, pero WEBsweeper no lo comprueba.

Configuración de ejemplo de IBM Firewall y SurfinGate: Si instala IBM Firewall y SurfinGate, puede utilizar la configuración que se describe en este apartado.

- SurfinGate comprueba si hay controles ActiveX u otros elementos en el tráfico de tipo Web.
- SurfinGate actúa como un proxy Web intermedio. Los clientes utilizan SurfinGate como proxy para HTTP, FTP y HTTPS. A continuación, SurfinGate reenvía la petición al proxy de IBM Firewall.
- Deben haberse configurado reglas en el cortafuegos para permitir el tráfico del proxy.
- La peticiones de proxy sólo pueden provenir de la red segura que se encuentra detrás del cortafuegos.

Configuración de ejemplo de IBM Firewall, MIMEsweeper y SurfinGate: Si instala IBM Firewall, MIMEsweeper y SurfinGate, puede utilizar la configuración que se describe en este apartado.



- SurfinGate comprueba si hay controles ActiveX u otros elementos en el tráfico de tipo Web. Utiliza comprobaciones diferentes que el componente WEBsweeper de MIMEsweeper.
- SurfinGate y WEBsweeper actúan como proxys Web intermedios. Los clientes apuntan a SurfinGate como su proxy para HTTP y FTP. A continuación, SurfinGate reenvía la petición a WEBsweeper. WEBsweeper reenvía la petición al proxy de IBM Firewall.

- Deben haberse configurado reglas en el cortafuegos para permitir el tráfico del proxy. Estas reglas están definidas en la publicación *IBM eNetwork Firewall Versión 3.3 para Windows NT Guía del usuario*.
- La peticiones de proxy sólo pueden provenir de la red segura que se encuentra detrás del cortafuegos.
- WEBsweeper no maneja HTTPS. Al utilizar HTTPS, para evitar problemas con el cortafuegos y a fin de garantizar que se comprueba todo el tráfico de tipo Web, debe saltarse WEBsweeper. Debe apuntar directamente al proxy del cortafuegos. El tráfico tipo Web sigue siendo seguro, pero WEBsweeper no lo comprueba.

Consideraciones acerca de MIMEsweeper

El siguiente es un sistema WEBsweeper típico:

- Un procesador Intel Pentium 400 MHz o superior
- 1 GB de espacio de disco y 128 MB de RAM
- Windows NT Server o Workstation Versión 4.0 Server Service Pack 3 o superior
- Protocolo TCP/IP, incluido un sistema principal y un nombre de dominio
- Herramientas antivirus

El siguiente es un entorno WEBsweeper típico de alto volumen de hasta 500 usuarios simultáneos:

- Un Intel Pentium II, 450 MHz o superior dual
- 3 GB de espacio de disco y 256 MB de RAM
- Windows NT Server o Workstation Versión 4.0 Server Service Pack 3 o superior
- Protocolo TCP/IP, incluido un sistema principal y un nombre de dominio
- Herramientas antivirus

Si el entorno soporta más de 500 usuarios simultáneos, entonces se recomienda utilizar varios servidores WEBsweeper.

Capítulo 13. Consideraciones sobre la instalación de Intrusion Immunity y requisitos

Este capítulo lista los requisitos de hardware y software para los componentes de Intrusion Immunity, Tivoli Cross-Site for Security y Norton AntiVirus.

Requisitos de hardware y software de Intrusion Immunity

En el siguiente apartado se describe la documentación de instalación y configuración para los productos del componente Intrusion Immunity.

Los requisitos de hardware y software para Tivoli Cross-Site for Security se muestran en la Tabla 5 en la página 70, la Tabla 6 en la página 70 y la Tabla 7 en la página 71. Los requisitos de hardware y software para los productos del componente Norton AntiVirus se muestran en la Tabla 8 en la página 71 y en la Tabla 9 en la página 72.

Tabla 5. Requisitos de hardware y software para los servidores Tivoli Cross-Site for Security	
Requisitos del servidor	
Sistema operativo	• AIX 4.3.2 • Windows NT Versión 4.0, Service Pack 5 • Solaris 2.5.1 ó 2.6
Java	JDK 1.1.6 revisión 04 o superior
Servidor Web	Netscape Enterprise Server 3.51
Base de datos	• IBM DB2 Release 5.2 • Oracle 7.3.4 (o 8.0.4 recomendado) • Microsoft SQL Server
Espacio en disco	• Windows NT 290 MB • AIX 180 MB • Solaris 180 MB
Memoria	256 MB
Espacio de intercambio	300 MB (400 MB recomendados)
Notas: 1. No se da soporte a Netscape Enterprise Server 3.51 y 3.6. 2. Consulte los requisitos de parche para Solaris en la documentación de instalación de Tivoli Cross-Site for Security.	

Tabla 6. Requisitos de hardware y software para la consola de gestión Tivoli Cross-Site for Security	
Requisitos de Management Console	
Sistemas operativos	• Windows 95 • Windows 98 • Windows NT Versión 4.0, Service Pack 5 (máquina de 166 MHz o superior recomendada) • Solaris 2.5.1 ó 2.6 ejecutándose en Sun SPARC
Espacio en disco	25 MB para todas las plataformas
Memoria	• Windows NT 40 MB • AIX 64 MB • Solaris 40 MB

Tabla 7. Requisitos de hardware y software para agentes Tivoli Cross-Site for Security

Requisitos de Security Agent	
Sistemas operativos	• Windows NT Versión 4.0, Service Pack 5 o superior • AIX 4.3.2 • Solaris 2.5.1 ó 2.6 ejecutándose en Sun SPARC
Java	JDK 1.1.6 revisión 04 o superior, en Solaris (necesario sólo para UNIX)
Espacio en disco	• 15 MB en Windows NT • 10 MB en AIX • 10 MB en Solaris
Memoria	• 32 MB en Windows NT • 32 MB en AIX • 20 MB en Solaris

Notas:

1. No se da soporte a Netscape Enterprise Server 3.51 y 3.6.
2. Consulte los requisitos de parche para Solaris en la documentación de instalación de Tivoli Cross-Site for Security.

La Tabla 8 lista los requisitos de hardware para Norton AntiVirus.

Tabla 8. Requisitos de hardware para Norton AntiVirus.

Componente de Intrusion Immunity	**Tipo de máquina**	**Espacio en disco**	**Memoria**	**Otros**
Norton AntiVirus	CPU Intel	24 MB	Mínimo: 16 MB Recomendado: 32 MB	Unidad de CD-ROM
Norton AntiVirus para pasarelas de correo electrónico de Internet	Pentium 133 o superior	6 MB	32 MB	Unidad de CD-ROM 500 MB - 5 GB para un eficaz funcionamiento del correo

Tabla 9. Requisitos de software para Norton AntiVirus			
Componente de Intrusion Immunity	**Plataformas Microsoft Windows**		**OS/2**
	Cliente	**Servidor**	**Cliente**
Norton AntiVirus[1]	Windows NT 4.0 Windows 95, Windows 98	Windows NT 4.0	OS/2 2.11 o superior
Notas: 1. Además, se requiere una conexión Internet TCP/IP para Norton AntiVirus para pasarelas de correo electrónico de Internet.			

Norton AntiVirus no está disponible en AIX ni Solaris.

Consideraciones acerca de la instalación de Tivoli Cross-Site for Security

Las ilustraciones siguientes muestran las ubicaciones típicas de Cross-Site for Security Agent y Cross-Site for Security Management Server en una red de e-business.

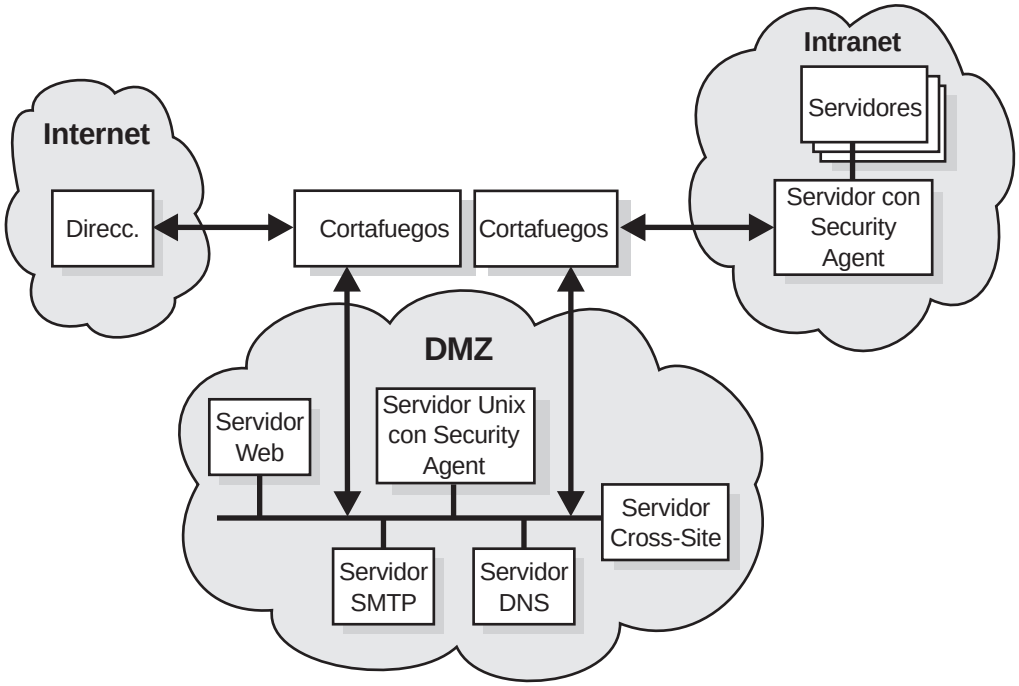


Figura 11. Instalación de Cross-Site for Security Management Server en la DMZ

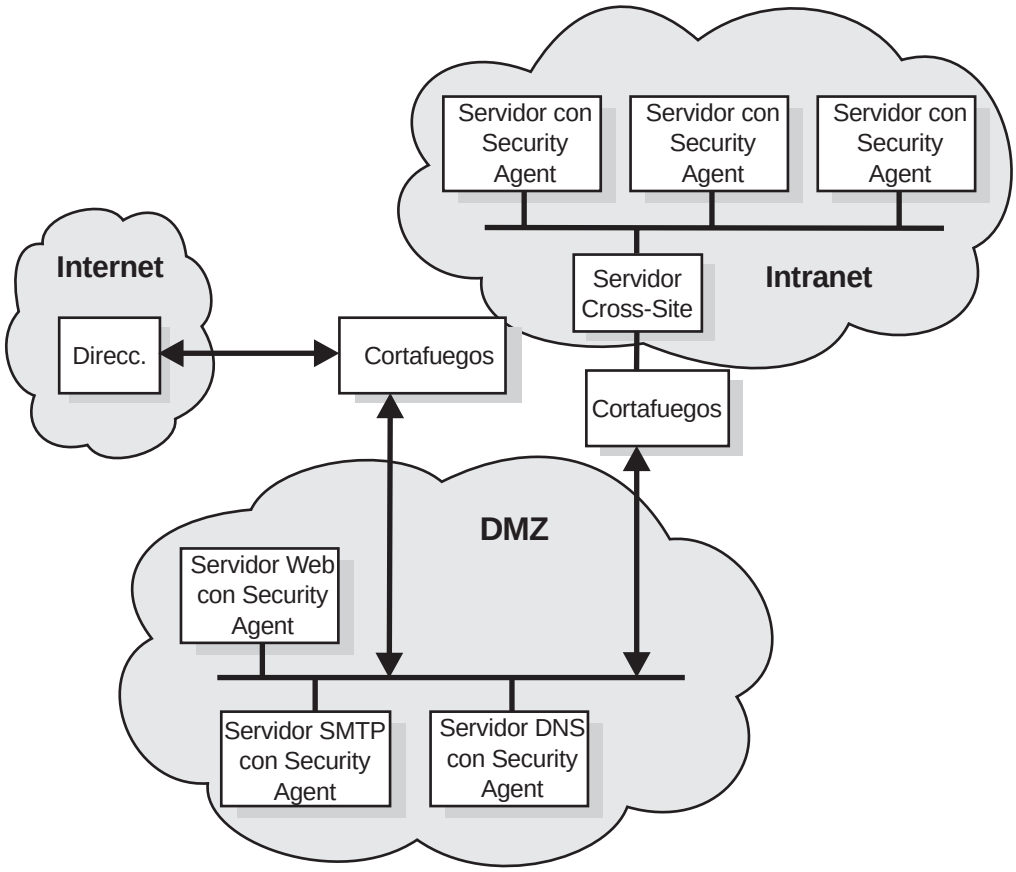


Figura 12. Instalación de Cross-Site for Security Management Server en la intranet

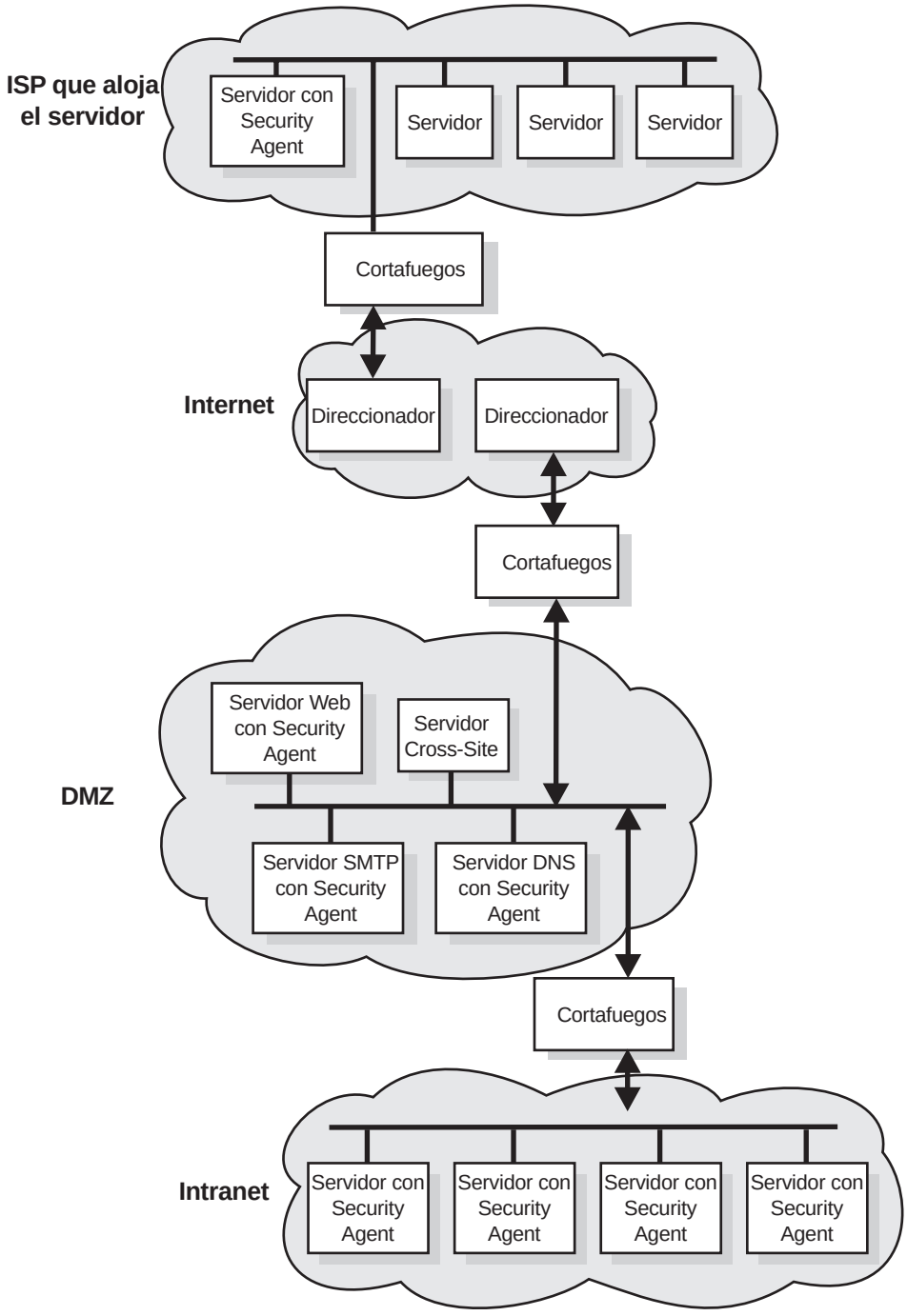


Figura 13. Instalación de Cross-Site for Security Management Server en la DMZ con soporte a un servidor conectado a Internet

Consideraciones acerca de la instalación de Norton AntiVirus

Para obtener información acerca de la instalación de Norton AntiVirus, consulte el archivo contents.txt que encontrará en el directorio raíz del CD del producto.

Capítulo 14. Consideraciones sobre la instalación de Public Key Infrastructure y requisitos

Actualmente las empresas necesitan una infraestructura de clave pública para proteger las aplicaciones de e-business, y FirstSecure Trust Authority proporciona dos niveles de funciones que implantan una infraestructura de clave pública:

- Gestión completa de la duración completa de los certificados digitales, con:
  - La posibilidad de solicitar, renovar y revocar certificados
  - Una autorización de registro para aprobar peticiones de certificado
  - Una autorización de certificado para crear certificados digitales y listas de anulación
- Posibilidades mejoradas de registro para que las empresas puedan registrar en línea sus entidades de e-business fiables. La aplicación de registro se basa en los siguientes principios:
  - Los certificados que se emiten y gestionan deben tener la fiabilidad requerida por las aplicaciones de e-business confidenciales, y la autorización de registro debe cumplir los mismos requisitos de fiabilidad y seguridad.
  - La aplicación debe proporcionar flexibilidad para dar soporte a diversas políticas de registro, incluidas las aprobaciones manuales o automáticas, la autentificación flexible interna o externa y la opción de aislar políticas de registro en dominios fiables separados.

El modelo de fiabilidad ayuda a garantizar la accesibilidad, confidencialidad, integridad y autoría de las transacciones electrónicas. Mediante el cifrado digital, la certificación y signaturas, Trust Authority permite realizar operaciones de e-business seguras a través de Internet, una intranet, o una VPN (Red privada virtual). Para una mayor seguridad de su clave de signatura, se ha diseñado la autoridad de certificación de modo que pueda funcionar con hardware de cifrado.

Requisitos de hardware y software del servidor Trust Authority

Los requisitos de software de servidor del componente Trust Authority se listan en la Tabla 10.

Tabla 10. Requisitos de software del servidor y hardware opcional para el componente Public Key Infrastructure de Trust Authority

Producto	**Notas**
Uno de los siguientes sistemas operativos: • IBM AIX/6000 (AIX), versión 4.3.2 • Microsoft Windows NT, versión 4.0 con Service Pack 5	• Necesario. • Debe instalar todos los programas de servidor Trust Authority en la misma plataforma. No se pueden combinar máquinas AIX y Windows NT en la misma configuración del sistema.
IBM SecureWay Directory Versión 3.1.1	• Necesario. Está integrado en el código de Trust Authority. • Durante la instalación de Trust Authority, puede instalar el software de Directory en la misma máquina en la que instala Trust Authority, o puede instalarlo en una máquina remota.
IBM WebSphere Application Server Versión 2.02, Standard Edition. Incluye IBM HTTP Server Versión 1.3.3 y Sun Java Development Kit (JDK) 1.1.7.	• Necesario. Se proporciona en el paquete de soportes físicos de Trust Authority. • Antes de instalar Trust Authority, debe instalar el software de servidor Web en la misma máquina en la que piensa instalar el software de servidor de Trust Authority y Trust Authority.
IBM DB2 Universal Database Enterprise Edition Versión 5.2 con el parche de mantenimiento 9.	• Necesario. Se proporciona en el paquete de soportes físicos de Trust Authority. • Existe una instancia de base de datos exclusiva para cada componente de servidor. Antes de instalar Trust Authority, debe instalar DB2 en cada máquina que piense utilizar como servidor Trust Authority.
• IBM SecureWay 4758 PCI Cryptographic Coprocessor, Modelo 001 • IBM SecureWay 4758 CCA Support Program, Versión 1.3.0.0 con el parche de mantenimiento 1.3.0.1	• *Opcional*, y únicamente disponible para los sistemas AIX. Este producto se debe solicitar mediante los mecanismos normales para realizar pedidos IBM. • Antes de instalar Trust Authority, debe instalar el hardware 4758 y el programa de soporte en el servidor en el que piense instalar la CA de Trust Authority. • La 4758 Cryptographic Card requiere un bus PCI en el sistema RS/6000.

La Tabla 11 en la página 79 y la Tabla 12 en la página 80 listan los requisitos de hardware para Trust Authority.

En la Tabla 11 y en la Tabla 12 en la página 80:

- Un entorno de producción pequeño emite cientos de certificados diariamente.
- Un entorno de producción de tamaño medio emite miles de certificados diariamente.
- Un entorno de producción de gran tamaño emite muchos miles de certificados diariamente. También puede ser un sistema que proporcione servicios CA de terceros a otras organizaciones.

Si piensa ejecutar Trust Authority bajo Windows NT, IBM le recomienda que lo instale en un servidor IBM Netfinity®. La tabla siguiente proporciona las recomendaciones en cuanto a las dimensiones del sistema que están basadas en el número de certificados que espera emitir a través de una autoridad de certificación, CA, de Trust Authority.

Tabla 11. Configuraciones de máquinas Windows NT de ejemplo

Tipo de máquina	**Procesadores**	**Espacio en disco**	**Memoria**
Entorno de producción pequeño			
Netfinity 3000	1 (450 MHz, Pentium II)	2 unidades (9,1 GB)	256 MB
Netfinity 5000	2 (450 MHz, Pentium II)	2 unidades (9,1 GB)	512 MB
Entorno de producción de tamaño medio			
Netfinity 3000	1 (500 MHz, Pentium III)	4 unidades (18,2 GB)	768 MB
Netfinity 5000	2 (500 MHz, Pentium III)	4 unidades (9,1 GB)	1 GB
Entorno de producción de gran tamaño			
Netfinity 5500	2 (450 MHz, Pentium III)	4 unidades (9,1 GB de alta velocidad)	1 GB
Netfinity 5500	4 (500 MHz, Pentium III Xeon con Caché L2 de 1024 K)	4 unidades (9,1 GB de alta velocidad)	1 GB
Netfinity 7000	2 (500 MHz, Pentium III con caché L2 de 512 K)	4 unidades (9,1 GB de alta velocidad)	1 GB
Netfinity 7000	4 (500 MHz, Pentium III Xeon con Caché L2 de 1024 K)	4 unidades (18,2 GB)	2 GB

Si piensa ejecutar Trust Authority bajo AIX, debe instalarlo en una máquina IBM RISC System/6000®. La tabla siguiente proporciona las recomendaciones en cuanto a las dimensiones del sistema que están basadas en el número de certificados que espera emitir a través de una autoridad de certificación, CA, de Trust Authority.

Tabla 12. Configuración de hardware de máquinas AIX de ejemplo

Tipo de máquina	Procesadores	Espacio en disco	Memoria
Entorno de producción pequeño			
F40	2 (233 MHz)	2 unidades (9,1 GB, Ultra 2 Fast Wide)	512 MB
Entorno de producción de tamaño medio			
F40	2 (233 MHz)	3 unidades (9,1 GB, Ultra 2 Fast Wide)	1 GB
Entorno de producción de gran tamaño			
F50	4 (332 MHz)	5 unidades (una de 9,1 GB, Ultra 2 Fast Wide, más cuatro de 9,1 GB, SSA)	2 GB
H50	4 (332 MHz)	5 unidades (una de 9,1 GB, Ultra 2 Fast Wide, más cuatro de 9,1 GB, SSA)	2 GB
R50	6 (200 MHz)	2 unidades (9,1 GB Ultra 2 Fast Wide)	1 GB
R50	8 (200 MHz)	5 unidades (una de 9,1 GB, Ultra 2 Fast Wide, más una 7133 SSA Rack con cuatro de 9,1 GB, SSA)	2 GB

Requisitos de hardware y software del cliente Trust Authority

IBM recomienda la siguiente configuración de las estaciones de trabajo para utilizar los formularios de incorporación del navegador y para ejecutar la aplicación Trust Authority Client.

- La siguiente configuración de las máquinas:
  - Procesador Intel 486 de 166 MHz con 32 MB de memoria, como mínimo (se recomienda un procesador Intel Pentium de 200 MHz con 64 MB de memoria como mínimo)
  - Tarjetas de gráficos
  - Pantalla de vídeo VGA, o mejor
  - Ratón o dispositivo de puntero compatible con el ratón
- Uno de los siguientes sistemas operativos:
  - Microsoft Windows 95

  - Microsoft Windows 98
  - Microsoft Windows NT, versión 4.0
- Uno de los siguientes navegadores Web:
  - Netscape Navigator o Netscape Communicator, Versión 3.0 o posterior
  - Microsoft Internet Explorer, Versión 4.0 o posterior, habilitado para Java.

Interacción entre IBM KeyWorks Toolkit e IBM SecureWay Trust Authority

No instale IBM KeyWorks Toolkit en el mismo servidor que IBM SecureWay Trust Authority.

Capítulo 15. Consideraciones sobre la instalación de Toolbox y requisitos

FirstSecure Toolbox es un conjunto de API que ayudan a desarrollar aplicaciones seguras para e-business.

- Servicios de autorización
- Servicios de certificado y gestión
- Servicios de directorio
- Servicios de protocolo SSL (Secure Sockets Layer)
- Servicios de cifrado y de gestión de fiabilidad KeyWorks
  - Las API de IBM Key Recovery Service Provider 1.1.3.0. IBM Key Recovery Service Provider permite recuperar la información cifrada.
  - IBM Key Recovery Server 1.1.3.0. IBM Key Recovery Server 1.1.3.0 es una aplicación que, mediante una petición autorizada, puede recuperar la información cifrada cuando las claves no están disponibles o se han perdido o dañado.

    Estos dos kits de herramientas proporcionan interfaces estándar que las aplicaciones pueden utilizar para invocar los servicios de seguridad críticos, junto con interfaces estándar que los proveedores de seguridad pueden utilizar para conectarse con el kit de herramientas. Las interfaces estándar están basadas en la arquitectura CDSA (Common Data Security Architecture). Estos kits de herramientas están disponibles en Windows NT, Solaris y AIX.

Requisitos de hardware y software de Toolbox

Los requisitos de hardware para Toolbox se listan en la Tabla 13.

Tabla 13. Requisitos de hardware para Toolbox

Plataforma	Espacio en disco	Memoria
Windows NT Versión 4.0, Service Pack 5	2 - 4 GB	64 MB
AIX 4.3.2	9,1 GB	1 GB
Sun Solaris, Versión 2.6 con el Fix Pak de Mayo 1999	4,2 GB	128 MB

Tabla 14. Requisitos de hardware para los productos componentes de Toolbox

Kit de herramientas	Tipo de máquina	Espacio en disco	Memoria
IBM KeyWorks Toolkit	Hardware que soporta productos que se ejecutan en: Windows NT Versión 4.0, Service Pack 5 o superior Windows 95 AIX 4.2 o superior Sun Solaris	50 MB	32 MB
IBM Key Recovery Service Provider	Hardware que soporta productos que se ejecutan en: Windows NT Versión 4.0, Service Pack 5 o superior Windows 95 AIX 4.2 o superior Sun Solaris	50 MB	32 MB

En la tabla siguiente se indican los requisitos de software para los productos componentes del Toolbox.

Tabla 15. Requisitos de software para los productos componentes de Toolbox

Componente Toolbox	Plataformas Microsoft Windows		AIX	Solaris
	Cliente	Servidor	Servidor	Servidor
IBM KeyWorks Toolkit	Windows NT Versión 4.0, Service Pack 5 o superior	Windows NT Versión 4.0, Service Pack 5 o superior Windows 95	AIX 4.2 o superior[1]	Sun Solaris
IBM Key Recovery Service Provider	Windows NT Versión 4.0, Service Pack 5 o superior [2] Windows 95	Windows NT Versión 4.0, Service Pack 5 o superior	AIX 4.2 o superior	Sun Solaris

Notas:

1. También se da soporte al cliente AIX.
2. Además, se requiere IBM KeyWorks Toolkit.

IBM KeyWorks Toolkit 1.1

IBM KeyWorks Toolkit 1.1 proporciona a los desarrolladores de aplicaciones un mecanismo ampliable, abierto y estándar para acceder a funciones de cifrado y otras funciones de seguridad en diferentes entornos operativos.

IBM KeyWorks Toolkit proporciona unas API (interfaz de programación de aplicaciones) estándar que las aplicaciones pueden utilizar para invocar a servicios de cifrado, de fiabilidad y seguridad fundamentales, así como interfaces estándar que los módulos incorporados de Service Provider pueden utilizan para interactuar con el kit de herramientas. Estas interfaces estándar están basadas en CDSA (Common Data Security Architecture), un estándar de Open Group desarrollado inicialmente por Intel™ Corporation y ampliado por IBM para conformar KeyWorks Toolkit. Cuando utiliza interfaces estándar:

- Su empresa puede seleccionar la implantación de cifrado y de fiabilidad que mejor se adapte a sus necesidades sin tener que realizar cambios en las aplicaciones que utilizan los servicios de seguridad.
- Aumenta la productividad de los programadores de middleware y de aplicaciones.

IBM KeyWorks Toolkit proporciona una capa de aislamiento entre las aplicaciones y el middleware, en forma de clase, funciones de cifrado y proveedores de servicio. El kit de herramientas contiene módulos conectores de infraestructura y de Service Provider.

Para las aplicaciones, la infraestructura proporciona la potente API CSSM (Common Security Services Manager) de CDSA de Intel Corporation. IBM ha ampliado la API CSSM añadiendo funciones de recuperación de claves. Cuando utiliza IBM KeyWorks Toolkit, su aplicación puede:

- Cifrar y descifrar información
- Verificar signaturas digitales para diversos propósitos
- Recuperar de directorios los certificados y listas de revocación de certificados
- Crear campos de recuperación de claves para la copia de seguridad de cifrado y la recuperación de claves
- Decidir si un certificado puede ser fiable, en función de los criterios establecidos por los programadores y diseñadores de sistemas según lo indicado por los usuarios

Normalmente, una empresa u OEM integra IBM KeyWorks Toolkit e IBM Key Recovery Service Provider Toolkit con aplicaciones y middleware de manera que pueden utilizarse las API CSSM en la infraestructura CSSM. El resultado de esta integración es un conjunto de aplicaciones y middleware de tiempo de ejecución para los servidores y clientes distribuidos por los entornos operativos. Los demás elementos de FirstSecure dependerán de IBM KeyWorks Toolkit para todos los servicios de cifrado y operaciones de política de fiabilidad.

Se aconseja que entre los que realicen la integración utilizando IBM KeyWorks Toolkit haya programadores o técnicos de sistemas con amplia experiencia en programación y diseño de cifrado así como en middleware e infraestructuras, o que se pueda contratar a integradores u OEM que posean esta experiencia.

Para los proveedores de servicio, la infraestructura proporciona la interfaz estándar SPI (Service Provider Interface), la CDSA de Open Group. IBM ha mejorado la SPI, añadiéndole funciones de recuperación de claves.

IBM KeyWorks Toolkit (SDK) incluye módulos conectores de Service Provider que dan soporte a estándares abiertos y certificados propietarios de claves públicas. Estos módulos incluyen PKCS NŒ11, funciones de cifrado BSAFE de RSA Data Security, certificados X.509V3, las políticas de fiabilidad de Entrust y Verisign y Lightweight Directory Access Protocol (LDAP). La infraestructura proporciona integración sólida de las funciones de cifrado, fiabilidad y seguridad proporcionadas por los módulos de Service Provider independientes.

IBM KeyWorks Toolkit puede proporcionar funciones de administración fundamentales, entre las cuales se incluyen:

- Protección contra la omisión de pasos esenciales en un proceso soportado por KeyWorks
- Verificación de que los módulos conectores de Service Provider no se han modificado antes de su uso
- Uso de los módulos conectores de Service Provider sólo a través de la infraestructura
- Soporte para la utilización de una política de cifrado y de fiabilidad específica de la empresa y del país

IBM KeyWorks Toolkit ofrece las siguientes ventajas a su empresa:

- Permite cambiar o sustituir módulos de Service Provider sin tener que volver a escribir las aplicaciones y el middleware
- Proporciona soporte sólido para el cifrado del hardware y la creación de signaturas digitales
- Da soporte a directorios LDAP y el estándar de signaturas DSA
- No requiere la utilización de ninguna autoridad de certificación en particular

Para obtener más información acerca de IBM KeyWorks Toolkit, consulte la publicación *IBM KeyWorks Toolkit Developer's Guide*.

Interacción entre IBM KeyWorks Toolkit e IBM SecureWay Trust Authority

No instale IBM KeyWorks Toolkit en el mismo servidor que IBM SecureWay Trust Authority.

IBM Key Recovery Service Provider Toolkit 1.1

IBM Key Recovery Service Provider 1.1.3.0, proporcionado en formato de kit de herramientas, es un módulo de Service Provider que utiliza las funciones estándar proporcionadas por IBM KeyWorks Toolkit. IBM Key Recovery Service Provider permite la recuperación de información cifrada almacenada y transmitida sin recopilar ni garantizar claves privadas y crear puntos de vulnerabilidad de cifrado.

Como IBM Key Recovery Service Provider utiliza las funciones estándar proporcionadas por IBM KeyWorks Toolkit, la función de recuperación de claves puede utilizarse con diferentes suministradores de cifrado, certificados estándar de varias autoridades de certificados, políticas fiables de Verisign y Entrust, y cualquier directorio al que se pueda acceder mediante LDAP. IBM Key Recovery Service Provider crea información de recuperación de claves en base a la clave de sesión asociada con la comunicación entre las partes correspondientes.

Encontrará más información acerca de IBM Key Recovery Service Provider en la publicación *Key Recovery Server Installation and Usage Guide*, que se incluye en el paquete de documentación de FirstSecure.

Capítulo 16. Documentación que se proporciona con FirstSecure

Cada producto componente incluido en FirstSecure tiene su propia documentación. En este capítulo se proporciona información sobre la documentación incluida con cada uno de los productos integrantes de FirstSecure.

Para los productos SecureWay FirstSecure, SecureWay Policy Director y SecureWay Boundary Server, se adjunta un paquete de soporte físicos y un paquete de documentación. Los paquetes de soportes físicos contienen los CD del producto, que se utilizarán para instalar los productos componentes de la oferta, y algunos de estos CD contienen documentación en línea. Los paquetes de documentación contienen manuales en copia impresa para los productos integrantes que los proporcionan. Consulte el apartado “Paquete de documentación de FirstSecure” en la página 98 donde se lista el contenido de los paquetes de documentación.

Policy Director

Junto con los productos que integran Policy Director se proporciona la documentación siguiente.

IBM SecureWay Policy Director Up and Running Contiene las instrucciones de instalación y configuración de IBM SecureWay Policy Director.

IBM SecureWay Policy Director Administration Guide Contiene instrucciones sobre cómo administrar IBM SecureWay Policy Director. Este manual se proporciona en formato PDF.

IBM SecureWay Policy Director Programming Guide and Reference Contiene las instrucciones sobre cómo escribir programas para IBM SecureWay Policy Director. Este manual se proporciona en formato PDF.

Léame (Readme) del producto Está información está disponible en la Web en la dirección www.ibm.com/software/security/policy

SecureWay Boundary Server

El manual siguiente describe los productos que integran SecureWay Boundary Server, sus requisitos y sus interacciones.

IBM SecureWay Boundary Server for Windows NT and AIX: Up and Running Un
: manual en copia impresa que describe los productos que integran SecureWay Boundary Server.

En los siguientes apartados se describe la documentación proporcionada con los productos integrantes de SecureWay Boundary Server.

IBM SecureWay Firewall

Toda la documentación de IBM Firewall se proporciona en copia software. IBM Firewall proporciona la siguiente documentación:

IBM SecureWay Firewall for AIX Setup and Installation
: Instrucciones para la instalación y configuración de IBM SecureWay Firewall para AIX.

IBM SecureWay Firewall for Windows NT Setup and Installation
: Instrucciones para la instalación y configuración de IBM SecureWay Firewall para Windows NT.

IBM SecureWay Firewall for AIX User's Guide
: Instrucciones para la instalación y configuración de IBM SecureWay Firewall para Windows NT.

IBM SecureWay Firewall for Windows NT User's Guide
: Información acerca de cómo utilizar IBM Firewall para Windows NT.

IBM SecureWay Firewall for Windows NT Reference
: Contiene material de consulta para utilizar IBM Firewall para Windows NT.

IBM SecureWay Firewall for AIX Reference
: Contiene material de consulta para utilizar IBM Firewall para AIX.

IBM SecureWay Firewall Problem Determination Guide for Windows NT and AIX
: Contiene instrucciones para la determinación de problemas.

IBM SecureWay Firewall VPN Client User's Guide
: Contiene instrucciones sobre cómo configurar y utilizar una VPN (Red privada virtual).

MIMEsweeper

MIMEsweeper incluye la siguiente documentación:

MIMEsweeper Administrator's Guide
: Contiene un apartado de notas del Release, seguido de información para el administrador, con información de planificación e instalación.

  Este manual se proporciona en formato HTML en el CD del producto. Puede visualizarlo en línea editando el archivo \DOC\MANUAL.HTM con un navegador Web.

MIMEsweeper Release Notes
: Contiene documentación actualizada, que incluye información para la instalación e instrucciones para visualizar la documentación en línea.

  Este manual se proporciona en formato HTML en el CD del producto. Puede visualizarlo en línea editando el archivo \DOC\RELNOTES.HTM con un navegador Web.

MIMEsweeper Configuration Editor Help
: Contiene información sobre la edición de los archivos de configuración de MIMEsweeper.

  Este documento se proporciona en formato HTML en el CD del producto.

SurfinGate

SurfinGate incluye la siguiente documentación en copia software:

SurfinGate Installation Guide
: Información sobre la instalación y configuración de los componentes de SurfinGate 4.05 en Windows NT. Además, se proporciona una versión en formato PDF de la publicación *SurfinGate Installation Guide* en el CD del producto en el siguiente archivo: \docs\install.pdf.

SurfinGate User Guide
: Información sobre la planificación y utilización de SurfinGate. Se proporciona una versión en formato PDF de la publicación *SurfinGate User Guide* en el CD del producto, en el siguiente archivo: \docs\manual.pdf.

SurfinGate 4.05 for Windows NT Release Notes
: Información sobre SurfinGate 4.05, incluidos los requisitos del sistema y las limitaciones del producto. Se proporciona una versión en formato PDF de *SurfinGate 4.05 for Windows NT Release Notes* en el CD del producto, en el siguiente archivo: \docs\relnotes.pdf.

SurfinGate for Windows NT/UNIX Solaris Release Notes, Appendix A
: Documento en línea que cubre los cambios realizados en SurfinGate. Este documento se proporciona en el CD del producto, en el siguiente archivo: \docs\rnappen.pdf.

Intrusion Immunity

En los siguientes apartados se describe la documentación proporcionada con el producto Intrusion Immunity.

Tivoli Cross-Site for Security

Tivoli Cross-Site for Security, Versión 1.1 incluye la siguiente documentación en formato PDF:

Tivoli Cross-Site for Security Installation Este documento ofrece información detallada sobre los requisitos de instalación y le guía por los pasos de instalación.

Tivoli Cross-Site for Security User's Guide Este documento ofrece una visión general del producto, las instrucciones sobre cómo utilizar la consola y realizar tareas, información de consulta, como por ejemplo, interfaces de línea de mandatos, archivos de configuración y un glosario. Se puede acceder a este documento en el CD-ROM del producto.

Norton AntiVirus

Norton AntiVirus incluye la siguiente documentación para los componentes soportados en FirstSecure. Todos los documentos, excepto el archivo contents.txt, se entregan en formato PDF en el CD de Norton AntiVirus. El archivo contents.txt es un archivo ASCII del CD del producto.

Documentación que contiene el CD de Norton AntiVirus Solution Release 3.04

El archivo del CD de Norton AntiVirus Solution Release 3.04 denominado \contents.txt lista toda la documentación que contiene el CD.

Soluciones de administración

Norton AntiVirus Solution Implementation Guide Consulte el archivo \docs\admin\navimp.pdf del CD del producto.

Norton AntiVirus Command-Line Scanner Consulte el archivo \docs\navc\navcugd.pdf del CD del producto.

Emergency Rescue Disk creation Consulte el archivo \navc\readme.txt del CD del producto.

Soluciones de servidor

Norton AntiVirus for Windows NT Server Administrator's Guide Consulte el archivo \docs\admin\navnts50.pdf del CD del producto.

Norton AntiVirus for NetWare User's Guide Consulte el archivo \docs\NAVNLM\NVN4.pdf del CD del producto.

Norton AntiVirus for Lotus Notes Installation Guide Consulte el archivo \docs\NAVNOTES\NAVNOTES.pdf del CD del producto.

Norton AntiVirus for Lotus Notes Installation Guide Consulte el archivo \docs\NAVNOTES\NAVNOTES.pdf del CD del producto.

Norton AntiVirus for OS/2 Lotus Notes Installation Guide Consulte el archivo \docs\NOTESOS2\NOTESOS2.pdf del CD del producto.

Norton AntiVirus for Microsoft Exchange Installation Guide Consulte el archivo \docs\NAVXCHNG\NAVXCHNG.pdf del CD del producto.

Soluciones de pasarela

Norton AntiVirus for Internet Email Gateway User's Guide Consulte el archivo \docs\navieg\navieg.pdf del CD del producto.

Norton AntiVirus for Firewalls Administrator's Guide Consulte el archivo \docs\navfw\navfw.pdf del CD del producto.

Soluciones de escritorio

Norton AntiVirus User's Guide for Windows 3.1/DOS Consulte el archivo \docs\navwks\nav4dusr.pdf del CD del producto.

Norton AntiVirus Reference Guide for Windows 3.1/DOS Consulte el archivo \docs\navwks\nav4dref.pdf del CD del producto.

Norton AntiVirus for Windows 95/98 User's Guide Consulte el archivo \docs\navwks\nav98usr.pdf del CD del producto.

Norton AntiVirus for Windows 95/98 Reference Guide Consulte el archivo \docs\navwks\nav98ref.pdf del CD del producto.

Norton AntiVirus for Windows NT User's Guide Consulte el archivo \docs\navwks\nav5nusr.pdf del CD del producto.

Norton AntiVirus for Windows NT Reference Guide Consulte el archivo \docs\navwks\nav5nref.pdf del CD del producto.

Norton AntiVirus v4.0 User's Guide for Windows NT Consulte el archivo \docs\351\navntugd.pdf del CD del producto.

Norton AntiVirus v4.0 Reference Guide for Windows NT Consulte el archivo \docs\351\navntref.pdf del CD del producto.

Norton AntiVirus User's Guide for OS/2 Consulte el archivo \docs\navos2\navos2ug.pdf del CD del producto.

Norton AntiVirus Distribution Guide for OS/2 Consulte el archivo \docs\navos2\navos2dg.pdf del CD del producto.

Norton AntiVirus for Macintosh User's Guide Consulte el archivo \docs\navmac\navmac.pdf del CD del producto.

Libros blancos del CD de Norton AntiVirus Solution Release 3.04: El CD también contiene libros blancos en el directorio \sarc. Todos los libros blancos tienen formato PDF.

Vídeos del CD de Norton AntiVirus Solution Release 3.04: El CD también contiene vídeos. Para visualizar un vídeo, debe tener un reproductor multimedia (Media Player) u otro programa con posibilidad de reproducir archivos .AVI. Los vídeos están en los archivos siguientes:

SARC \sarc\sarc.avi

About Viruses \sarc\aboutvir.avi

Norton AntiVirus: the Guided Tour \navtour\guided\demo32.exe

How to Respond When Norton AntiVirus Alerts You \navtour\alert\demo32.exe

A Tour of Norton System Center \nsctour\setup.exe

o, para ejecutarlo directamente desde el CD,

\nsctour\demo32.exe

Para obtener más información sobre la guía, consulte el archivo \ncstour\readme.txt

Trust Authority

La documentación del producto IBM SecureWay Trust Authority está disponible en formato PDF (Portable Document Format) y en formato HTML en el CD-ROM *Trust Authority Documentation*. Gran parte de esta información se ha traducido a los idiomas que soporta Trust Authority. Para obtener instrucciones sobre cómo acceder a una publicación en el idioma que desea, consulte el archivo *Readme (Léame)*. La versión más reciente del archivo *Readme (Léame)* siempre está disponible en la página Library (Biblioteca) del sitio Web de IBM SecureWay Trust Authority en la siguiente dirección: http://www.ibm.com/software/security/trust/library

La biblioteca Trust Authority incluye la documentación siguiente:

IBM SecureWay Trust Authority Up and Running Este manual es una visión general del producto. Lista los requisitos del producto, incluye los procedimientos de instalación y proporciona información acerca de cómo acceder a la ayuda en línea disponible para cada componente del producto. Además de estar

disponible en el CD-ROM *Documentation*, este manual se distribuye impreso con el producto.

IBM SecureWay Trust Authority System Administration Guide Este manual contiene información general acerca de cómo administrar el sistema Trust Authority. Incluye los procedimientos para iniciar y detener servidores, cambiar contraseñas, administrar la autoridad de certificación, realizar auditorías y ejecutar comprobaciones de la integridad de los datos.

IBM SecureWay Trust Authority Configuration Guide Este manual contiene información acerca de cómo utilizar el Asistente para la configuración para configurar un sistema Trust Authority. Se puede acceder a la versión HTML de esta guía mientras se visualiza la ayuda en línea para el Asistente.

IBM SecureWay Trust Authority Registration Authority Desktop Guide Este manual contiene información acerca de cómo utilizar RA Desktop para administrar certificados durante la duración completa del certificado. Se puede acceder a la versión HTML de esta guía mientras se visualiza la ayuda en línea para el Escritorio.

IBM SecureWay Trust Authority User's Guide Este manual contiene información acerca de cómo obtener certificados. Proporciona procedimientos para utilizar los formularios de registro a Trust Authority para solicitar certificados para navegadores, servidores y dispositivos. También muestra cómo registrarse previamente a los usuarios para un certificado PKIX y cómo utilizar Trust Authority Client para almacenar y administrar certificados PKIX. Puede acceder a la versión HTML de esta guía mientras visualiza la ayuda en línea para el cliente.

Toolbox

En los siguientes apartados se describe la documentación proporcionada con los productos integrantes de Toolbox.

Las API de Toolbox

Toda la documentación de Toolbox está disponible en el siguiente sitio Web: `www.ibm.com/software/security/firstsecure/library`. La documentación incluida es la siguiente:

IBM SecureWay Secure Sockets Layer Toolkit Programming Guide and Reference Proporciona una visión general de las API y de iKeyman. Define cada una de las API, su sintaxis y su utilización.

IBM SecureWay Directory Client SDK Programming Reference Incluye varios programas cliente de ejemplo LDAP y una biblioteca de clientes LDAP que proporciona a los servidores LDAP acceso a las aplicaciones. Se proporciona soporte para C y para Java.

IBM SecureWay Policy Director Programming Guide and Reference Define cada una de las API, su sintaxis y su utilización.

IBM SecureWay X.509 Public Key Infrastructure for Multiplatforms Installation Guide Ofrece instrucciones de instalación y los requisitos.

IBM SecureWay X.509 Public Key Infrastructure for Multiplatforms Programming Guide and Reference Proporciona información para los programadores que desarrollan aplicaciones mediante IBM SecureWay X.509 Public Key Infrastructure para múltiples plataformas, conocido también como PKIX. Incluye una visión general del producto, instrucciones para escribir programas para componentes PKIX individuales y descripciones de las API de PKIX.

IBM KeyWorks Toolkit

Toda la documentación proporcionada con IBM KeyWorks Toolkit es documentación en línea, en formato PDF en el CD del producto. La documentación es la siguiente:

IBM KeyWorks Toolkit Developer's Guide
Presenta una visión general del kit de herramientas. Además, explica cómo integrar el kit de herramientas en aplicaciones, y contiene una aplicación de ejemplo.

IBM KeyWorks Toolkit Application Programming Interface (API) Specification
Define la interfaz que los desarrolladores de aplicaciones utilizan para acceder a servicios de seguridad proporcionados por los módulos de Service Provider e infraestructura.

IBM KeyWorks Toolkit Service Provider Module Structure & Administration
Describe las características comunes a todos los módulos de Service Provider del kit de herramientas. Este documento debe utilizarse conjuntamente con las especificaciones de interfaz de Service Provider individuales a fin de crear un módulo de Service Provider.

IBM KeyWorks Toolkit Cryptographic Service Provider Interface Specification
Define la interfaz a la que deben ajustarse los módulos de Service Provider de cifrado para poder ser accesibles a través del kit de herramientas.

IBM Key Recovery Service Provider Interface (KRSPI) Specification
Define la interfaz a la que deben ajustarse los módulos de Service Provider de recuperación para poder ser accesibles a través del kit de herramientas.

IBM KeyWorks Toolkit Trust Policy Interface Specification
: Define la interfaz que deben utilizar los diseñadores de políticas, tales como Autoridades Certificadoras, emisores de certificados y desarrolladores de aplicaciones que definen políticas, para poder ampliar el kit de herramientas con políticas modelo o específicas de la aplicación.

IBM KeyWorks Toolkit Certificate Library Interface (CLI) Specification
: Define la interfaz que deben utilizar los desarrolladores de bibliotecas de certificados para proporcionar servicios de manipulación de certificados específicos del formato a numerosas aplicaciones del kit de herramientas y módulos de políticas fiables.

IBM KeyWorks Toolkit Data Storage Library Interface (DLI) Specification
: Define la interfaz que deben utilizar los desarrolladores de bibliotecas para proporcionar almacenamiento persistente de certificados específico o independiente del formato.

IBM Key Recovery Service Provider

La siguiente documentación se proporciona con IBM Key Recovery Service Provider en formato PDF en el CD del producto:

IBM Key Recovery Service Provider Key Recovery Server Installation and Usage Guide
: Explica los conceptos de la recuperación de claves, proporciona una guía para configurar una solución de recuperación de claves para una organización y procedimientos para instalar, configurar y operar con IBM Key Recovery Server.

Libros rojos sobre seguridad

Los siguientes libros rojos, editados por la ITSO (IBM International Technical Support Organization) tratan los productos relacionados con la seguridad y sus procesos. Están disponibles en la dirección siguiente: www.us.ibm.com/redbooks.

- Understanding the IBM SecureWay FirstSecure Framework
- *High Availability IBM eNetwork Firewall*

Paquetes de documentación

Se dispone de los siguientes paquetes de documentación para IBM SecureWay FirstSecure.

Paquete de documentación de FirstSecure

El paquete de documentación de FirstSecure contiene las publicaciones siguientes:

- FirstSecure License Information
- *IBM SecureWay FirstSecure Planning and Integration*
- *IBM SecureWay Policy Director Up and Running*
- *IBM SecureWay Boundary Server for Windows NT and AIX: Up and Running*
- *IBM SecureWay Trust Authority Up and Running*
- *Tivoli Cross-Site for Security Installation*

Paquete de documentación de Policy Director

El paquete de documentación de Policy Director contiene las publicaciones siguientes:

- Policy Director License Information
- *IBM SecureWay Policy Director Up and Running*

Paquete de documentación de SecureWay Boundary Server

El paquete de documentación de SecureWay Boundary Server contiene las publicaciones siguientes:

- SecureWay Boundary Server License Information
- *IBM SecureWay Boundary Server for Windows NT and AIX: Up and Running*

Parte 4. Apéndices

Apéndice A. Avisos

Esta información se desarrolló para productos y servicios ofrecidos en los Estados Unidos. Es posible que IBM no ofrezca en otros países los productos, servicios o funciones descritos en este documento. Para obtener información sobre los productos y servicios disponibles actualmente en su país, póngase en contacto con su representante local de IBM. Las referencias hechas a productos, programas o servicios de IBM no pretenden afirmar ni implicar que sólo puedan utilizarse esos productos, programas o servicios de IBM. Puede utilizarse cualquier producto, programa o servicio funcionalmente equivalente y que no infrinja ninguno de los derechos de propiedad intelectual de IBM. Sin embargo, es responsabilidad del usuario evaluar y verificar el funcionamiento de los productos, programas o servicios que no sean de IBM.

IBM puede tener patentes o solicitudes de patente pendientes que cubran algunos temas presentados en este documento. La adquisición de este documento no confiere ninguna licencia sobre dichas patentes. Puede enviar consultas sobre licencias, por escrito, a:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
Estados Unidos

Si desea realizar alguna consulta relativa a la información DBCS (doble byte), póngase en contacto con el departamento de propiedad intelectual de IBM de su país o envíe su consulta, por escrito, a:

IBM World Trade Asia Corporation Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokio 106, Japón

El siguiente párrafo no es aplicable en el Reino Unido ni en ningún otro país en donde estas estipulaciones no sean coherentes con la legislación local:
INTERNATIONAL BUSINESS MACHINES CORPORATION PROPORCIONA ESTA PUBLICACIÓN “TAL CUAL”, SIN NINGÚN TIPO DE GARANTÍA, EXPLÍCITA O IMPLÍCITA, INCLUIDAS, PERO SIN LIMITARSE A, LAS GARANTÍAS IMPLÍCITAS DE NO VULNERACIÓN, COMERCIALIZACIÓN E IDONEIDAD PARA UNA FINALIDAD DETERMINADA. Algunos estados no permiten la declaración de limitación de responsabilidad de garantías explícitas o implícitas en determinadas transacciones; por consiguiente, es posible que esta declaración no sea aplicable en su caso.

Esta publicación puede contener imprecisiones técnicas o errores tipográficos. Periódicamente se realizan cambios en la información contenida en este documento; dichos cambios se incorporarán en nuevas ediciones de la publicación. IBM puede

realizar mejoras y/o cambios en los productos y/o programas descritos en esta publicación en cualquier momento y sin previo aviso.

Las referencias realizadas en esta información a páginas Web que no son de IBM se proporcionan tan sólo a título informativo y no significa que se avalen, en ningún caso, dichos sitios Web. El material de estas páginas Web no forma parte del material para este producto de IBM y el usuario será el único responsable del uso de estos sitios Web.

IBM puede utilizar o distribuir la información que usted proporcione de la forma que crea oportuna sin incurrir por ello en ninguna obligación con el remitente.

Los licenciatarios de este programa que deseen información acerca del mismo a fin de habilitar: (i) el intercambio de información entre programas creados de forma independiente y otros programas (incluido éste), y (ii) la utilización mutua de la información que se ha intercambiado, deben ponerse en contacto con:

IBM Corporation
Department LZKS
11400 Burnet Road
Austin, TX 78758
Estados Unidos

Dicha información estará disponible de acuerdo con los términos y condiciones oportunos, que en algunos casos puede incluir el pago de una determinada cantidad.

El programa bajo licencia que se describe en este documento y todo el material bajo licencia disponible para el mismo los proporciona IBM bajo las condiciones indicadas en el documento IBM Customer Agreement, en el documento IBM International Program License Agreement o cualquier otro acuerdo equivalente entre las partes.

Los datos de rendimiento contenidos en este manual se obtuvieron en un entorno controlado. Por lo tanto, los resultados obtenidos en otros entornos operativos pueden variar significativamente. Algunas mediciones pueden haberse realizado en sistemas a nivel de desarrollo y no se garantiza que estas mediciones sean las mismas en los sistemas comercializados. Es más, es posible que alguna medición se haya estimado mediante la extrapolación. Los resultados reales pueden variar. Los usuarios de este documento deben verificar los datos aplicables para su entorno específico.

La información relativa a productos que no son IBM se ha obtenido de los distribuidores de dichos productos, de los anuncios publicados o de otras fuentes disponibles públicamente. IBM no ha probado estos productos y no puede confirmar la precisión del rendimiento, la compatibilidad o ninguna otra afirmación relativa a los productos no IBM. Las consultas sobre las posibilidades de los productos no IBM deben remitirse a los distribuidores de dichos productos.

Todas las afirmaciones referentes a los planes futuros de IBM están sujetas a cambios o renuncias sin previo aviso, y representan únicamente metas y objetivos.

Todos los precios de IBM mostrados son precios de venta al por menor sugeridos por IBM, están actualizados y están sujetos a cambios sin previo aviso. Los precios de concesionario pueden variar.

Esta información es únicamente para fines de planificación. La información incluida aquí puede cambiar antes de que los productos descritos pasen a estar disponibles.

Marcas registradas

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

AIX
AIX/6000
DB2
DB2 Universal Database
eNetwork
Global Sign-On
GSO
IBM
Netfinity
OS/2
RS/6000
SecureWay
Websphere

Intel y Pentium son marcas registradas de Intel Corporation en los Estados Unidos y en otros países.

Java y todas las marcas registradas y logotipos basados en Java son marcas registradas de Sun Microsystems, Inc. en los Estados Unidos y en otros países.

Lotus, Lotus Notes, Domino y cc:Mail son marcas registradas de Lotus Development Corporation en los Estados Unidos, otros países, o en ambos.

Microsoft, Windows, Windows NT y el logotipo de Windows son marcas registradas de Microsoft Corporation en los Estados Unidos y en otros países.

Tivoli es una marca registrada de Tivoli Systems Inc. en los Estados Unidos y/o en otros países.

UNIX es una marca registrada en los Estados Unidos y en otros países, bajo la licencia exclusiva de X/Open Company Limited.

Otros nombres de empresas, productos y servicios son marcas registradas o marcas de servicio de terceros.

Glosario

Este glosario define términos y abreviaturas que se utilizan en esta publicación que pueden resultarle nuevos o desconocidos y términos que pueden resultarle de interés. Incluye términos y definiciones de:

- IBM Dictionary of Computing, Nueva York: McGraw-Hill, 1994.
- American National Standard Dictionary for Information Systems, ANSI X3.172–1990, American National Standards Institute (ANSI), 1990.
- Answers to Frequently Asked Questions, Versión 3.0, California: RSA Data Security, Inc., 1996.

.

A

ACL. Lista de control de accesos.

ActiveX. En programación de Microsoft, un conjunto de términos y tecnología orientada a objetos.

agente. En Tivoli Cross-Site for Security, un supervisor inteligente de paquetes IP que atrapa los paquetes, comprueba que no presenten anomalías en las diferentes capas de la red y mantiene un seguimiento del estado de las conexiones establecidas y de las estadísticas.

API. Interfaz de programas de aplicación.

aplicación Web. Una aplicación diseñada para acceder a través de la World Wide Web.

applet. Un programa informático escrito en Java que se ejecuta en un navegador compatible con Java como Netscape Navigator. Se le conoce también como applet Java.

asistente. Un diálogo de una aplicación que utiliza instrucciones paso a paso que guían al usuario en la realización de una tarea específica.

autentificación. El proceso de determinar de forma fiable la identidad del que inicia la comunicación.

autoridad de certificación. La entidad, aplicación de software o personas responsables de seguir las políticas de seguridad de las organizaciones y de asignar identidades electrónicas seguras en forma de certificados. La autoridad de certificación procesa peticiones para emitir, renovar y revocar certificados.

autorización. El proceso de determinar qué tipos de actividades puede realizar un usuario. Generalmente la autorización se produce después de la autentificación.

B

Bloodhound. En Norton AntiVirus, el componente que localiza un virus.

C

cámara de seguridad. Una cámara de seguridad utiliza el cifrado para impedir que personas no autorizadas, como por ejemplo los administradores de sistemas y los propietarios de otras cámaras de seguridad, revelen la información. También utiliza las signaturas digitales para impedir intromisiones y los certificados digitales como protección contra las comunicaciones de desconocidos. También utiliza el cifrado, las signaturas y certificados para transmitir la información de forma segura a otras cámaras.

canal. Una vía por la que pueden enviarse señales.

célula. En DCE, un grupo de usuarios, sistemas y recursos que generalmente está centrado en una finalidad común y que comparte límites de seguridad, de administración y de nombres. Generalmente, una célula está compuesta por usuarios, máquinas y recursos que comparten una finalidad común y un nivel más elevado de fiabilidad entre sí que con los usuarios, máquinas y recursos externos a la célula.

certificado digital. Una credencial electrónica que emite una entidad fiable de terceros a una persona o entidad. Un certificado contiene información acerca de la entidad que certifica.

cifrar. Desordenar la información de modo que aquel que conozca el código de descifrado pueda obtener la información original una vez descifrada.

clave pública. La clave en un par de claves pública/privada que está a disposición de otros. Permite dirigir una transacción al propietario de la clave o verificar la signatura digital. Los datos cifrados con una clave pública únicamente se pueden descifrar con la clave privada correspondiente. *Vea también* par de claves pública/privada.

cliente. (1) Una unidad funcional que recibe servicios compartidos de un servidor. (2) Un sistema o programa que solicita un servicio de otro sistema o programa.

código móvil. Relativo a las operaciones que realiza en un sistema portátil un usuario que frecuentemente se traslada por diferentes lugares y utiliza diferentes tipos de conexiones de red (por ejemplo, de marcación, LAN o inalámbrica).

comercio electrónico. La realización de transacciones de empresa a empresa. Incluye comprar y vender bienes y servicios (con clientes, proveedores, distribuidores y demás) a través de Internet. Es un elemento primario de e-business.

conector. Un programa que puede utilizarse como parte del navegador Web.

control de acceso. En la seguridad de sistemas, el proceso de asegurar que sólo los usuarios autorizados puedan acceder de forma autorizada a los recursos de un sistema.

correo basura. Correo electrónico no solicitado enviado generalmente a multitud de destinatarios.

cortafuegos. Un sistema o combinación de sistemas que impone un límite entre dos o más redes.

D

daemon. En AIX, un programa que permanece residente a la espera de dar servicio a una petición.

DCE. Entorno de sistemas distribuidos.

E

e-business. La realización de transacciones comerciales a través de redes y sistemas. Incluye comprar y vender bienes y servicios. También incluye la transferencia de fondos a través de las comunicaciones digitales.

entorno de desarrollo integrado. Un programa para el desarrollo de aplicaciones que le permite codificar la aplicación, ejecutarla con puntos de interrupción y recibir ayuda de diagnóstico para los errores del programa.

entorno de sistemas distribuidos. Los servicios y herramientas que soportan la creación, utilización y mantenimiento de las aplicaciones distribuidas en un entorno de sistemas heterogéneo.

espacio de nombres. En lo referente al directorio, la estructura externa de nombres a la que pueden acceder los usuarios.

extranet. Un derivado de Internet que utiliza tecnología similar. Las empresas comienzan a aplicar la edición Web, el comercio electrónico, las funciones de mensajería y groupware a una amplia gama de clientes, socios comerciales y personal interno.

F

filtrado de contenido. Encubrir una transmisión para leer el contenido y poder determinar si la transmisión cumple con los estándares específicos sobre contenido.

filtrado de direcciones de red. El proceso de comprobar la dirección del correo electrónico de entrada y salida para comprobar si el destinatario o remitente son aceptables.

FTP (File Transfer Protocol). Un protocolo cliente/servidor que se puede utilizar para transferir archivos entre sistemas.
REFID='REV3'.

I

IDE. Entorno de desarrollo integrado.

Implementation Services. El soporte de instalación en el local que proporciona IBM

incidente. En Tivoli Cross-Site for Security, una actividad sospechosa que puede ser un ataque al sistema.

interfaz de programas de aplicación. Una interfaz funcional que permite escribir un programa de aplicación en un lenguaje de alto nivel de modo que pueda utilizar funciones específicas.

Internet. Una agrupación de redes a nivel mundial que proporciona comunicaciones electrónicas entre sistemas. Permite que los sistemas se comuniquen entre sí a través de dispositivos de software, como por ejemplo, correo electrónico o navegadores Web. Por ejemplo, algunas universidades están en una red que, a su vez, se enlaza con otras redes similares para formar Internet.

intranet. Una red en una empresa que generalmente reside detrás de los cortafuegos. Es un derivado de Internet que utiliza tecnología similar. Técnicamente, intranet es una mera extensión de Internet. HTML (un lenguaje utilizado para la representación de información) y HTTP (un protocolo que mueve los archivos de hipertexto a través de Internet) son algunos de los elementos comunes.

IPSec. Un estándar de Internet Protocol Security desarrollado por IETF. IPSec es un protocolo de capas de red diseñado para proporcionar servicios de seguridad de cifrado que soportan de forma flexible combinaciones de funciones de autentificación, integridad, control de acceso y confidencialidad. Debido a sus potentes funciones de autentificación, ha sido adoptado por muchos de los distribuidores de productos VPN como el protocolo para establecer conexiones protegidas punto a punto a través de Internet.

ISV. Distribuido de software independiente.

J

Java. Un conjunto de tecnologías de sistemas de plataformas no específicas utilizables en la red y desarrollado por Sun Microsystems, Incorporated. El entorno Java está compuesto por el sistema operativo Java, las máquinas virtuales para diferentes plataformas, el lenguaje de programación Java orientado a objetos y varias bibliotecas de clases.

JavaScript. Un lenguaje de script que se asemeja a Java y que ha sido desarrollado por Netscape para utilizarlo con el navegador Netscape.

K

Kerberos. Un método seguro de autentificar un servicio solicitando un sistema. Kerberos ha sido desarrollado dentro del Athena Project en el Massachusetts Institute of Technology (MIT). En la mitología griega, Kerberos era un perro de tres cabezas que guardaba las puertas del infierno. Kerberos permite que un usuario solicite un ticket cifrado a un proceso de autentificación que, a continuación, puede utilizarse para solicitar un servicio específico a un servidor. No es necesario que la contraseña del usuario pase a través de la red.

L

LDAP. Lightweight Directory Access Protocol.

Lightweight Directory Access Protocol. En IBM SecureWay Directory, LDAP proporciona un medio de mantener la información del directorio en una ubicación central para su almacenamiento, actualización, recuperación e intercambio.

lista de control de accesos. Un mecanismo para limitar el uso de un recurso específico a los usuarios autorizados.

llamada a procedimiento remoto. (1) Un recurso que utiliza un cliente para solicitar la ejecución de una llamada a un procedimiento desde un servidor. Este recurso incluye una biblioteca de procedimientos y una representación externa de los datos. (2) Una petición de cliente a un proveedor de servicios situado en otro nodo.

M

macro "bomba". Una secuencia grabada de mandatos que se envían a otro usuario para ocasionar resultados no deseados.

MPEG. El estándar bajo desarrollo de Moving Pictures Experts Group para comprimir y almacenar vídeo y animación en formato digital.

N

navegador Web. Software de cliente que se ejecuta en un PC de escritorio y que le permite navegar por la World Wide Web o por páginas locales. Es una herramienta para recuperación que proporciona acceso universal a una gran gama de material hipermedia disponible en la Web y en Internet. Los ejemplos más destacados son Netscape Navigator y Microsoft Internet Explorer. *Consulte también* servidor.

O

Object Request Broker. En programación orientada a objetos, el software que sirve de intermediario y permite que los objetos puedan intercambiar de forma transparente peticiones y respuestas.

objeto Web. Los datos disponibles a través de un navegador Web. Un objeto Web puede ser una página Web, una parte de una página Web, un archivo, una imagen, un directorio, un programa CGI o un applet Java.

OEM. Fabricante del equipo original.

P

par de claves pública/privada. Un par de claves pública/privada forma parte del concepto de cifrado por par de claves (presentado en 1976 por Diffie y Hellman para solucionar los problemas de gestión de claves). En su concepto cada persona obtiene un par de claves, una denominada la clave pública y la otra denominada la clave privada. La clave pública de cada persona es pública mientras que la clave privada se mantiene en secreto. El remitente y el destinatario no tienen por qué compartir la información secreta: todas las comunicaciones requieren únicamente claves públicas, y nunca se transmite o comparte ninguna clave privada. Ya no es necesario confiar en algunos canales de comunicaciones para protegerse de intromisiones o traiciones. El único requisito es que las claves públicas estén asociadas a los usuarios de forma fiable (mediante métodos de autentificación), por ejemplo en un directorio fiable. Cualquiera puede enviar un mensaje confidencial utilizando información pública. Sin embargo, el mensaje únicamente puede descifrarlo una clave privada, y ésta la posee el destinatario. Y lo que es más, el cifrado por par de claves se puede utilizar no sólo para confidencialidad (cifrado), sino para autentificación (signaturas digitales).

pasarela. Un sistema que permite que redes o aplicaciones incompatibles se puedan comunicar entre sí.

pasarela a nivel de circuito. En un cortafuegos, un servidor proxy que redirige una petición del cliente a través del cortafuegos al servidor destino.

pirata informático. Una persona que intenta acceder a una máquina o sistema sin la autorización correspondiente. Los piratas informáticos suelen utilizar recursos sin permiso.

principal. En DCE, una entidad que puede comunicarse con seguridad con otra entidad a través de la seguridad DCE. Los principales pueden ser usuarios, servidores o sistemas.

Protocolo de Control de Transmisión/Protocolo Internet. Un conjunto de protocolos de comunicaciones que soportan las funciones de conectividad de igual a igual en redes de área local y de área amplia.

protocolo SOCKS. Un protocolo que permite que una aplicación de una red protegida se comunique a través de un cortafuegos mediante un servidor socks.

pulsación. Una comunicación de un programa a un programa de gestión confirmando la continuación de la actividad. El programa indica al programa de gestión que continúa activo y realizando sus tareas.

R

Red privada virtual (VPN). Una red de datos privada que utiliza Internet, en lugar de las líneas telefónicas para establecer conexiones remotas. Dado que los usuarios acceden a los recursos de red corporativos a través de un ISP (Internet Service Provider) y no a través de una compañía telefónica, las empresas pueden disminuir de forma significativa los costes del acceso remoto. Una VPN también mejora la seguridad en el intercambio de datos. En la tecnología de cortafuegos tradicional, el contenido del mensaje se puede cifrar, pero las direcciones de origen y destino no. En la tecnología VPN, los usuarios pueden establecer una conexión de túnel en la que todo el paquete de información (contenido y cabecera) están cifrados y encapsulados.

RPC. En DCE, una llamada a procedimiento remoto

S

Secure Sockets Layer (SSL). (1) Un protocolo de comunicaciones estándar IETF con servicios de seguridad incorporados que son lo más transparentes posibles para el usuario final. Proporciona un canal de comunicaciones protegido. (2) Un servidor con posibilidad de SSL que generalmente acepta peticiones de conexiones SSL en un puerto diferente al de las peticiones HTTP estándar. SSL crea una sesión durante la cual el saludo sólo se ha de realizar una vez. Una vez

finalizado el saludo, se cifra la comunicación. Hasta que caduca la sesión SSL se realizan comprobaciones de la integridad de los mensajes.

seguimiento de auditoría. Datos, con el formato de una vía de acceso lógica, que enlazan una secuencia de sucesos. Se puede utilizar un seguimiento de auditoría para efectuar un rastreo de las transacciones o de la historia de una actividad determinada. Por ejemplo, puede seguir las actividades de una cuenta de un cliente.

Señal SecurID. El método de autentificación ACE/Server de Security Dynamics que incluye un ID de usuario y una señal SecurID. Cuando se inicia la sesión remotamente, la contraseña se obtiene de la señal SecurID. La contraseña cambia cada 60 segundos y sólo se puede utilizar una vez. Incluso si alguien intercepta su contraseña a través de la red abierta, la contraseña no es válida para utilizarla más veces.

servicio de directorio de células. Un componente de un entorno de sistemas distribuidos, DCE (Distributed Computing Environment), que gestiona una base de datos de información sobre los recursos de una célula DCE.

servidor. (1) En una red, una estación de datos que proporciona recursos a otras estaciones, por ejemplo, un servidor de archivos. (2) En TCP/IP, un sistema en una red que maneja las peticiones de un sistema situado en otra ubicación, denominado cliente/servidor.

servidor Apache. Un conjunto de software de servidor Web de libre disposición.

servidor IntraVerse. En IntraVerse, un sistema de red que contiene el software de servidor IntraVerse y que puede comunicarse con todos los sistemas principales que se ejecutan en el software del cliente NetSEAT. El servidor IntraVerse hace referencia a un sistema o combinación de sistemas que ejecutan los programas relacionados del producto.

servidor proxy. Un intermediario entre el sistema que solicita acceso (A) y el sistema al que se accede (B). De este modo, si un usuario final efectúa una petición de un recurso desde el sistema A, esta petición está dirigida a un servidor proxy. El servidor proxy efectúa la petición, obtiene la respuesta del sistema B y, a continuación, reenvía la respuesta al usuario final. Los servidores proxy son útiles para acceder a los recursos de la World Wide Web desde el interior de un cortafuegos.

servidor socks. Una pasarela a nivel de circuito que proporciona una conexión protegida en una dirección a través de un cortafuegos con las aplicaciones servidor de una red no protegida.

servidor Web. Un programa de servidor que responde a las peticiones de recursos de información de programas navegadores.

sin denegación. El uso de una clave privada digital para impedir que el que firma un documento niegue falsamente haberlo firmado.

T

TCP/IP. Protocolo de Control de Transmisión/Protocolo Internet

telnet. En la suite de protocolos de Internet, un protocolo que proporciona un servicio de conexión de terminal remoto. Permite a los usuarios de un sistema principal conectarse a un sistema principal remoto e interactuar como los usuarios de dicho sistema principal que están conectados directamente.

U

URL. Universal Resource Locator.

URL (Universal Resource Locator). El convenio de asignación de nombres para las comunicaciones en la World Wide Web en el que la vía de acceso de un objeto de la Web comienza por el nombre de servicio, el nombre de la organización, la vía de acceso y el nombre de archivo, por ejemplo, http://www.ibm.com/software/security/firstsecure.

V

VPN. Red privada virtual.

W

worm. Un virus informático que puede ocasionar daños.

X.509. Un estándar de certificados de aceptación general diseñado para dar soporte a la gestión y distribución segura de certificados PKI con signaturas digitales a través de redes Internet seguras. El certificado X.509 define las estructuras de datos que

acomodan procedimientos relacionados con la distribución de claves públicas con signaturas digitales por parte de entidades fiables de terceros.

Índice

F

I

M

N

P

R

S

T

V

W

Z

Hoja de Comentarios

IBM® SecureWay® FirstSecure
Planificación e integración
Versión 2

Número Pieza CT7EHES

En general, ¿está Ud. satisfecho con la información de este libro?

	Muy satisfecho	Satisfecho	Normal	Insatisfecho	Muy insatisfecho
Satisfacción general	□	□	□	□	□

¿Cómo valora los siguientes aspectos de este libro?

	Muy bien	Bien	Acep-table	Insatisfecho	Muy insatisfecho
Organización	□	□	□	□	□
Información completa y precisa	□	□	□	□	□
Información fácil de encontrar	□	□	□	□	□
Utilidad de las ilustraciones	□	□	□	□	□
Claridad de la redacción	□	□	□	□	□
Calidad de la edición	□	□	□	□	□
Adaptación a los formatos, unidades, etc. del país	□	□	□	□	□

Comentarios y sugerencias:

Nombre

Dirección

Compañía u Organización

Teléfono

Hoja de Comentarios

Corte o Doble
Por la Línea

Dóblese por la línea de puntos **Por favor no lo grape** Dóblese por la línea de puntos

PONER
EL
SELLO
AQUÍ

IBM, S.A.
National Language Solutions Center
Av. Diagonal, 571
08029 Barcelona
España

Dóblese por la línea de puntos **Por favor no lo grape** Dóblese por la línea de puntos

Corte o Doble
Por la Línea

Número Pieza: CT7EHES

Printed in Dublin

CT7EHES