



System i

Seguridad

System i y la seguridad en Internet

Versión 6 Release 1





System i

Seguridad

System i y la seguridad en Internet

Versión 6 Release 1

Nota

Antes de utilizar esta información y el producto al que hace referencia, lea la información que figura en el apartado “Avisos”, en la página 29.

Esta edición atañe a la versión 6, release 1, modificación 0 de IBM i5/OS (producto número 5761-SS1) y a todos los releases y modificaciones ulteriores hasta que se indique lo contrario en nuevas ediciones. Esta versión no se ejecuta en todos los modelos de sistema con conjunto reducido de instrucciones (RISC) ni tampoco se ejecuta en modelos CISC.

© Copyright International Business Machines Corporation 1999, 2008. Reservados todos los derechos.

Contenido

System i y la seguridad en Internet . . . 1

Archivo PDF de System i y la seguridad en Internet	1
Consideraciones sobre System i y la seguridad en Internet	2
Planificar la seguridad en Internet	3
Seguridad basada en la defensa por capas	4
Política y objetivos de seguridad.	6
Escenario: planes de la compañía JKL Toy para el e-business	8
Niveles de seguridad para la disponibilidad básica de Internet	10
Opciones de seguridad de la red	11
Cortafuegos	12
Reglas de paquetes de i5/OS	14
Detección de intrusiones	15
Elegir opciones de seguridad de red para i5/OS	15
Opciones de seguridad de aplicaciones	17
Seguridad del servicio Web	17

La seguridad Java en Internet	18
Seguridad del correo electrónico	20
Seguridad de FTP	22
Opciones de seguridad de la transmisión	24
Utilizar certificados digitales para SSL	25
Capa de sockets segura (SSL) para proteger el acceso a Telnet	26
Capa de sockets segura (SSL) para proteger System i Access para Windows.	27
Redes privadas virtuales (VPN) para proteger las comunicaciones privadas	27

Apéndice. Avisos 29

Información de la interfaz de programación	31
Marcas registradas	31
Términos y condiciones	31

System i y la seguridad en Internet

El acceso a Internet desde la red de área local (LAN) le exige volver a evaluar los requisitos de seguridad.

Las soluciones de software integradas y la arquitectura de seguridad del producto IBM System i le permite construir una buena defensa contra los intrusos y las brechas de seguridad potenciales de Internet. El uso de estas ofertas de seguridad garantiza que los clientes, empleados y socios comerciales puedan obtener la información que necesiten para trabajar en un entorno seguro.

Este temario explica las amenazas de seguridad más conocidas y cómo se relacionan estos riesgos con Internet y sus objetivos de e-business. En este temario también se enseña a evaluar los riesgos y a sopesarlos con respecto a las ventajas que supone utilizar las distintas opciones de seguridad que ofrece el sistema para manejar los riesgos. Puede determinar cómo puede utilizar esta información para desarrollar un plan de seguridad de la red que se ajuste a las necesidades de su compañía,

Archivo PDF de System i y la seguridad en Internet

Puede ver e imprimir un archivo PDF de esta información.

Para ver o descargar la versión PDF de este documento, seleccione System i y la seguridad en Internet (alrededor de 456 KB).

Los temas relacionados que puede ver o descargar son:


- Detección de intrusiones (alrededor de 285 KB). Puede crear una política de detección de intrusiones que audite los eventos de intrusión sospechosos que entran a través de la red TCP/IP, como por ejemplo paquetes IP creados incorrectamente. También puede escribir una aplicación para analizar los datos de auditoría y notificar al administrador de seguridad si es probable que se estén produciendo intrusiones TCP/IP.
- Correlación de identidades de empresa (EIM) (alrededor de 1954 KB). La correlación de identidades de empresa (EIM) es un mecanismo para correlacionar una persona o entidad (como un servicio) con las identidades de usuario pertinentes de diversos registros de la empresa.
- Inicio de sesión único (SSO) (alrededor de 1203 KB). La solución de inicio de sesión único (SSO) reduce el número de inicios de sesión que un usuario debe realizar, así como el número de contraseñas que el usuario necesita para acceder a múltiples aplicaciones y sistemas.
- Planificar y configurar la seguridad del sistema (alrededor de 3992 KB). Este tema proporciona información sobre cómo planificar y configurar de manera eficaz y sistemática la seguridad a nivel del sistema.

Cómo guardar los archivos PDF

Si desea guardar un archivo PDF en su estación de trabajo para verlo o imprimirlo:

1. En el navegador, pulse el enlace del PDF con el botón derecho del ratón.
2. Pulse en la opción que guarda el PDF localmente.
3. Navegue hasta el directorio en el que desea guardar el archivo PDF.
4. Pulse **Guardar**.

Cómo descargar Adobe Reader

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

Conceptos relacionados

Detección de intrusiones

Correlación de identidades de empresa (EIM)

Inicio de sesión único (SSO)

Planificar y configurar la seguridad del sistema

Consideraciones sobre System i y la seguridad en Internet

Los problemas de seguridad relacionados con Internet son muchos. En este tema se proporciona una visión general de las ventajas de la seguridad del i5/OS y de sus ofertas en materia de seguridad.

Cuando conecta la plataforma System i a Internet, una de las primeras preguntas que uno se plantea es "¿Qué debo saber sobre la seguridad e Internet?". Este tema se propone ayudarle a responder a esta pregunta.

Lo que debe saber depende de cómo desee utilizar Internet. El primer uso que se hace de Internet es proporcionar a los usuarios de la red interna acceso a la Web y al correo electrónico de Internet. También podría interesarle la capacidad de transferir información confidencial de un sitio a otro. Por último, es posible que desee utilizar Internet para el comercio electrónico o para crear una extranet entre su compañía y sus socios comerciales y distribuidores.

Antes de empezar a utilizar Internet, debe pensar cuáles son sus objetivos y cómo desea implantarlos. La toma de decisiones sobre el uso y la seguridad de Internet puede ser una cuestión compleja.

Nota: Si no está familiarizado con la terminología de seguridad y de Internet, consulte la terminología de seguridad común mientras trabaja con esta documentación).

Cuando haya determinado el uso que desea hacer de Internet para e-business, así como las cuestiones de seguridad y las ofertas, funciones y herramientas de seguridad disponibles, puede desarrollar una política y unos objetivos de seguridad. Son varios los factores que afectan a las opciones que elija al desarrollar la política de seguridad. Cuando amplíe su organización para llevarla a Internet, la política de seguridad será la piedra angular para garantizar que los sistemas y recursos están protegidos.

Características de seguridad del i5/OS

Además de las distintas ofertas de seguridad específicas para proteger el sistema en Internet, el sistema operativo i5/OS tiene las siguientes características de seguridad:

- Seguridad integrada, muy difícil de sortear si se compara con los paquetes de software de seguridad complementarios que se ofrecen en otros sistemas.
- Arquitectura basada en objetos, que dificulta técnicamente la creación y la propagación de los virus. En el sistema operativo i5/OS, un archivo no puede hacerse pasar por un programa, ni un programa puede cambiar otro programa. Las características de integridad del i5/OS exigen el uso de interfaces proporcionadas por el sistema para acceder a los objetos. No se puede acceder a un objeto directamente a partir de su dirección en el sistema. No se puede tomar un desplazamiento y convertirlo en un puntero ni fabricarlo. La manipulación de punteros es una técnica muy extendida entre los piratas informáticos en otras arquitecturas del sistema.
- Flexibilidad, que permite configurar la seguridad del sistema para dar respuesta a sus requisitos específicos. Puede utilizar el planificador de seguridad para determinar qué recomendaciones de seguridad se ajustan a sus necesidades.

Ofertas de seguridad avanzada del i5/OS

El sistema operativo i5/OS también ofrece varias ofertas de seguridad específicas que le permitirán mejorar la seguridad del sistema cuando se conecte a Internet. En función del uso que haga de Internet, podría aprovechar las ventajas de una o varias de estas ofertas:

- Redes privadas virtuales (VPN), que son una ampliación de la intranet privada de una empresa a través de una red pública como Internet. Puede utilizar una VPN para crear una conexión privada segura, creando básicamente un túnel privado a través de una red pública. VPN es una característica integrada del sistema operativo i5/OS, disponible en la interfaz de System i Navigator.
- Las reglas de paquetes son una característica integrada del sistema operativo i5/OS, disponible en la interfaz de System i Navigator. Mediante esta característica, puede configurar reglas de filtrado de paquetes IP y de conversión de direcciones de red (NAT) para controlar el flujo del tráfico TCP/IP dentro y fuera del sistema.
- Con los protocolos de capa de sockets segura (SSL), puede configurar las aplicaciones para que utilicen SSL con el fin de establecer conexiones seguras entre las aplicaciones de servidor y sus clientes. SSL se desarrolló originalmente para proteger las aplicaciones de servidor y los navegadores Web, pero se pueden habilitar otras aplicaciones para que utilicen SSL. Ahora son numerosas las aplicaciones que están habilitadas para SSL, incluido IBM HTTP Server para i5/OS, System i Access para Windows, el protocolo de transferencia de archivos (FTP), Telnet, etcétera.

Conceptos relacionados

“Política y objetivos de seguridad” en la página 6

La política de seguridad define qué es lo que desea proteger, y los objetivos de seguridad expresan lo que espera de los usuarios del sistema.

“Redes privadas virtuales (VPN) para proteger las comunicaciones privadas” en la página 27

Las redes privadas virtuales (VPN), que son una extensión de la intranet de una compañía a través de la infraestructura existente ya sea de una red pública o de una red privada, pueden ayudarle a comunicarse de manera privada y segura dentro de su organización.

“Escenario: planes de la compañía JKL Toy para el e-business” en la página 8

Escenario típico de una compañía JKL Toy, que ha decidido ampliar sus objetivos de negocio utilizando Internet, y que podría serle de utilidad si desea establecer sus propios planes para e-business.

Información relacionada

Conectarse a Internet

Planificador de la seguridad de eServer

Filtrado IP y conversión de direcciones de red

Capa de sockets segura (SSL)



AS/400 Internet Security: Protecting Your AS/400 from HARM on the Internet

Planificar la seguridad en Internet

Cuando elabore planes para el uso que se va a hacer de Internet, deberá planificar las necesidades de seguridad en Internet.

Debe reunir información detallada sobre los planes del uso de Internet y documentar la configuración de la red interna. A partir de la información que haya reunido, podrá evaluar con precisión sus necesidades de seguridad.

Por ejemplo, debe documentar y describir la siguiente información:

- La configuración de la red actual.
- Información de configuración del servidor de correo electrónico y del sistema de nombres de dominio (DNS).

- La conexión con el proveedor de servicios de Internet (ISP).
- Los servicios de Internet que desea utilizar.
- Los servicios que desea prestar a los usuarios de Internet.

La documentación de este tipo de información le ayudará a determinar cuáles son los riesgos de seguridad a que se expone y qué medidas de seguridad necesita para minimizarlos.

Por ejemplo, supongamos que le interesa que los usuarios internos utilicen Telnet para conectarse a los hosts de una ubicación de investigación especial. Los usuarios internos necesitan este servicio como ayuda para desarrollar nuevos productos para la compañía; sin embargo, usted podría estar preocupado por el flujo de datos confidenciales sin protección a través de Internet. Si la competencia captura estos datos y los utiliza, la compañía podría enfrentarse a graves riesgos económicos. Una vez identificadas las necesidades de uso (Telnet) y los riesgos asociados (exposición de información confidencial), ya puede determinar qué medidas de seguridad adicionales debe implantar para garantizar la confidencialidad de los datos en este uso (como la habilitación de la capa de sockets segura (SSL)).

Seguridad basada en la defensa por capas

La política de seguridad define qué es lo que desea proteger y qué espera de los usuarios del sistema.

La política de seguridad proporciona una base para la planificación de la seguridad al diseñar nuevas aplicaciones o ampliar la red actual. Describe responsabilidades del usuario como las de proteger información confidencial y crear contraseñas no triviales.

Nota: Debe crear y establecer una política de seguridad en su compañía que minimice los riesgos de la red interna. Las características de seguridad inherentes del sistema operativo i5/OS, si se configuran correctamente, le permiten minimizar muchos riesgos. No obstante, cuando conecte el sistema a Internet, deberá proporcionar medidas de seguridad adicionales que garanticen la seguridad de la red interna.

El uso del acceso a Internet en actividades empresariales lleva asociado muchos riesgos. Siempre que cree una política de seguridad, deberá sopesar el suministro de servicios con el control del acceso a las funciones y los datos. En los sistemas conectados en red, la seguridad es más difícil porque el propio canal de comunicaciones está abierto a los ataques.

Algunos servicios de Internet son más vulnerables a ciertos tipos de ataques que otros. Por lo tanto, es fundamental que comprenda los riesgos que supone cada servicio que se proponga utilizar o prestar. Además, el conocimiento de los posibles riesgos de seguridad ayuda a determinar un conjunto claro de objetivos de seguridad.

En Internet hay determinados individuos que suponen una amenaza para la seguridad de las comunicaciones por Internet. En la siguiente lista se describen algunos de los riesgos de seguridad más típicos con los que se puede encontrar:

- **Ataques pasivos**

En un ataque pasivo, el autor supervisa el tráfico de la red para intentar conocer algunos secretos. Estos ataques se pueden basar en la red (rastreamiento de los enlaces de comunicaciones) o en el sistema (sustituyendo un componente del sistema por un programa caballo de Troya que captura los datos clandestinamente). Los ataques pasivos son los más difíciles de detectar. Por ello, deberá presuponer que alguien está a la escucha de todo lo que envía por Internet.

- **Ataques activos**

En un ataque activo, el autor intenta abrirse paso a través de sus defensas para entrar en los sistemas de la red. Hay varios tipos de ataques activos:

- En los **intentos de acceso al sistema**, el atacante intenta aprovechar las brechas de seguridad para acceder a un cliente o un sistema y controlarlo.

- En los ataques de **usurpación**, el atacante intenta abrirse paso a través de sus defensas haciéndose pasar por un sistema de confianza o bien un usuario intenta persuadirle de que le envíe información secreta.
- En los **ataques de denegación de servicio**, el atacante intenta interferir en las operaciones o detenerlas, redirigiendo el tráfico o bombardeando el sistema con correo basura.
- En los **ataques criptográficos**, el atacante intenta adivinar o robar las contraseñas o bien utiliza herramientas especializadas para intentar descifrar los datos cifrados.

Múltiples capas de defensa

Como los riesgos potenciales de Internet se pueden producir en varios niveles, deberá configurar medidas de seguridad que ofrezcan múltiples capas de defensa contra los riesgos. En general, cuando se conecte a Internet, no debe preguntarse si hay alguna posibilidad de que se produzcan intrusiones o ataques de denegación de servicio. Por el contrario, debe dar por sentado que sí se producirán problemas de seguridad. De esta forma, la mejor defensa será un ataque proactivo y deliberado. El uso de un enfoque por capas al planificar la estrategia de seguridad de Internet garantiza que el atacante que logre penetrar en una de las capas de defensa será detenido en una capa ulterior.

La estrategia de seguridad debe incluir medidas que ofrezcan protección en las siguientes capas del modelo informático de red tradicional. En general, debe planificar la seguridad desde el nivel más básico (seguridad del sistema) hasta el nivel más complejo (seguridad de transacciones).

Seguridad a nivel de sistema

Las medidas de seguridad del sistema representan la última línea de defensa contra un problema de seguridad relacionado con Internet. Por lo tanto, el primer paso de una estrategia de seguridad en Internet completa debe ser configurar debidamente la seguridad básica del sistema.

Seguridad a nivel de red

Las medidas de seguridad de la red controlan el acceso al sistema operativo i5/OS y a otros sistemas de la red. Cuando conecta la red a Internet, debe asegurarse de que tiene implantadas las debidas medidas de seguridad adecuadas a nivel de la red para proteger los recursos internos de la red contra la intrusión y el acceso no autorizado. El medio más común para garantizar la seguridad de la red es un cortafuegos. El proveedor de servicios de Internet (ISP) puede proporcionar una parte importante del plan de seguridad de la red. El esquema de seguridad de la red debe indicar qué medidas de seguridad proporciona el ISP, como las reglas de filtrado de la conexión del direccionador del ISP y las medidas de precaución del sistema de nombres de dominio (DNS) público.

Seguridad a nivel de aplicaciones

Las medidas de seguridad a nivel de aplicaciones controlan cómo pueden interaccionar los usuarios con las aplicaciones concretas. En general, tendrá que configurar valores de seguridad para cada una de las aplicaciones que utilice. Sin embargo, conviene que preste una atención especial al configurar la seguridad de las aplicaciones y los servicios que utilizará de Internet o que proporcionará a Internet. Estas aplicaciones y servicios son vulnerables al mal uso por parte de los usuarios no autorizados que buscan una manera de acceder a los sistemas de la red. Las medidas de seguridad que decida utilizar deberán incluir los riesgos del lado del servidor y del lado del cliente.

Seguridad a nivel de transmisión

Las medidas de seguridad a nivel de transmisión protegen las comunicaciones de datos dentro de la red y entre varias redes. Cuando se comunica en una red que no es de confianza como Internet, no puede controlar cómo fluye el tráfico desde el origen hasta el destino. El tráfico y los datos transportados fluyen a través de distintos sistemas que están fuera de su control. A menos que implante medidas de seguridad como las de configurar las aplicaciones para que utilicen la capa de sockets segura (SSL), los datos direccionados estarán a disposición de cualquier persona que desee verlos y utilizarlos. Las medidas de seguridad a nivel de transmisión protegen los datos mientras fluyen entre los límites de otros niveles de seguridad.

Cuando elabore una política de seguridad global de Internet, deberá desarrollar individualmente una estrategia de seguridad para cada capa. Asimismo, deberá describir cómo interaccionarán entre sí los distintos conjuntos de estrategias para ofrecer así a su empresa una red de seguridad exhaustiva.

Conceptos relacionados

“Niveles de seguridad para la disponibilidad básica de Internet” en la página 10

Antes de conectarse a Internet, debe determinar qué nivel de seguridad necesita adoptar para proteger el sistema.

“Opciones de seguridad de la red” en la página 11

Para proteger los recursos internos, elija las medidas de seguridad pertinentes a nivel de red.

“Opciones de seguridad de aplicaciones” en la página 17

Dispone de algunas opciones a la hora de gestionar los riesgos de seguridad para numerosas y conocidas aplicaciones y servicios de Internet.

“Opciones de seguridad de la transmisión” en la página 24

Para proteger los datos cuando fluyen por una red que no sea de confianza, como Internet, debe aplicar las medidas de seguridad pertinentes. Estas medidas son la capa de sockets segura (SSL), System i Access para Windows y las conexiones de redes privadas virtuales (VPN).

“Política y objetivos de seguridad”

La política de seguridad define qué es lo que desea proteger, y los objetivos de seguridad expresan lo que espera de los usuarios del sistema.

“Seguridad del correo electrónico” en la página 20

La utilización del correo electrónico por Internet o por otras redes que no sean de confianza supone riesgos de seguridad para su sistema, aunque este esté protegido por un cortafuegos.

Referencia relacionada



Guía de seguridad de System i para IBM i5/OS Versión 5 Release 4

Política y objetivos de seguridad

La política de seguridad define qué es lo que desea proteger, y los objetivos de seguridad expresan lo que espera de los usuarios del sistema.

La política de seguridad

Cada servicio de Internet que utilice o preste supone riesgos para el sistema y para la red a la que está conectado. La política de seguridad es un conjunto de reglas que se aplican a las actividades del sistema y a los recursos de comunicaciones que pertenecen a una organización. Estas reglas incluyen áreas como la seguridad física, personal, administrativa y de la red.

La política de seguridad define qué es lo que desea proteger y qué espera de los usuarios del sistema. Proporciona una base para la planificación de la seguridad al diseñar nuevas aplicaciones o ampliar la red actual. Describe responsabilidades del usuario como las de proteger información confidencial y crear contraseñas no triviales. La política de seguridad también debe describir cómo se va a supervisar la efectividad de las medidas de seguridad. Esta supervisión le ayudará a determinar si alguna persona podría intentar burlar sus defensas.

Para desarrollar una política de seguridad, debe definir claramente sus objetivos de seguridad. Cuando haya creado una política de seguridad, el siguiente paso es poner en práctica las reglas de la política. Este paso incluye la formación de los empleados y la adición de piezas de hardware y programas de software que se necesiten para poner en vigor las reglas. Asimismo, cuando realice cambios en el entorno informático, deberá actualizar la política de seguridad. De esta forma se cubren los posibles riesgos que puedan implicar estos cambios.

Los objetivos de seguridad

Cuando cree y desarrolle una política de seguridad, deberá tener claros los objetivos. Los objetivos de seguridad entran dentro de una o más de estas categorías:

protección de recursos

El esquema de protección de recursos garantiza que solo los usuarios autorizados podrán acceder a los objetos del sistema. La capacidad de asegurar todo tipo de recursos del sistema es una de las ventajas del System i. Primero deberá definir con precisión las distintas categorías de usuarios que pueden acceder al sistema. Asimismo, cuando cree la política de seguridad, deberá definir qué tipo de autorización de acceso desea otorgar a estos grupos de usuarios.

autenticación

Es la seguridad o la verificación de que el recurso (persona o máquina) situado en el otro extremo de la sesión es realmente el que dice ser. Una autenticación convincente defiende el sistema contra riesgos de seguridad como las imitaciones, en las que el remitente o el destinatario utiliza una identidad falsa para acceder al sistema. Tradicionalmente, los sistemas han utilizado contraseñas y nombres de usuario para la autenticación; los certificados digitales pueden ofrecer un método más seguro de autenticación, a la vez que proporcionan otras ventajas de seguridad. Cuando enlaza su sistema con una red pública como Internet, la autenticación de usuario toma nuevas dimensiones. Una diferencia importante entre Internet y una intranet es la capacidad de confiar en la identidad del usuario que inicia la sesión. Por lo tanto, debe considerar seriamente la posibilidad de utilizar unos métodos más potentes de autenticación que los que proporcionan los procedimientos tradicionales de conexión mediante nombre de usuario y contraseña. Los usuarios autenticados podrían tener distintos tipos de permisos, según su nivel de autorización.

autorización

Es la seguridad de que la persona o el sistema situado en el otro extremo de la sesión tiene permiso para llevar a cabo la petición. La autorización es el proceso de determinar quién o qué puede acceder a los recursos del sistema o ejecutar determinadas actividades en un sistema. Normalmente, la autorización se realiza en el contexto de la autenticación.

integridad

Es la seguridad de que la información entrante es la misma que la que se ha enviado. Para entender la integridad, primero deberá comprender los conceptos de integridad de los datos e integridad del sistema.

- **Integridad de los datos:** los datos están protegidos contra cambios o manipulaciones no autorizados. La integridad de los datos los defiende contra riesgos de seguridad como la manipulación, donde alguien intercepta y modifica la información sin estar autorizado para ello. Además de proteger los datos que están almacenados en la red, podría necesitar medidas de seguridad adicionales para garantizar la integridad de los datos cuando estos entran en su sistema procedentes de fuentes que no sean de confianza. Cuando los datos que entran en su sistema proceden de una red pública, necesitará métodos de seguridad para realizar estas tareas:
 - Proteger los datos para que no se puedan husmear ni interpretar, lo que se suele hacer cifrándolos.
 - Asegurar que las transmisiones no han sido alteradas (integridad de los datos).
 - Demostrar que se ha producido la transmisión (no repudio). En el futuro, es posible que necesite el equivalente electrónico del correo certificado.
- **Integridad del sistema:** el sistema proporciona resultados coherentes con el rendimiento esperado. En el caso del sistema operativo i5/OS, la integridad del sistema es el componente de seguridad más vigilado, porque es una parte fundamental de la arquitectura del i5/OS. Por ejemplo, la arquitectura del i5/OS dificulta enormemente que los intrusos puedan imitar o cambiar un programa del sistema operativo cuando se utiliza el nivel de seguridad 40 ó 50.

No repudio

Prueba de que se ha producido una transacción o de que se ha enviado o recibido un mensaje. El

uso de certificados digitales y de la criptografía de claves públicas para firmar transacciones, mensajes y documentos es la base del no repudio. El remitente y el destinatario están ambos de acuerdo en que el intercambio tiene lugar. La firma digital de los datos es una prueba suficiente.

Confidencialidad

Es la seguridad de que la información confidencial permanece privada y no es visible para los escuchas intrusos. La confidencialidad es fundamental para la seguridad total de los datos. El cifrado de los datos con certificados digitales y la capa de sockets segura (SSL) o con una conexión de redes privadas virtuales (VPN) permite asegurar la confidencialidad al transmitir datos entre varias redes que no sean de confianza. La política de seguridad debe indicar qué métodos se emplearán para proporcionar la confidencialidad de la información dentro de la red y de la información que sale de ella.

Actividades de seguridad de auditoría

Consisten en supervisar los eventos relacionados con la seguridad para proporcionar un archivo de anotaciones de los accesos satisfactorios y de los no satisfactorios (denegados). Los registros de accesos satisfactorios indican quién está haciendo cada tarea en los sistemas. Los registros de accesos no satisfactorios (denegados) indican que alguien está intentando abrirse paso a través de las barreras de seguridad del sistema o que alguien tiene dificultades para acceder al sistema.

Conceptos relacionados

“Consideraciones sobre System i y la seguridad en Internet” en la página 2

Los problemas de seguridad relacionados con Internet son muchos. En este tema se proporciona una visión general de las ventajas de la seguridad del i5/OS y de sus ofertas en materia de seguridad.

“Seguridad basada en la defensa por capas” en la página 4

La política de seguridad define qué es lo que desea proteger y qué espera de los usuarios del sistema.

Configurar DCM

Capa de sockets segura (SSL)

“Escenario: planes de la compañía JKL Toy para el e-business”

Escenario típico de una compañía JKL Toy, que ha decidido ampliar sus objetivos de negocio utilizando Internet, y que podría serle de utilidad si desea establecer sus propios planes para e-business.

Escenario: planes de la compañía JKL Toy para el e-business

Escenario típico de una compañía JKL Toy, que ha decidido ampliar sus objetivos de negocio utilizando Internet, y que podría serle de utilidad si desea establecer sus propios planes para e-business.

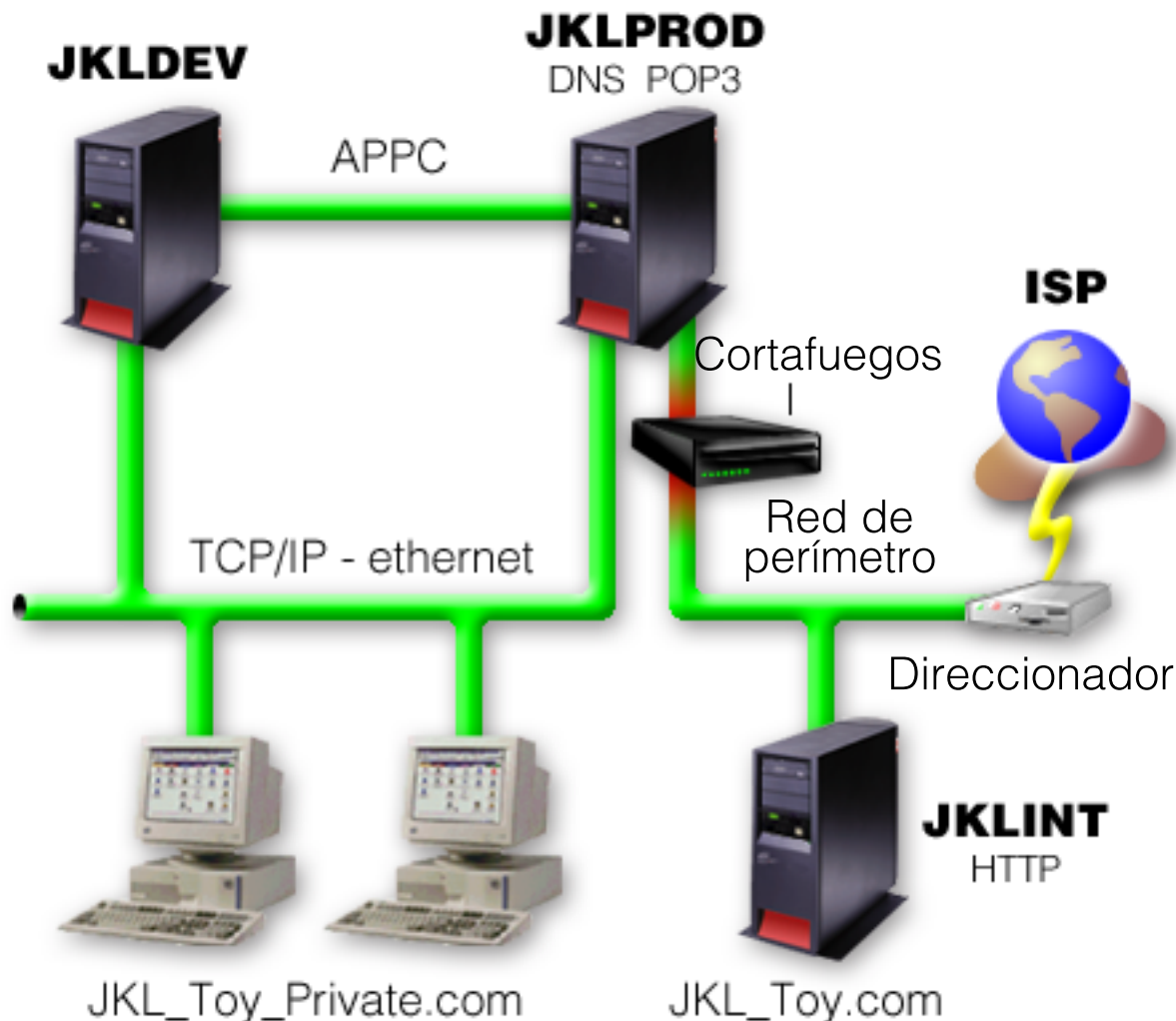
La compañía JKL Toy es un empresa fabricante de juguetes, pequeña pero en rápida expansión. El presidente de la compañía está contento con el crecimiento de la empresa y con las posibilidades que el nuevo sistema operativo i5/OS le ofrece para aliviar la carga de dicho crecimiento. Sharon Jones, directora de contabilidad, se encarga de la administración y la seguridad del sistema.

La compañía JKL Toy ha utilizado con éxito su política de seguridad para las aplicaciones internas durante un año. La compañía tiene previsto ahora configurar una intranet para compartir de forma más eficaz la información interna. También tiene previsto empezar a utilizar Internet para ampliar sus objetivos comerciales. Uno de estos objetivos es crear una presencia corporativa de marketing en Internet incluyendo un catálogo en línea. También desea utilizar Internet para transmitir información confidencial desde sitios remotos a la oficina corporativa. Además, la compañía desea ofrecer acceso a Internet a los empleados del laboratorio de diseño para la investigación y el desarrollo. Por último, la compañía espera que los clientes utilicen su sitio Web para realizar compras directas en línea. Sharon está desarrollando un informe sobre los riesgos potenciales de seguridad de estas actividades y las medidas de seguridad que convendría utilizar para minimizar estos riesgos. Sharon se encarga de actualizar la política de seguridad de la compañía y de poner en práctica las medidas de seguridad que la compañía decida utilizar.

Los objetivos de esta mayor presencia en Internet son los siguientes:

- Promover la presencia de una imagen corporativa general como parte de una campaña global de marketing.
- Proporcionar un catálogo de productos en línea para los clientes y el personal de ventas.
- Mejorar el servicio al consumidor.
- Proporcionar a los empleados acceso a la Web y al correo electrónico.

Una vez comprobada la seguridad básica del sistema, la compañía JKL Toy ha decidido adquirir y utilizar un producto cortafuegos para proporcionar protección a nivel de red. El cortafuegos protegerá la red interna de numerosos riesgos potenciales relacionados con Internet. En la siguiente figura se describe la configuración de red o de Internet de la compañía.



Como se ve en la figura, la compañía JKL Toy tiene dos sistemas primarios. Uno de ellos se utiliza para aplicaciones de desarrollo (JKLDEV) y el otro para aplicaciones de producción (JKLPROD). Los dos sistemas manejan datos y aplicaciones críticas del negocio. Por lo tanto, la compañía no se siente segura al ejecutar las aplicaciones de Internet en estos sistemas. Han optado por añadir un nuevo sistema (JKLINT) para que ejecute estas aplicaciones.

La compañía ha colocado el nuevo sistema en una red de perímetro y está utilizando un cortafuegos entre ella y la red interna principal de la compañía para asegurar una separación más eficaz entre la red e Internet. Esta separación disminuye los riesgos de Internet a los que son vulnerables los sistemas internos de la compañía. Al designar este nuevo sistema como servidor solo de Internet, la compañía también disminuye la complejidad que supone gestionar la seguridad de la red.

La compañía no ejecutará aplicaciones de misión crítica en el nuevo sistema en este momento. Durante esta etapa de elaboración de planes para el e-business, el nuevo sistema solo proporciona un sitio Web público estático. No obstante, la compañía desea implantar medidas de seguridad para proteger el sistema y el sitio Web público que ejecuta con el fin de impedir que se produzcan interrupciones del servicio y otros posibles ataques. Por lo tanto, la compañía protegerá el sistema con reglas de filtrado de paquetes y reglas de conversión de direcciones de red (NAT), así como con potentes medidas de seguridad básica.

A medida que la compañía desarrolle aplicaciones públicas más avanzadas (como un sitio Web de comercio electrónico o el acceso a una extranet), se implantarán medidas de seguridad más avanzadas.

Conceptos relacionados

“Política y objetivos de seguridad” en la página 6

La política de seguridad define qué es lo que desea proteger, y los objetivos de seguridad expresan lo que espera de los usuarios del sistema.

“Consideraciones sobre System i y la seguridad en Internet” en la página 2

Los problemas de seguridad relacionados con Internet son muchos. En este tema se proporciona una visión general de las ventajas de la seguridad del i5/OS y de sus ofertas en materia de seguridad.

“Opciones de seguridad de la red” en la página 11

Para proteger los recursos internos, elija las medidas de seguridad pertinentes a nivel de red.

“Opciones de seguridad de la transmisión” en la página 24

Para proteger los datos cuando fluyen por una red que no sea de confianza, como Internet, debe aplicar las medidas de seguridad pertinentes. Estas medidas son la capa de sockets segura (SSL), System i Access para Windows y las conexiones de redes privadas virtuales (VPN).

Niveles de seguridad para la disponibilidad básica de Internet

Antes de conectarse a Internet, debe determinar qué nivel de seguridad necesita adoptar para proteger el sistema.

Las medidas de seguridad del sistema representan la última línea de defensa contra un problema de seguridad relacionado con Internet. El primer paso de una estrategia de seguridad total de Internet debe ser configurar debidamente los valores de la seguridad básica del i5/OS. Para garantizar que la seguridad del sistema responde a los requisitos mínimos, realice estas tareas:

- Establezca el nivel de seguridad (valor QSECURITY del sistema) en 50. El nivel de seguridad 50 proporciona el máximo nivel de protección de la integridad, que es el valor sugerido para proteger el sistema en entornos de alto riesgo, como Internet.

Nota: Si está ejecutando un nivel de seguridad menor que 50, es posible que tenga que actualizar los procedimientos de funcionamiento o las aplicaciones. Debe revisar el manual de consulta de seguridad de System i antes de pasar a un nivel de seguridad mayor.

- Configure los valores del sistema relacionados con la seguridad para que sean al menos tan restrictivos como los valores recomendados. Puede utilizar el asistente de seguridad de System i Navigator para configurar los valores de seguridad recomendados.
- Asegúrese de que ninguno de los perfiles de usuario, ni siquiera los suministrados por IBM, tenga contraseñas por omisión. El mandato ANZDFTPWD (Analizar contraseñas por omisión) le permitirá comprobar si tiene contraseñas por omisión.
- Utilice la autorización sobre objeto para proteger los recursos importantes del sistema. Aplique un enfoque restrictivo en el sistema. Esto es, restrinja por defecto a todos los usuarios (PUBLIC *EXCLUDE) el uso de recursos del sistema como las bibliotecas y los directorios. Autorice solamente a algunos usuarios a acceder a los recursos restringidos. La restricción del acceso mediante menús no es suficiente en un entorno de Internet.
- Debe configurar la autorización sobre objetos en el sistema.

Como ayuda para configurar estos requisitos mínimos de seguridad del sistema, puede utilizar el planificador de seguridad de eServer o el asistente de seguridad, disponible en la interfaz de System i Navigator. El planificador de seguridad le proporciona un conjunto de recomendaciones de seguridad en función de lo que responda a una serie de preguntas. Luego podrá utilizar las recomendaciones para configurar los valores de seguridad del sistema que necesite. A diferencia de lo que sucede con el planificador de seguridad, el asistente utiliza las recomendaciones para configurar automáticamente los valores de seguridad del sistema.

Las características de seguridad inherentes del i5/OS, cuando estén debidamente configuradas y gestionadas, le proporcionan capacidad para minimizar numerosos riesgos. No obstante, cuando conecte el sistema a Internet, deberá proporcionar medidas de seguridad adicionales que garanticen la seguridad de la red interna. Tras haberse asegurado de que el sistema dispone de una buena seguridad general a nivel del sistema, ya estará listo para configurar medidas de seguridad adicionales como parte del plan de seguridad global para el uso de Internet.

Conceptos relacionados

“Seguridad basada en la defensa por capas” en la página 4

La política de seguridad define qué es lo que desea proteger y qué espera de los usuarios del sistema.

Referencia relacionada

Valor de sistema de nivel de seguridad

Security reference

Opciones de seguridad de la red

Para proteger los recursos internos, elija las medidas de seguridad pertinentes a nivel de red.

Cuando se conecte a una red que no sea de confianza, su política de seguridad debe describir un esquema de seguridad exhaustivo que incluya las medidas de seguridad que va a establecer a nivel de red. La instalación de un cortafuegos es uno de los mejores medios para desplegar un conjunto completo de medidas de seguridad en la red.

El proveedor de servicios de Internet (ISP) puede proporcionar una parte importante del plan de seguridad de la red. El esquema de seguridad de la red debe indicar qué medidas de seguridad proporcionará el ISP, como las reglas de filtrado para la conexión del direccionador del ISP y las medidas de precaución del servicio de nombres de dominio (DNS) público.

Aunque el cortafuegos representa una de las mejores líneas de defensa del plan general de seguridad, no debe ser la única. Como los riesgos potenciales de Internet se pueden producir en varios niveles, deberá configurar medidas de seguridad que ofrezcan múltiples capas de defensa contra los riesgos.

Plantéese la posibilidad de usar un producto cortafuegos como línea de defensa principal siempre que conecte el sistema o la red interna a Internet. Aunque ya no se puede adquirir el producto IBM Firewall para i5/OS y el soporte del product ha dejado de estar disponible, existen otros productos que sí se pueden utilizar.

Como los productos cortafuegos del mercado proporcionan una amplia gama de tecnologías de seguridad de red, la compañía JKL Toy ha elegido uno para proteger su red. El cortafuegos que eligieron no protege el sistema operativo, por lo que han añadido la característica de seguridad adicional proporcionada al utilizar las reglas de paquetes de i5/OS. Ello les permite crear reglas de filtros y de NAT para controlar el tráfico del servidor Internet.

Conceptos relacionados

“Seguridad basada en la defensa por capas” en la página 4

La política de seguridad define qué es lo que desea proteger y qué espera de los usuarios del sistema.

“Escenario: planes de la compañía JKL Toy para el e-business” en la página 8
Escenario típico de una compañía JKL Toy, que ha decidido ampliar sus objetivos de negocio utilizando Internet, y que podría serle de utilidad si desea establecer sus propios planes para e-business.

Detección de intrusiones

Información relacionada



Redbook: All You Need to Know When Migrating from IBM Firewall for AS/400

Cortafuegos

El cortafuegos es una barrera entre una red interna segura y una red que no sea de confianza, como Internet.

La mayoría de las compañías utilizan un cortafuegos para conectar sin peligro la red interna segura a Internet, aunque el cortafuegos también sirve para proteger una red interna frente a otra.

El cortafuegos proporciona un único punto de contacto controlado (llamado *punto de estrangulamiento*) entre la red interna segura y la red que no es de confianza. Las funciones del cortafuegos son:

- Permitir a los usuarios de la red interna utilizar los recursos situados fuera de la red.
- Impedir que los usuarios no autorizados de la red externa puedan utilizar los recursos de la red interna.

Cuando se utiliza un cortafuegos como pasarela a Internet (o a otras redes), se reduce el riesgo de la red interna. El uso del cortafuegos también facilita la administración de la seguridad de la red, ya que sus funciones llevan a cabo muchas de las directivas de la política de seguridad.

Cómo funciona un cortafuego

Para entender cómo funciona un cortafuegos, imagine que la red es un edificio cuyo acceso quiere controlar. El edificio tiene una sala de recepción como único punto de entrada. En esta sala de recepción, hay recepcionistas que dan la bienvenida a los visitantes, guardias de seguridad que vigilan a los visitantes, cámaras para grabar las acciones de los visitantes y lectores de identificadores para autenticar a los visitantes que entran en el edificio.

Estas medidas podrían funcionar correctamente para controlar el acceso al edificio. Sin embargo, si una persona no autorizada consigue entrar en el edificio, no habrá ninguna manera de proteger el edificio contra las acciones del intruso. Sin embargo, si supervisa los movimientos del intruso, es probable que pueda detectar sus actividades sospechosas.

Componentes del cortafuegos

El cortafuegos es un conjunto de piezas de hardware y aplicaciones de software que, utilizadas conjuntamente, impiden el acceso no autorizado a una parte de la red. El cortafuegos está formado por los siguientes componentes:

- **Hardware**

El hardware del cortafuegos suele constar de una máquina independiente o un dispositivo dedicado para ejecutar las funciones del software del cortafuegos.

- **Software**

El software del cortafuegos proporciona una amplia variedad de aplicaciones. En términos de seguridad de la red, el cortafuegos proporciona, mediante diversas tecnologías, estos controles de seguridad:

- filtrado de paquetes de protocolo de Internet (IP)
- Servicios de conversión de direcciones de red (NAT)

- Servidor SOCKS
- Servidores proxy para distintos servicios, como HTTP, Telnet, FTP, etcétera
- Servicios de retransmisión de correo
- Sistema de nombres de dominio (DNS) dividido
- Archivos de anotaciones
- Supervisión en tiempo real

Nota: Algunos cortafuegos proporcionan servicios de redes privadas virtuales (VPN) que le permiten configurar sesiones cifradas entre el cortafuegos y otros cortafuegos compatibles.

Utilización de las tecnologías de cortafuegos

Los servidores proxy de cortafuegos, los servidores SOCKS o las reglas NAT permiten proporcionar a los usuarios internos un acceso seguro a los servicios de Internet. Los servidores proxy y SOCKS desglosan las conexiones TCP/IP en el cortafuegos para ocultar información de la red interna a la red que no es de confianza. Los servidores también proporcionan funciones adicionales de archivos de anotaciones.

Puede utilizar NAT para ofrecer a los usuarios de Internet un acceso fácil al sistema público situado detrás del cortafuegos. El cortafuegos aún protege la red, porque NAT oculta las direcciones IP internas.

El cortafuegos también puede proteger información interna si utiliza un servidor DNS. De hecho, tiene dos servidores DNS: uno que se utiliza para los datos relacionados con la red interna y otro, situado en el cortafuegos, para los datos relacionados con las redes externas y el propio cortafuegos. Esto le permite controlar el acceso externo a la información relacionada con los sistemas internos.

Cuando define una estrategia de cortafuegos, tal vez piense que es suficiente con prohibir todo aquello que represente un riesgo para la organización y permitir todo lo demás. Sin embargo, como los delincuentes informáticos están creando constantemente nuevos métodos de ataque, conviene que se anticipe a ellos para impedir que se salgan con la suya. Al igual que en el ejemplo del edificio, también necesitará supervisar en busca de signos que indiquen que alguien, de alguna manera, ha burlado las defensas. Normalmente, es mucho más perjudicial y costoso recuperar el sistema ante una invasión que prevenirla.

En el caso del cortafuegos, la mejor estrategia es permitir solo aquellas aplicaciones que hayan sido comprobadas y que sean de confianza. Si sigue esta estrategia, deberá definir de modo exhaustivo la lista de servicios que desea ejecutar en el cortafuegos. Puede caracterizar cada servicio con la dirección de la conexión (de dentro a fuera o de fuera a dentro). También debe crear una lista con los usuarios a los que autorizará a utilizar cada servicio y las máquinas que pueden emitir una conexión para el servicio.

¿Qué puede hacer un cortafuegos para proteger la red?

El cortafuegos se instala entre la red y el punto de conexión a Internet (o a otra red que no sea de confianza). Luego podrá limitar los puntos de entrada a la red. El cortafuegos proporciona un único punto de contacto (llamado punto de estrangulamiento) entre la red e Internet. El hecho de tener un solo punto de contacto le da más control sobre qué tráfico puede entrar y salir de la red.

El cortafuegos aparece como una dirección única a la vista del público. Proporciona acceso a la red que no es de confianza mediante los servidores proxy o SOCKS o mediante la conversión de direcciones de red (NAT), a la vez que oculta las direcciones de la red interna. De esta forma, el cortafuegos mantiene la privacidad de la red interna. El mantenimiento de la privacidad de la información de la red es uno de los métodos que utiliza el cortafuegos para disminuir la probabilidad de que se lleven a cabo ataques de imitación (usurpación).

Un cortafuegos permite controlar el tráfico hacia dentro y hacia fuera de la red para minimizar el riesgo de ataques. Filtra de forma segura todo el tráfico que entra en la red, para que solo puedan entrar tipos

determinados de tráfico con destinos específicos. Así se minimiza el riesgo de que se utilice Telnet o el protocolo de transferencia de archivos (FTP) para acceder a los sistemas internos.

¿Qué es lo que no puede hacer un cortafuegos para proteger la red?

El cortafuegos, si bien proporciona una gran protección contra algunos tipos de ataques, solo es una parte de la solución total de seguridad. Por ejemplo, el cortafuegos no necesariamente podrá proteger los datos que se envíen por Internet mediante aplicaciones como las de correo de protocolo simple de transferencia de correo (SMTP), FTP y Telnet. A menos que opte por cifrar esos datos, cualquier persona podrá acceder a ellos desde Internet mientras viajan a su destino.

Reglas de paquetes de i5/OS

Puede utilizar las reglas de paquetes de i5/OS para proteger el sistema. Las reglas de paquetes son funciones del sistema operativo i5/OS y están disponibles en la interfaz de System i Navigator.

Puede utilizar las reglas de paquetes para configurar dos tecnologías de seguridad de red centrales que controlan el flujo del tráfico TCP/IP:

- Conversión de direcciones de red (NAT)
- Filtrado de paquetes IP

La NAT y el filtrado IP están integrados en el sistema operativo i5/OS, por lo que representan una forma económica de proteger el sistema. En algunos casos, estas tecnologías de seguridad pueden ofrecer todo lo necesario sin que tenga que adquirir nuevos componentes. No obstante, estas tecnologías no crean un cortafuegos totalmente funcional. Puede utilizar la seguridad de paquetes IP aisladamente o junto con un cortafuegos, en función de las necesidades de seguridad y de los objetivos.

Nota: La seguridad del sistema debe prevalecer sobre el coste. Para asegurar la protección máxima del sistema de producción, plantéese la posibilidad de usar un cortafuegos.

Conversión de direcciones de red (NAT) y filtrado de paquetes IP

La conversión de direcciones de red (NAT) cambia la dirección IP de origen o de destino de los paquetes que fluyen a través del sistema. La NAT proporciona una alternativa más transparente a los servidores proxy y SOCKS de un cortafuegos. La NAT también puede simplificar la configuración de la red, ya que permite conectar redes con estructuras de dirección incompatibles. Por lo tanto, podrá utilizar las reglas NAT para que el sistema operativo i5/OS funcione como pasarela entre dos redes que tengan esquemas de direcciones incompatibles o en conflicto. También podrá emplear la NAT para ocultar las direcciones IP reales de una red, o sustituir de forma dinámica una o más direcciones por las reales. Como el filtrado de paquetes IP y la conversión de direcciones de red se complementan, a menudo podrá utilizarlos conjuntamente para mejorar la seguridad del sistema.

La utilización de NAT también facilita el funcionamiento de un servidor Web público detrás de un cortafuegos. Las direcciones IP públicas del servidor Web se convierten en direcciones IP internas privadas. De esta forma se reduce el número de direcciones IP registradas que se necesitan y se minimiza el efecto que ello tiene en la red existente. Además proporciona un mecanismo para que los usuarios internos puedan acceder a Internet, manteniendo ocultas las direcciones IP internas privadas.

Filtrado de paquetes IP permite bloquear de forma selectiva o proteger el tráfico IP en función de la información de las cabeceras de los paquetes. Puede utilizar el asistente de configuración de Internet de System i Navigator para configurar de forma rápida y sencilla las reglas de filtrado básicas para bloquear el tráfico de red no deseado.

Puede utilizar el filtrado de paquetes IP para realizar las siguientes tareas:

- Crear un conjunto de reglas de filtrado para especificar a qué paquetes IP se permite entrar en la red y a cuáles se les deniega el acceso a la red. Cuando crea las reglas de filtrado, las aplica a una interfaz

física (por ejemplo, a una línea Token Ring o Ethernet). Podrá aplicar las reglas a múltiples interfaces físicas o bien aplicar reglas diferentes a cada interfaz.

- Crear reglas para permitir o denegar paquetes específicos, tomando como base la siguiente información de cabecera:
 - Dirección IP de destino
 - Protocolo de direcciones IP de origen (por ejemplo, TCP, UDP, etcétera)
 - Puerto de destino (por ejemplo, el puerto 80 para HTTP)
 - Puerto de origen
 - Dirección de datagrama IP (entrante o saliente)
 - Reenviado o local
- Impedir que el tráfico no deseado o innecesario llegue a las aplicaciones del sistema. También puede impedir que el tráfico se reenvíe a otros sistemas. Esto incluye los paquetes de protocolo Internet de mensajes de control (ICMP) de bajo nivel (por ejemplo, paquetes PING) para los que no se necesita ningún servidor de aplicaciones específico.
- Especificar si una regla de filtrado crea una entrada de archivo de anotaciones con información sobre los paquetes que coincidan con la regla en un diario del sistema. Cuando la información se haya escrito en un diario del sistema, no podrá cambiar la entrada del archivo de anotaciones. El archivo de anotaciones es una herramienta ideal para auditar la actividad de la red.

Con las reglas de filtrado de paquetes, podrá proteger los sistemas informáticos, rechazando o aceptando los paquetes IP según los criterios que haya definido. Las reglas de NAT le permiten ocultar la información interna del sistema a los usuarios externos, sustituyendo una dirección IP pública de la información de direcciones IP internas. Aunque las reglas de NAT y de filtrado de paquetes IP constituyen una tecnología básica de seguridad de la red, no pueden ofrecer el mismo nivel de seguridad que un cortafuegos totalmente funcional. Debe analizar detenidamente las necesidades y los objetivos de seguridad para decidirse entre un producto cortafuegos completo o la característica de reglas de paquetes del i5/OS.

Conceptos relacionados

Conversión de direcciones de red (NAT)

Filtrado de paquetes IP

Detección de intrusiones

La *detección de intrusiones* implica reunir información sobre los intentos de acceso no autorizados y los ataques que se perpetran por medio de la red TCP/IP. La política de seguridad global puede constar de una sección dedicada a la detección de intrusiones.

El término *detección de intrusiones* tiene dos sentidos en la documentación de i5/OS. En el primer sentido, la detección de intrusiones se refiere a la prevención y detección de riesgos de seguridad. Por ejemplo, un pirata informático podría intentar introducirse en el sistema utilizando un ID de usuario no válido, o un usuario sin experiencia con demasiada autorización podría modificar objetos importantes de las bibliotecas del sistema.

En el segundo sentido, la detección de intrusiones se refiere a la nueva función de detección que utiliza políticas para supervisar el tráfico sospechoso del sistema. Puede crear una política de detección de intrusiones que audite los eventos de intrusión sospechosos que entran a través de la red TCP/IP.

Elegir opciones de seguridad de red para i5/OS

Debe elegir las opciones de seguridad de red de acuerdo con sus planes de uso de Internet.

Las soluciones de seguridad de red que permiten defenderse contra el acceso no autorizado se basan generalmente en las tecnologías de cortafuegos. Para proteger el sistema, puede utilizar un producto cortafuegos de funcionalidad completa o bien poner en vigor tecnologías de seguridad de red específicas

como parte de la implementación TCP/IP del i5/OS. Esta implementación está formada por la característica de reglas de paquetes (que incluye el filtrado IP y la NAT) y el programa bajo licencia de servidor proxy HTTP para i5/OS.

La elección de la característica de reglas de paquetes o de un cortafuegos depende del entorno de red, de los requisitos de acceso y de las necesidades de seguridad. Debe plantearse la posibilidad de usar un producto cortafuegos como línea de defensa principal siempre que conecte el sistema o la red interna a Internet o a otra red que no sea de confianza.

Un cortafuegos es preferible en este caso, ya que es un dispositivo de hardware y software dedicado con un número limitado de interfaces para el acceso externo. Cuando utiliza tecnologías TCP/IP del i5/OS para la protección del acceso de Internet, está utilizando una plataforma informática de uso general que tiene miles y miles de interfaces y aplicaciones abiertas al acceso externo.

Nota: Es posible que le interese utilizar ambas tecnologías, la de un cortafuegos y la de seguridad de red integrada en el i5/OS. Ello ayuda a proteger el sistema contra los ataques internos (desde detrás del cortafuegos) y de los ataques que podrían penetrar en el cortafuegos debido a una mala configuración o por otros medios.

La diferencia es importante por varias razones. Por ejemplo, un cortafuegos dedicado no proporciona otras funciones o aplicaciones aparte de las que forman el propio cortafuegos. Por lo tanto, si un atacante sorteó con éxito el cortafuegos y consigue acceder a él, el atacante no podrá hacer gran cosa. Mientras que un atacante que consiga sortear las funciones de seguridad de TCP/IP del sistema podría tener acceso potencial a una amplia variedad de aplicaciones, servicios y datos de gran utilidad. Luego el atacante podría emplear todos estos elementos para destruir el propio sistema o para obtener acceso a otros sistemas de la red interna.

Como con todas las opciones de seguridad, deberá basar la decisión en las concesiones que esté dispuesto a hacer entre costes y ventajas de seguridad. Debe analizar los objetivos de su compañía y sopesar qué riesgos está dispuesto a aceptar en beneficio del coste que desea pagar por la seguridad para minimizar estos riesgos. En la siguiente tabla se proporciona información sobre cuándo es mejor utilizar las características de seguridad de TCP/IP o un cortafuegos totalmente funcional. Esta tabla le permitirá determinar si conviene utilizar un cortafuegos, las características de seguridad de TCP/IP o una combinación de ambas tecnologías para garantizar la protección del sistema y de la red.

Tecnología de seguridad	Es mejor utilizar la tecnología TCP/IP del i5/OS	Es mejor usar un cortafuegos totalmente funcional
Filtrado de paquetes IP	<ul style="list-style-type: none"> • Para proporcionar protección adicional a un solo sistema operativo i5/OS, como puede ser un servidor Web público o un sistema de intranet que tenga datos confidenciales. • Para proteger una subred de una intranet corporativa si el sistema operativo i5/OS funciona como pasarela (direccionador de uso ocasional) para el resto de la red. • Para controlar la comunicación con un socio de confianza (en cierta medida) a través de una red privada o de una extranet en la que el sistema operativo i5/OS funciona como pasarela. 	<ul style="list-style-type: none"> • Para proteger toda una red corporativa contra Internet o contra otra red que no sea de confianza a la que su red esté conectada. • Para proteger una subred de gran tamaño que tenga tráfico importante contra el resto de la red corporativa.

Tecnología de seguridad	Es mejor utilizar la tecnología TCP/IP del i5/OS	Es mejor usar un cortafuegos totalmente funcional
Conversión de direcciones de red (NAT)	<ul style="list-style-type: none"> • Para habilitar la conexión de dos redes privadas con estructuras de direcciones incompatibles. • Para ocultar las direcciones de una subred a una red de menor confianza. 	<ul style="list-style-type: none"> • Para ocultar las direcciones de los clientes que acceden a Internet o a otra red que no sea de confianza. Para utilizar una alternativa a los servidores proxy y SOCKS. • Para poner a disposición de los clientes de Internet los servicios de un sistema en una red privada.
Servidor proxy	<ul style="list-style-type: none"> • Para funcionar a modo de proxy en las ubicaciones remotas de una red corporativa cuando el cortafuegos central proporciona acceso a Internet. 	<ul style="list-style-type: none"> • Para funcionar a modo de proxy en toda una red corporativa cuando se accede a Internet.

Referencia relacionada

Filtrado IP y conversión de direcciones de red



HTTP Server para i5/OS

Información relacionada



AS/400 Internet Scenarios: A Practical Approach

Opciones de seguridad de aplicaciones

Dispone de algunas opciones a la hora de gestionar los riesgos de seguridad para numerosas y conocidas aplicaciones y servicios de Internet.

Las medidas de seguridad a nivel de aplicaciones controlan cómo pueden interactuar los usuarios con las aplicaciones concretas. En general, debe configurar valores de seguridad para cada una de las aplicaciones que utilice. Sin embargo, conviene que tome medidas de precaución especiales para configurar la seguridad de las aplicaciones y los servicios que utilizará de Internet o prestará a Internet. Estas aplicaciones y servicios son vulnerables al mal uso por parte de los usuarios no autorizados que buscan una manera de acceder a los sistemas de la red. Las medidas de seguridad que utilice deberán incluir los riesgos del lado del servidor y del lado del cliente.

Aunque es importante proteger todas y cada una de las aplicaciones que emplee, las medidas de seguridad juegan un papel pequeño en la implementación global de la política de seguridad global.

Conceptos relacionados


“Seguridad basada en la defensa por capas” en la página 4

La política de seguridad define qué es lo que desea proteger y qué espera de los usuarios del sistema.

Seguridad del servicio Web

Cuando proporciona acceso a los visitantes de su sitio Web, no exponga a la vista de todos la información sobre cómo está configurado el sitio ni el código que sirve para generar la página. La visita a su página tiene que ser rápida, fácil y sin problemas, todo el trabajo se debe realizar internamente.

Como administrador, debe asegurarse de que las medidas de seguridad no afecten negativamente al sitio Web y que implementen los modelos de seguridad que ha elegido. Para lograrlo, tendrá que elegir entre las características de seguridad incorporadas en IBM HTTP Server para i5/OS.

En el libro rojo IBM HTTP Server (powered by Apache) Redbook  , el capítulo sobre cómo desplegar la seguridad describe cómo utilizar la autenticación, el control de acceso y el cifrado para implementar las características de seguridad.

El protocolo de transferencia de hipertexto (HTTP) le proporciona capacidad para visualizar datos, pero no para alterar los datos que hay en un archivo de base de datos. Sin embargo, en algunas ocasiones es posible que tenga que escribir algunas aplicaciones que deban actualizar un archivo de base de datos. Por ejemplo, supongamos que desea crear formularios que, una vez cumplimentados por los usuarios, actualicen una base de datos del i5/OS. Para hacerlo, puede utilizar los programas de la interfaz de pasarela común (CGI).

Otra característica de seguridad que puede utilizar es el servidor proxy. Este recibe las peticiones destinadas a otros servidores y luego las cumplimenta, reenvía, redirige o rechaza.

El servidor HTTP proporciona un archivo de anotaciones de acceso que le permitirá supervisar los accesos y los intentos de acceso mediante el servidor.

Además de emplear programas CGI en las páginas Web, también puede emplear la programación Java. Antes de añadir Java a las páginas Web, primero debe comprender cómo funciona la seguridad Java.

Conceptos relacionados

“La seguridad Java en Internet”

La programación Java se está extendiendo cada vez más en los entornos informáticos actuales. Debe prepararse para manejar los factores de seguridad asociados a Java.

Información relacionada

Tipos de servidor proxy y usos para HTTP Server (basado en Apache)

Consejos de seguridad para HTTP Server

Interfaz de pasarela común (CGI)

La seguridad Java en Internet

La programación Java se está extendiendo cada vez más en los entornos informáticos actuales. Debe prepararse para manejar los factores de seguridad asociados a Java.

Aunque los cortafuegos son una buena defensa contra la mayoría de los riesgos de seguridad de Internet, no proporcionan protección contra numerosos riesgos que representa la utilización de Java. La política de seguridad debe incluir medidas para proteger el sistema en tres áreas afectadas por el uso de Java: aplicaciones, applets y servlets. Asimismo, conviene comprender cómo interaccionan Java y la seguridad de los recursos en términos de autenticación y autorización de los programas Java.

aplicaciones Java

Como lenguaje de programación, Java incluye algunas características que protegen a los programadores de Java contra errores no intencionados que pueden provocar problemas de integridad. (Los otros lenguajes que se utilizan normalmente para las aplicaciones de PC, como los lenguajes C o C++, no protegen a los programadores contra los errores no intencionados con la misma intensidad que Java). Por ejemplo, Java utiliza una tipificación estricta (la aplicación estricta de reglas de tipos sin excepciones) para proteger al programador contra la utilización de objetos de una forma que no era la prevista. Java no permite la manipulación de punteros, lo que evita que los programadores se salgan accidentalmente de los límites de memoria del programa. Desde la perspectiva del desarrollo de aplicaciones, Java es equivalente a los demás lenguajes de alto nivel. En el diseño de aplicaciones hay que aplicar las mismas reglas de seguridad que las que se aplican con otros lenguajes en el sistema.

Applets Java

Applets Java son pequeños programas Java que se pueden incluir en las páginas HTML que se ejecutan en el cliente, pero tienen potencial para acceder al sistema operativo i5/OS. Un programa ODBC (Open Database Connectivity) o un programa de comunicaciones avanzadas programa a programa (APPC) que funcione en un PC de la red también puede acceder potencialmente al sistema operativo cuando, por ejemplo, el sistema se emplea para servir aplicaciones o se utiliza como servidor Web. En general, los applets Java solo pueden establecer una sesión con el sistema operativo i5/OS en el que se originaron. Por lo tanto, un applet Java solo puede acceder al sistema operativo i5/OS desde un PC conectado cuando el applet procede de ese sistema operativo i5/OS.

El applet puede intentar conectarse a cualquier puerto TCP/IP de un sistema. No hace falta que se comunique con un servidor de software escrito en Java. Pero, en el caso de los sistemas que se hayan escrito con IBM Toolbox para Java, el applet debe proporcionar un ID de usuario y una contraseña cuando establece conexiones de nuevo con el sistema. En esta documentación, todos los sistemas descritos son sistemas operativos i5/OS. (No hace falta que un servidor de aplicaciones Java utilice IBM Toolbox para Java). Por lo general, la clase IBM Toolbox para Java solicita al usuario un ID de usuario y una contraseña en la primera conexión.

El applet únicamente puede realizar funciones en el sistema operativo i5/OS si el perfil de usuario tiene autorización sobre dichas funciones. Por lo tanto, es fundamental que tenga un buen esquema de seguridad de recursos cuando empiece a utilizar applets Java para proporcionar nuevas funciones de aplicaciones. El sistema, cuando procesa las peticiones procedentes de los applets, no utiliza el valor de capacidad limitada que se ha especificado en el perfil de usuario.

El visor de applets le permite someter a prueba un applet en el sistema operativo i5/OS; no obstante, no está sujeto a las restricciones de seguridad del navegador. Por lo tanto, solo debe utilizar el visor de applets para someter a prueba sus propios applets, nunca para ejecutar applets que proceden de fuentes externas. Los applets Java escriben a menudo en la unidad del PC del usuario, lo que ofrece al applet la oportunidad de ejecutar una acción destructiva. Sin embargo, puede utilizar un certificado digital para firmar un applet Java con el objeto de establecer su autenticidad. El applet firmado puede escribir en las unidades locales del PC, aunque el valor predeterminado del navegador no lo permita. El applet firmado también puede escribir en unidades correlacionadas del sistema, ya que estas aparecen en el PC como si fuesen unidades locales.

En el caso de los applets Java originados en el sistema, tal vez tenga que utilizar applets firmados. No obstante, debe indicar a los usuarios que, en general, no acepten applets firmados procedentes de fuentes desconocidas.

A partir de la versión V4R4, puede utilizar IBM Toolbox para Java para configurar un entorno de capa de sockets segura (SSL). También puede utilizar IBM Developer Toolkit para Java para proteger las aplicaciones Java con SSL. La utilización de SSL con las aplicaciones Java garantiza el cifrado de los datos, incluidos los ID de usuario y las contraseñas que pasan entre el cliente y el servidor. Puede utilizar el gestor de certificados digitales (DCM) para configurar los programas Java registrados para que utilicen SSL.

Servlets Java

Los servlets son componentes del lado del servidor escritos en Java que amplían dinámicamente la función de un servidor Web sin cambiar el código del servidor Web. El servidor IBM WebSphere Application Server que viene con IBM Web Enablement para i5/OS proporciona soporte para usar servlets en los sistemas operativos i5/OS.

En los objetos servlet debe utilizar la seguridad de recursos que se utiliza en el sistema. Sin embargo, el hecho de aplicar la seguridad de recursos a un servlet no es una garantía suficiente de que quede protegido. Cuando un servidor Web carga un servlet, la seguridad de recursos no puede impedir que

otros también lo ejecuten. Por lo tanto, además de la seguridad de recursos, conviene que utilice las directivas y los controles de seguridad del servidor HTTP. Por ejemplo, no permita que los servlets se ejecuten únicamente bajo el perfil del servidor Web. También debe utilizar las características de seguridad que ofrecen las herramientas de desarrollo de servlets, como las que se encuentran en WebSphere Application Server para i5/OS.

Consulte estos recursos para obtener más información sobre las medidas de seguridad generales para Java:

- IBM Developer Kit para Java: Seguridad Java.
- IBM Toolbox para Java: Clases de seguridad.
- Consideraciones sobre seguridad para navegadores de Internet.

Autenticación y autorización Java en los recursos

IBM Toolbox para Java contiene clases de seguridad destinadas a verificar la identidad del usuario y para asignar opcionalmente esa identidad a la hebra del sistema operativo de una aplicación o un servlet que se ejecute en un sistema operativo i5/OS. Las comprobaciones posteriores de la seguridad de recursos se producirán bajo la identidad asignada.

IBM Developer Kit para Java proporciona soporte para JAAS (servicio de autorización y autenticación Java, que es una extensión estándar de Java 2 Software Development Kit (J2SDK), Standard Edition. Actualmente, J2SDK proporciona controles de acceso basados en dónde se ha originado el código y en quién lo ha firmado (controles de acceso basados en el origen del código).

Proteger las aplicaciones Java con SSL

Puede utilizar la capa de sockets segura (SSL) para proteger las comunicaciones de las aplicaciones de i5/OS que desarrolle con IBM Developer Kit para Java. Las aplicaciones de cliente que utilizan IBM Toolbox para Java también pueden aprovechar las ventajas de SSL. El proceso de habilitar SSL para sus propias aplicaciones Java es algo distinto del proceso de habilitar SSL para las otras aplicaciones.

Conceptos relacionados

“Seguridad del servicio Web” en la página 17

Cuando proporciona acceso a los visitantes de su sitio Web, no exponga a la vista de todos la información sobre cómo está configurado el sitio ni el código que sirve para generar la página. La visita a su página tiene que ser rápida, fácil y sin problemas, todo el trabajo se debe realizar internamente.

Configurar DCM

Servicios de autenticación

Información relacionada

Servicio de autorización y autenticación Java (JAAS)

Capa de sockets segura (SSL)

Seguridad del correo electrónico

La utilización del correo electrónico por Internet o por otras redes que no sean de confianza supone riesgos de seguridad para su sistema, aunque este esté protegido por un cortafuegos.

Debe conocer estos riesgos para garantizar que su política de seguridad indique cómo minimizarlos.

El correo electrónico es similar a otras formas de comunicación. Es importante ser prudente a la hora de enviar información confidencial por correo electrónico. El correo electrónico viaja a través de numerosos sistemas antes de llegar a su destino, por lo que es posible que alguien lo intercepte y lo lea. Por lo tanto, convendrá que emplee medidas de seguridad para proteger la confidencialidad del correo electrónico.

Riesgos más comunes de la seguridad del correo electrónico

Estos son algunos de los riesgos asociados al uso del correo electrónico:

- La **Inundación** (tipo de ataque de denegación de servicio) se produce cuando un sistema queda sobrecargado con múltiples mensajes de correo electrónico. Para un atacante es relativamente fácil crear un programa sencillo que envíe millones de mensajes de correo electrónico (incluso mensajes vacíos) a un único servidor de correo electrónico para intentar inundarlo. Sin la seguridad correcta, el servidor de destino puede experimentar una denegación de servicio porque el disco de almacenamiento del servidor queda lleno de mensajes inútiles. El sistema también puede dejar de responder porque todos sus recursos están ocupados en procesar el correo del ataque.
- **Correo masivo (spam)** (correo basura) es otro tipo de ataque común dirigido al correo electrónico. Con el aumento del número de empresas que practican el comercio electrónico en Internet, se ha producido una invasión de mensajes comerciales de correo electrónico no deseados o no solicitados. Este es el correo basura, que se envía a una amplia lista de distribución de usuarios de correo electrónico, llenando el buzón de correo de todos los usuarios.
- La **Confidencialidad** es un riesgo asociado al envío de correo electrónico a otra persona a través de Internet. El mensaje de correo electrónico pasa a través de numerosos sistemas antes de llegar al destinatario. Si el mensaje no está cifrado, cualquier pirata informático podría hacerse con él y leerlo en cualquier punto de la ruta de entrega.

Opciones de seguridad del correo electrónico

Para prevenir los riesgos de inundaciones y el correo masivo (spam), debe configurar el servidor de correo electrónico correctamente. La mayoría de las aplicaciones de servidor proporcionan métodos para combatir este tipo de ataques. Asimismo, puede colaborar con el proveedor de servicios de Internet (IPS) para asegurarse de que aporta algún tipo de protección adicional contra estos ataques.

Las medidas de seguridad adicionales que necesite dependerán del nivel de confidencialidad que desee, así como de qué características de seguridad ofrezcan sus aplicaciones de correo electrónico. Por ejemplo, ¿basta con mantener la confidencialidad del contenido del mensaje de correo electrónico?, ¿o bien desea que sea confidencial toda la información asociada al correo electrónico (como las direcciones IP de origen y destino)?

Algunas aplicaciones tienen características de seguridad integradas que tal vez ofrezcan la protección que necesita. Por ejemplo, Lotus Notes Domino proporciona varias características de seguridad integradas, como la capacidad de cifrado de un documento completo o de campos individuales de un documento.

Para cifrar el correo, Lotus Notes Domino crea una clave pública y una clave privada exclusivas para cada usuario. La clave privada se utiliza para cifrar el mensaje, de forma que solo lo podrán leer aquellos usuarios que tengan su clave pública. Debe enviar la clave pública a los destinatarios que desee, para que puedan utilizarla para descifrar la nota cifrada. Si alguien le envía correo cifrado, Lotus Notes Domino utiliza la clave pública del remitente para descifrar automáticamente la nota.

Puede encontrar más información sobre el uso de las características de cifrado de Notes en los archivos de ayuda en línea del programa.

Si desea proporcionar más confidencialidad para el correo electrónico o para otro tipo de información que fluya entre las sucursales, clientes remotos o socios comerciales, tiene dos opciones.

Si SSL está soportado por la aplicación del servidor de correo electrónico, puede utilizar la capa de sockets segura (SSL) para crear una sesión de comunicaciones seguras entre el servidor y los clientes de correo electrónico. SSL también proporciona soporte a la autenticación opcional del lado del cliente, si la aplicación de cliente está escrita para este uso. Como la sesión completa está cifrada, SSL también garantiza la integridad de los datos mientras se estén transmitiendo.

Otra posible opción es configurar una conexión de red privada virtual (VPN). Puede utilizar el sistema para configurar diversas conexiones VPN, incluso entre clientes remotos y su sistema. Cuando se utiliza una conexión VPN, todo el tráfico que fluye entre los extremos de la comunicación está cifrado, lo que garantiza la confidencialidad y la integridad de los datos.

Conceptos relacionados

“Seguridad de FTP”

El protocolo de transferencia de archivos (FTP) permite transferir archivos entre un cliente (un usuario situado en otro sistema) y el servidor. Conviene que comprenda los riesgos de seguridad con los que se puede encontrar al utilizar FTP para asegurarse de que su política de seguridad describe cómo se minimizan los riesgos.

“Seguridad basada en la defensa por capas” en la página 4

La política de seguridad define qué es lo que desea proteger y qué espera de los usuarios del sistema.

Red privada virtual (VPN)

Referencia relacionada

Terminología de seguridad

Información relacionada



Biblioteca de consulta de Lotus Domino



Documentación de Lotus



Lotus Notes and Domino R5.0 Security Infrastructure Revealed, Redbook



Lotus Domino for AS/400 Internet Mail and More, Redbook

Seguridad de FTP

El protocolo de transferencia de archivos (FTP) permite transferir archivos entre un cliente (un usuario situado en otro sistema) y el servidor. Conviene que comprenda los riesgos de seguridad con los que se puede encontrar al utilizar FTP para asegurarse de que su política de seguridad describe cómo se minimizan los riesgos.

También puede utilizar la función de mandatos remotos para enviar mandatos al servidor. Por lo tanto, FTP resulta útil a la hora de trabajar con los sistemas remotos o al mover archivos entre sistemas. Sin embargo, el uso del protocolo FTP por Internet o por otras redes que no sean de confianza le expone a algunos riesgos de seguridad. La comprensión de estos riesgos le ayudará a proteger el sistema.

- Su esquema de autorización sobre objeto podría no ofrecer suficiente protección cuando permite que se ejecute el protocolo de transferencia de archivos en su sistema.

Por ejemplo, supongamos que la autorización de uso público de los objetos sea *USE, pero que se está utilizando la seguridad de menú para impedir que los usuarios accedan a dichos objetos. (La seguridad de menú impide a los usuarios realizar cualquier acción que no esté en sus opciones de menú). Los usuarios de FTP, como no están restringidos a los menús, pueden leer todos los objetos del sistema.

A continuación se proporcionan algunas opciones para controlar este riesgo de seguridad:

- Ponga en vigor la seguridad completa de objetos del i5/OS en el sistema. En otras palabras, cambie el modelo de seguridad del sistema para que de seguridad de menú pase a ser seguridad de objetos. Esta es la opción mejor y más segura.
- Escriba programas de salida para FTP con objeto de restringir el acceso a los archivos que se puedan transferir por FTP. Estos programas de salida deben proporcionar una seguridad que sea como mínimo equivalente a la que proporciona el programa de menú. Es posible que le interese restringir aún más los controles de acceso a FTP. Esta opción solo se aplica a FTP, no a otras interfaces como la conectividad de bases de datos abierta (ODBC), la gestión de datos distribuidos (DDM) o la arquitectura de bases de datos relacionales distribuidas (DRDA).

Nota: La autorización *USE sobre un archivo permite al usuario descargar el archivo. La autorización *CHANGE sobre un archivo permite al usuario subir el archivo.

- Un pirata informático puede montar un ataque de denegación de servicio con el servidor FTP para inhabilitar perfiles de usuario en el sistema. Para ello, se realizan repetidos intentos de inicio de sesión con una contraseña incorrecta de un perfil de usuario, hasta que el perfil queda inhabilitado. Este tipo de ataque inhabilita el perfil de usuario si se alcanza un máximo de tres intentos de inicio de sesión.

Para evitar este riesgo, debe analizar qué concesiones está dispuesto a hacer y qué es preferible: aumentar la seguridad para minimizar los ataques o proporcionar facilidad de acceso a los usuarios. El servidor FTP normalmente pone en vigor el valor QMAXSIGN del sistema para impedir que los piratas informáticos tengan la oportunidad de realizar un número ilimitado de intentos de adivinar la contraseña y montar ataques por contraseña. A continuación se proporcionan algunas opciones que pueden ser de gran ayuda:

- Utilice un programa de salida de inicio de sesión del servidor FTP para rechazar las peticiones de inicio de sesión realizadas por los perfiles de usuario de cualquier sistema y por los perfiles de usuario a los que no desea permitir el acceso por FTP. Cuando se utiliza un programa de salida de este tipo, los intentos de inicio de sesión rechazados por el punto de salida de inicio de sesión de servidor de los perfiles de usuarios que bloquee no se incluyen en la cuenta de QMAXSIGN del perfil.
- Utilice un programa de salida de inicio de sesión del servidor FTP para limitar las máquinas cliente desde las que un perfil de usuario dado puede acceder al servidor FTP. Por ejemplo, si una persona de Contabilidad tiene autorización para acceder por FTP, solo debe permitir que ese perfil de usuario acceda al servidor FTP desde las máquinas que tengan direcciones IP en el departamento de Contabilidad.
- Utilice un programa de salida de inicio de sesión del servidor FTP para anotar el nombre de usuario y la dirección IP de todos los intentos de inicio de sesión de FTP. Revise las anotaciones periódicamente, y siempre que un perfil quede inhabilitado por sobrepasar el número máximo de intentos de contraseña, utilice la información de la dirección IP para identificar al responsable y tomar las medidas adecuadas.
- Utilice el sistema de detección de intrusiones para detectar ataques de denegación de servicio en el sistema.

Además, puede utilizar los puntos de salida del servidor FTP para proporcionar una función FTP anónima a los usuarios invitados. Para configurar un servidor FTP anónimo y seguro se necesitan programas de salida para los puntos de salida de inicio de sesión del servidor FTP y para los de validación de peticiones del servidor FTP.

Puede utilizar la capa de sockets segura (SSL) con objeto de proporcionar sesiones de comunicaciones seguras para el servidor FTP. SSL garantiza que todas las transmisiones de FTP estarán cifradas para mantener la confidencialidad de todos los datos que pasan entre el servidor FTP y el cliente, incluidos los nombres de usuario y las contraseñas. El servidor FTP también da soporte al uso de certificados digitales para la autenticación de los clientes.

Además de estas opciones de FTP, también puede considerar la posibilidad de utilizar FTP anónimo para ofrecer una forma de acceder fácilmente a material no confidencial, cómoda para los usuarios. FTP anónimo permite un acceso no protegido (no se necesita contraseña) a información seleccionada sobre un sistema remoto. El sitio remoto determina la información que se pone a disposición del acceso general. Esta información se considera de acceso público y cualquier usuario puede leerla. Antes de configurar FTP anónimo, pondere los riesgos de seguridad y considere la posibilidad de proteger el servidor FTP con programas de salida.

Conceptos relacionados

“Seguridad del correo electrónico” en la página 20

La utilización del correo electrónico por Internet o por otras redes que no sean de confianza supone riesgos de seguridad para su sistema, aunque este esté protegido por un cortafuegos.

Tareas relacionadas

Configurar el protocolo de transferencia de archivos (FTP) anónimo

Gestionar el acceso utilizando programas de salida de protocolo de transferencia de archivos (FTP)

Información relacionada

Proteger FTP

Utilizar SSL para proteger el servidor FTP

Opciones de seguridad de la transmisión

Para proteger los datos cuando fluyen por una red que no sea de confianza, como Internet, debe aplicar las medidas de seguridad pertinentes. Estas medidas son la capa de sockets segura (SSL), System i Access para Windows y las conexiones de redes privadas virtuales (VPN).

Recuerde que el escenario de la compañía JKL Toy tiene dos sistemas primarios. Uno de ellos se utiliza para el desarrollo y el otro para las aplicaciones de producción. Los dos sistemas manejan datos y aplicaciones críticas del negocio. Por lo tanto, la compañía opta por añadir un nuevo sistema en una red de perímetro para manejar las aplicaciones de Internet y de la intranet.

El establecimiento de una red de perímetro garantiza en parte una separación física entre la red interna e Internet. Esta separación disminuye los riesgos de Internet a los que son vulnerables los sistemas internos de la compañía. Al designar este nuevo sistema como servidor solo de Internet, la compañía también disminuye la complejidad que supone gestionar la seguridad de la red.

Debido a la necesidad generalizada de obtener seguridad en los entornos de Internet, IBM no cesa de desarrollar ofertas de seguridad para garantizar un entorno de red seguro en el que llevar negocios electrónicos (e-business) en Internet. Para los entornos de Internet se necesita la seguridad específica del sistema y la seguridad específica de las aplicaciones. Sin embargo, el movimiento de información confidencial a través de la intranet de la compañía o de la conexión a Internet aumenta aún más si cabe la necesidad de desarrollar soluciones de seguridad más potentes. Para combatir estos riesgos, debe implantar medidas de seguridad que protejan la transmisión de los datos mientras viajan por Internet.

Los riesgos asociados a mover información entre sistemas que no sean de confianza se pueden minimizar con dos ofertas de seguridad específicas a nivel de transmisión para el sistema operativo i5/OS: comunicaciones seguras SSL y conexiones VPN.

El protocolo SSL es un estándar del sector para proteger las comunicaciones entre clientes y servidores. SSL se desarrolló originalmente para las aplicaciones de navegador Web, pero son cada vez más las aplicaciones que pueden utilizar SSL. En el caso del sistema operativo i5/OS, son las siguientes:

- IBM HTTP Server para i5/OS (original y basado en Apache)
- Servidor FTP
- Servidor Telnet
- La arquitectura de bases de datos relacionales distribuidas (DRDA) y el servidor de gestión de datos distribuidos (DDM)
- Management Central de System i Navigator
- Servidor de servicios de directorio (LDAP)
- Aplicaciones System i Access para Windows, incluido System i Navigator, y aplicaciones escritas en el conjunto de interfaces de programación de aplicaciones (API) de System i Access para Windows
- Programas desarrollados con Developer Kit para Java y aplicaciones de cliente que utilizan IBM Toolkit para Java
- Programas desarrollados con las interfaces de programación de aplicaciones (API) de la capa de sockets segura (SSL), que sirven para habilitar SSL en las aplicaciones. En el tema Interfaces API de la capa de sockets segura (SSL) hallará más información sobre cómo escribir programas que empleen SSL.

Algunas de estas aplicaciones también dan soporte al uso de certificados digitales para la autenticación del cliente. SSL se basa en los certificados digitales para autenticar a los interlocutores de la comunicación y crear una conexión segura.

Redes privadas virtuales (VPN)

Puede utilizar las conexiones VPN para establecer un canal de comunicaciones seguro entre dos puntos finales. Al igual que en las conexiones SSL, los datos que viajan entre los extremos se pueden cifrar para garantizar así la confidencialidad y la integridad de los datos. Sin embargo, las conexiones VPN le permiten limitar el flujo del tráfico en los extremos que especifique y restringir el tipo de tráfico que puede usar la conexión. Por lo tanto, las conexiones VPN proporcionan seguridad a nivel de red, ayudándole a proteger los recursos de la red contra el acceso no autorizado.

Qué método debe utilizar

Ambos métodos, SSL y VPN, responden a la necesidad de una autenticación segura, de la confidencialidad de los datos y de su integridad. La elección de uno de los dos depende de varios factores. Debe tener en cuenta con quién se está comunicando, qué aplicaciones utiliza para comunicarse, qué grado de seguridad necesita para la comunicación y qué concesiones está dispuesto a hacer entre coste y rendimiento para proteger la comunicación.

Asimismo, si desea utilizar una aplicación específica con SSL, deberá configurarla para que emplee SSL. Aunque hay algunas aplicaciones que no pueden aprovechar las ventajas de SSL, muchas otras, como Telnet y System i Access para Windows, tienen capacidad para SSL. Sin embargo, las redes VPN permiten proteger todo el tráfico IP que fluye entre extremos específicos de la conexión.

Por ejemplo, actualmente puede utilizar HTTP a través de SSL para permitir a los socios comerciales comunicarse con un servidor Web en la red interna. Si el servidor Web es la única aplicación segura que necesita entre usted y el socio comercial, tal vez no le interese pasar a una conexión VPN. Sin embargo, si se propone ampliar las comunicaciones, sí que le interesará utilizar una conexión VPN. Asimismo, puede darse el caso de que necesite proteger el tráfico en una parte de la red, pero que no desee configurar individualmente cada cliente y cada servidor para que utilicen SSL. Puede crear una conexión VPN de pasarela a pasarela para esa parte de la red. De esta manera protegería el tráfico, pero la conexión sería transparente para los servidores y clientes individuales situados a cada lado de la conexión.

Conceptos relacionados

“Seguridad basada en la defensa por capas” en la página 4

La política de seguridad define qué es lo que desea proteger y qué espera de los usuarios del sistema.

“Escenario: planes de la compañía JKL Toy para el e-business” en la página 8

Escenario típico de una compañía JKL Toy, que ha decidido ampliar sus objetivos de negocio utilizando Internet, y que podría serle de utilidad si desea establecer sus propios planes para e-business.

Referencia relacionada

Interfaces API de sockets seguros

Información relacionada

Capa de sockets segura (SSL)

Redes privadas virtuales (VPN)

Utilizar certificados digitales para SSL

Los certificados digitales proporcionan el principio básico para utilizar la capa de sockets segura (SSL) con objeto de obtener comunicaciones seguras y son un medio de autenticación más potente.

El sistema operativo i5/OS le permite crear y gestionar fácilmente certificados digitales para los sistemas y usuarios con el gestor de certificados digitales (DCM), una característica integrada de i5/OS.

Además, puede configurar algunas aplicaciones, como IBM HTTP Server para i5/OS, para que utilicen certificados digitales como método más potente de autenticación de cliente, en lugar de usar tan solo el nombre de usuario y las contraseñas.

Qué es un certificado digital

Certificado digital es una credencial digital que valida la identidad del propietario del certificado, de manera muy parecida a como lo hace un pasaporte. Un tercero de confianza, llamada autoridad certificadora (CA), emite certificados digitales para los usuarios y servidores. La confianza en la CA es la base de la confianza en el certificado como credencial válida.

Cada CA tiene una política para determinar qué información de identificación exige la CA para emitir un certificado. Algunas CA de Internet pueden exigir poca información, como las que tan solo exigen un nombre distinguido. Nombre distinguido es el nombre de la persona o del sistema para el que la CA emite una dirección de certificado digital y una dirección de correo electrónico digital. Para cada certificado se generan una clave privada y una clave pública. El certificado contiene la clave pública, mientras que el navegador o un archivo seguro almacena la clave privada. Los pares de claves asociados al certificado pueden utilizarse para firmar y cifrar datos (como mensajes y documentos) que se envían entre los usuarios y los servidores. Las firmas digitales garantizan la fiabilidad del origen de un elemento y protegen su integridad.

Aunque hay algunas aplicaciones que no pueden aprovechar las ventajas de SSL, muchas otras, como Telnet y System i Access para Windows, tienen capacidad para SSL.

Conceptos relacionados

Configurar DCM

Capa de sockets segura (SSL)

Referencia relacionada

Terminología de seguridad

Capa de sockets segura (SSL) para proteger el acceso a Telnet

Puede configurar el servidor Telnet para que utilice la capa de sockets segura (SSL) con el fin de proteger las sesiones de comunicaciones Telnet.

Si desea configurar el servidor Telnet para que utilice SSL, debe emplear el gestor de certificados digitales (DCM) para configurar el certificado que utilizará el servidor Telnet. Por omisión, el servidor Telnet maneja las conexiones seguras y las no seguras. Sin embargo, podrá configurar Telnet para que solo permita las sesiones Telnet seguras. Además, podrá configurar el servidor Telnet para que utilice certificados digitales con objeto de obtener medidas más potentes de autenticación de los clientes.

Cuando opta por usar SSL con Telnet, obtiene algunas ventajas importantes de seguridad. En Telnet, además de la autenticación del servidor, los datos se cifran antes de que fluyan por el protocolo Telnet. Cuando haya establecido la sesión SSL, se cifrarán todos los datos de los protocolos Telnet, incluido el intercambio de ID de usuario y contraseña.

El factor más importante a tener en cuenta cuando se utiliza el servidor Telnet es la confidencialidad de la información utilizada en una sesión de cliente. Si la información es confidencial o privada, conviene que configure el servidor Telnet utilizando SSL. Cuando configura un certificado digital para la aplicación Telnet, el servidor Telnet tiene capacidad para funcionar con clientes SSL y no SSL. Si su política de seguridad exige que siempre cifre las sesiones Telnet, puede inhabilitar todas las sesiones Telnet no SSL. Cuando vea que no necesita utilizar el servidor Telnet con SSL, puede desactivar el puerto SSL. Puede controlar el uso de SSL para las sesiones Telnet utilizando el mandato Cambiar atributos de Telnet (CHGTELNA) con el parámetro Permitir capa de sockets segura (ALWSSL). Para garantizar que ninguna aplicación pueda utilizar los puertos SSL o no SSL según proceda, también puede imponer restricciones con el mandato Añadir restricción de puerto TCP/IP (ADDTCPPORT).

Para obtener más detalles sobre Telnet y algunos consejos relacionados con la seguridad de Telnet con y sin SSL, el tema IBM Systems Software Information Center sobre Telnet proporciona la información que necesita para utilizar Telnet en el sistema operativo i5/OS.

Conceptos relacionados

Escenario de Telnet: proteger Telnet con SSL

Planificar para DCM

Información relacionada

Telnet

Capa de sockets segura (SSL) para proteger System i Access para Windows

Para proteger las sesiones de comunicaciones de System i Access para Windows, puede configurar el System i Access para Windows para que utilice la capa de sockets segura (SSL).

Con SSL se asegura que todo el tráfico de las sesiones de System i Access para Windows estará cifrado. De esta forma se impide que se lean los datos mientras se transmiten entre los hosts local y remoto.

Información relacionada

Administración de capa de sockets segura (SSL)

Seguridad Java

Clases de seguridad

Redes privadas virtuales (VPN) para proteger las comunicaciones privadas

Las redes privadas virtuales (VPN), que son una extensión de la intranet de una compañía a través de la infraestructura existente ya sea de una red pública o de una red privada, pueden ayudarle a comunicarse de manera privada y segura dentro de su organización.

Con el aumento del uso de las VPN y la seguridad que proporcionan, la compañía JKL Toy se está planteando qué opciones podrá emplear para transmitir los datos por Internet. Recientemente, adquirieron otra pequeña compañía de fabricación de juguetes que desean que funcione como filial. JKL necesitará mover información entre las dos compañías. Ambas utilizan el sistema operativo i5/OS y una conexión VPN que pueden garantizar la seguridad que necesitan para comunicarse entre las dos redes. La creación de una VPN es más rentable que utilizar las líneas no conmutadas tradicionales.

Algunos de los usuarios que se pueden beneficiar de la conexión VPN son:

- Usuarios remotos y móviles.
- Usuarios que se comunican entre la oficina central y las sucursales u otras ubicaciones exteriores a la red.
- Usuarios que se comunican de empresa a empresa (B2B).

Se producirán riesgos de seguridad si no se limita el acceso de los usuarios a los sistemas confidenciales. Si no se imponen limitaciones en cuanto a quién puede acceder a un sistema, aumentarán las probabilidades de que no se mantenga la confidencialidad de la información de la compañía. Deberá elaborar un plan que restrinja el acceso al sistema a aquellos usuarios que necesiten compartir la información sobre el sistema. Una conexión VPN permite controlar el tráfico de la red, a la vez que ofrece importantes características de seguridad, como la autenticación y la privacidad de los datos. La creación de múltiples conexiones VPN le permitirá controlar quién puede acceder a cada uno de los sistemas en cada conexión. Por ejemplo, los departamentos de Contabilidad y Recursos Humanos se pueden conectar mediante su propia VPN.

Cuando permite a los usuarios conectarse al sistema por Internet, podría estar enviando datos corporativos confidenciales a través de redes públicas, lo que expondría estos datos a posibles ataques. Una de las opciones para proteger los datos transmitidos es utilizar métodos de cifrado y autenticación

para garantizar la privacidad y la seguridad contra los intrusos. Las conexiones VPN ofrecen una solución a una necesidad de seguridad concreta: proteger las comunicaciones entre sistemas. Las conexiones VPN protegen los datos que fluyen entre los dos extremos de la conexión. Además, podrá emplear la seguridad de reglas de paquetes para definir qué paquetes IP pueden pasar por la VPN.

El uso de VPN le permite crear conexiones seguras para proteger el tráfico que fluye entre extremos controlados y de confianza. No obstante, aún deberá tener cuidado sobre qué grado de acceso proporciona a los socios de la VPN. Las conexiones VPN pueden cifrar los datos mientras viajan a través de las redes públicas. Pero, según cómo la configure, es posible que los datos que fluyen por Internet no puedan transportarse a través de una conexión VPN. En este caso, los datos no estarían cifrados mientras fluyen a través de las redes internas que se comunican mediante la conexión. Por lo tanto, debe planificar detenidamente cómo hay que configurar cada conexión VPN. Asegúrese de que proporciona al socio de la VPN acceso a únicamente aquellos hosts o recursos de la red interna a los que le interesa que acceda.

Por ejemplo, puede darse el caso de un distribuidor que necesita obtener información sobre las piezas que hay en stock. Esta información se encuentra en una base de datos que permite actualizar las páginas Web de la intranet. Supongamos que le interesa autorizar a este distribuidor a acceder a estas páginas directamente por una conexión VPN. Pero, por otro lado, no quiere que el distribuidor pueda acceder a los otros recursos del sistema, como a la propia base de datos. Puede configurar la conexión VPN de forma que el tráfico entre los dos extremos esté restringido al puerto 80. El puerto 80 es el puerto por omisión que utiliza el tráfico de HTTP. Por lo tanto, el distribuidor solo podrá enviar y recibir las peticiones y las respuestas de HTTP a través de esa conexión.

El tipo de tráfico que fluye a través de la conexión VPN se puede restringir, por lo que la conexión proporciona una medida de seguridad a nivel de red. Sin embargo, VPN no funciona de la misma forma que un cortafuegos para regular el tráfico que entra y sale del sistema. Asimismo, una conexión VPN no es el único medio disponible para proteger las comunicaciones entre el sistema operativo i5/OS y los otros sistemas. En función de las necesidades de seguridad que tenga, podría resultar más interesante utilizar SSL.

La idoneidad de la conexión VPN para la seguridad que necesita dependerá de qué es lo que desee proteger. Asimismo, dependerá de las concesiones que esté dispuesto a hacer para garantizar la seguridad. Al igual que con todas las decisiones que se toman sobre seguridad, debe tener en cuenta cómo está soportada su política de seguridad por una conexión VPN.

Conceptos relacionados

“Consideraciones sobre System i y la seguridad en Internet” en la página 2

Los problemas de seguridad relacionados con Internet son muchos. En este tema se proporciona una visión general de las ventajas de la seguridad del i5/OS y de sus ofertas en materia de seguridad.

Redes privadas virtuales (VPN)

Apéndice. Avisos

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

Es posible que en otros países IBM no ofrezca los productos, los servicios o las características que se describen en este documento. Consulte al representante de IBM local acerca de los productos y servicios disponibles actualmente en su zona. Las referencias a productos, programas o servicios IBM no pretenden afirmar ni implican que únicamente puedan utilizarse dichos productos, programas o servicios IBM. En su lugar, puede utilizarse cualquier producto, programa o servicio funcionalmente equivalente que no vulnere ninguno de los derechos de propiedad intelectual de IBM. No obstante, es responsabilidad del usuario evaluar y verificar el funcionamiento de cualquier producto, programa o servicio que no sea de IBM.

IBM puede tener patentes o solicitudes de patente pendientes de aprobación que cubran los temas descritos en este documento. La entrega de este documento no le otorga ninguna licencia sobre dichas patentes. Puede enviar las consultas sobre licencias, por escrito, a la siguiente dirección:

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

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

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokio 106-0032, Japón

El párrafo siguiente no puede aplicarse en el Reino Unido ni en cualquier otro país en el que tales disposiciones sean incompatibles con la legislación local: INTERNATIONAL BUSINESS MACHINES CORPORATION PROPORCIONA ESTA PUBLICACIÓN "TAL CUAL" SIN GARANTÍA DE NINGUNA CLASE, EXPLÍCITA O IMPLÍCITA, INCLUIDAS, PERO SIN LIMITARSE A ELLAS, LAS GARANTÍAS IMPLÍCITAS DE NO VULNERABILIDAD, COMERCIALIZACIÓN O IDONEIDAD PARA UN PROPÓSITO DETERMINADO. Algunas legislaciones no contemplan la declaración de limitación de responsabilidad, ni implícitas ni explícitas, en determinadas transacciones, por lo que cabe la posibilidad de que esta declaración no se aplique en su caso.

Esta información puede contener imprecisiones técnicas o errores tipográficos. Periódicamente se efectúan cambios en la información incluida en este documento; estos cambios se incorporarán en nuevas ediciones de la publicación. IBM puede efectuar mejoras y/o cambios en el producto(s) y/o el programa(s) descritos en esta publicación en cualquier momento y sin previo aviso.

Cualquier referencia hecha en esta información a sitios Web no de IBM se proporciona únicamente para su comodidad y no debe considerarse en modo alguno como promoción de esos sitios Web. Los materiales de estos sitios Web no forman parte de los materiales de IBM para este producto y el uso que se haga de estos sitios Web es de la entera responsabilidad del usuario.

IBM puede utilizar o distribuir la información que proporcione de la manera que crea más oportuna sin incurrir en ningún tipo de obligación hacia usted.

Los licenciatarios de este programa que deseen obtener información acerca de él para: (i) intercambiar la información entre programas creados independientemente y otros programas (incluido este) y (ii) utilizar mutuamente la información que se ha intercambiado, deben ponerse en contacto con:

IBM Corporation
Software Interoperability Coordinator, Department YBWA
3605 Highway 52 N
Rochester, MN 55901
Estados Unidos

Esta información puede estar disponible, sujeta a los términos y condiciones adecuados, incluyendo en algunos casos el pago de una tarifa.

- | El programa bajo licencia descrito en este documento, así como todo el material bajo licencia disponible para él, lo proporciona IBM según los términos del Acuerdo de Cliente de IBM, el Acuerdo Internacional de Programas bajo Licencia de IBM, el Acuerdo de Licencia para Código de Máquina de IBM o cualquier otro acuerdo equivalente entre ambas partes.

Los datos de rendimiento contenidos en esta documentación se han determinado en un entorno controlado. Por tanto, los resultados obtenidos en otros entornos operativos pueden variar significativamente. Algunas de las mediciones pueden haberse efectuado en sistemas a nivel de desarrollo, y no existe garantía alguna de que dichas mediciones sean las mismas en sistemas disponibles a nivel general. Además, algunas mediciones pueden haberse estimado por extrapolación. Los resultados reales pueden variar. Los usuarios de este documento deben verificar los datos aplicables a su entorno específico.

La información concerniente a productos no IBM se ha obtenido de los suministradores de esos productos, de sus anuncios publicados o de otras fuentes de información pública disponibles. IBM no ha probado estos productos y no puede confirmar la exactitud del rendimiento, de la compatibilidad ni de ninguna otra afirmación relacionada con productos no IBM. Las consultas acerca de las posibilidades de productos no IBM deben dirigirse a los suministradores de los mismos.

Esta información está pensada a efectos de planificación. La información aquí contenida está sujeta a cambios antes de que los productos descritos estén disponibles.

Esta información contiene ejemplos de datos e informes utilizados en operaciones comerciales diarias. Para ilustrarlas de la forma más completa posible, los ejemplos incluyen nombres de personas, empresas, marcas y productos. Todos estos nombres son ficticios y cualquier parecido con nombres y direcciones utilizados por una empresa real es mera coincidencia.

LICENCIA DE COPYRIGHT:

Esta información contiene programas de aplicación de muestra en el lenguaje fuente, que ilustran técnicas de programación en varias plataformas operativas. Puede copiar, modificar y distribuir estos programas de ejemplo de cualquier forma sin pagar nada a IBM, bajo el propósito de desarrollo, uso, marketing o distribución de programas de aplicación de acuerdo con la interfaz de programación de la aplicación para la plataforma operativa para la cual se han escrito los programas de ejemplo. Estos ejemplos no se han verificado a fondo bajo todas las condiciones. IBM, por lo tanto, no puede garantizar ni dar por supuesta la fiabilidad, la posibilidad de servicio, ni el funcionamiento de estos programas.

Cada copia o cada parte de los programas de ejemplo o de los trabajos que se deriven de ellos debe incluir un aviso de copyright como se indica a continuación:

© (nombre de empresa) (año). Algunas partes de este código proceden de los programas de ejemplo de IBM Corp. © Copyright IBM Corp. _escriba el año o los años_. Reservados todos los derechos.

Si está viendo esta información en copia software, es posible que las fotografías y las ilustraciones en color no aparezcan.

Información de la interfaz de programación

Esta publicación de System i y la seguridad en Internet documenta las interfaces de programación destinadas a permitir que el cliente escriba programas para obtener los servicios de IBM i5/OS.

Marcas registradas

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

Domino
Distributed Relational Database Architecture (DRDA)
i5/OS
IBM
IBM (logotipo)
Lotus Notes
Notes
System i
WebSphere

- | Adobe, el logotipo de Adobe, PostScript y el logotipo de PostScript son marcas registradas de Adobe
- | Systems Incorporated en Estados Unidos y/o en otros países.

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

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

Los demás nombres de compañías, productos y servicios pueden ser marcas registradas o de servicio de otras empresas.

Términos y condiciones

Los permisos para utilizar estas publicaciones están sujetos a los siguientes términos y condiciones.

Uso personal: puede reproducir estas publicaciones para uso personal (no comercial) siempre y cuando incluya una copia de todos los avisos de derechos de autor. No puede distribuir ni visualizar estas publicaciones ni ninguna de sus partes, como tampoco elaborar trabajos que se deriven de ellas, sin el consentimiento explícito de IBM.

Uso comercial: puede reproducir, distribuir y visualizar estas publicaciones únicamente dentro de su empresa, siempre y cuando incluya una copia de todos los avisos de derechos de autor. No puede elaborar trabajos que se deriven de estas publicaciones, ni tampoco reproducir, distribuir ni visualizar estas publicaciones ni ninguna de sus partes fuera de su empresa, sin el consentimiento explícito de IBM.

Aparte de la autorización que se concede explícitamente en este permiso, no se otorga ningún otro permiso, licencia ni derecho, ya sea explícito o implícito, sobre las publicaciones, la información, los datos, el software o cualquier otra propiedad intelectual contenida en ellas.

IBM se reserva el derecho de retirar los permisos aquí concedidos siempre que, según el parecer del fabricante, se utilicen las publicaciones en detrimento de sus intereses o cuando, también según el parecer del fabricante, no se sigan debidamente las instrucciones anteriores.

No puede bajar, exportar ni reexportar esta información si no lo hace en plena conformidad con la legislación y normativa vigente, incluidas todas las leyes y normas de exportación de Estados Unidos.

IBM NO PROPORCIONA NINGUNA GARANTÍA SOBRE EL CONTENIDO DE ESTAS PUBLICACIONES. LAS PUBLICACIONES SE PROPORCIONAN "TAL CUAL", SIN GARANTÍA DE NINGUNA CLASE, YA SEA EXPLÍCITA O IMPLÍCITA, INCLUIDAS, PERO SIN LIMITARSE A ELLAS, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN, NO VULNERACIÓN E IDONEIDAD PARA UN FIN DETERMINADO.



Impreso en España