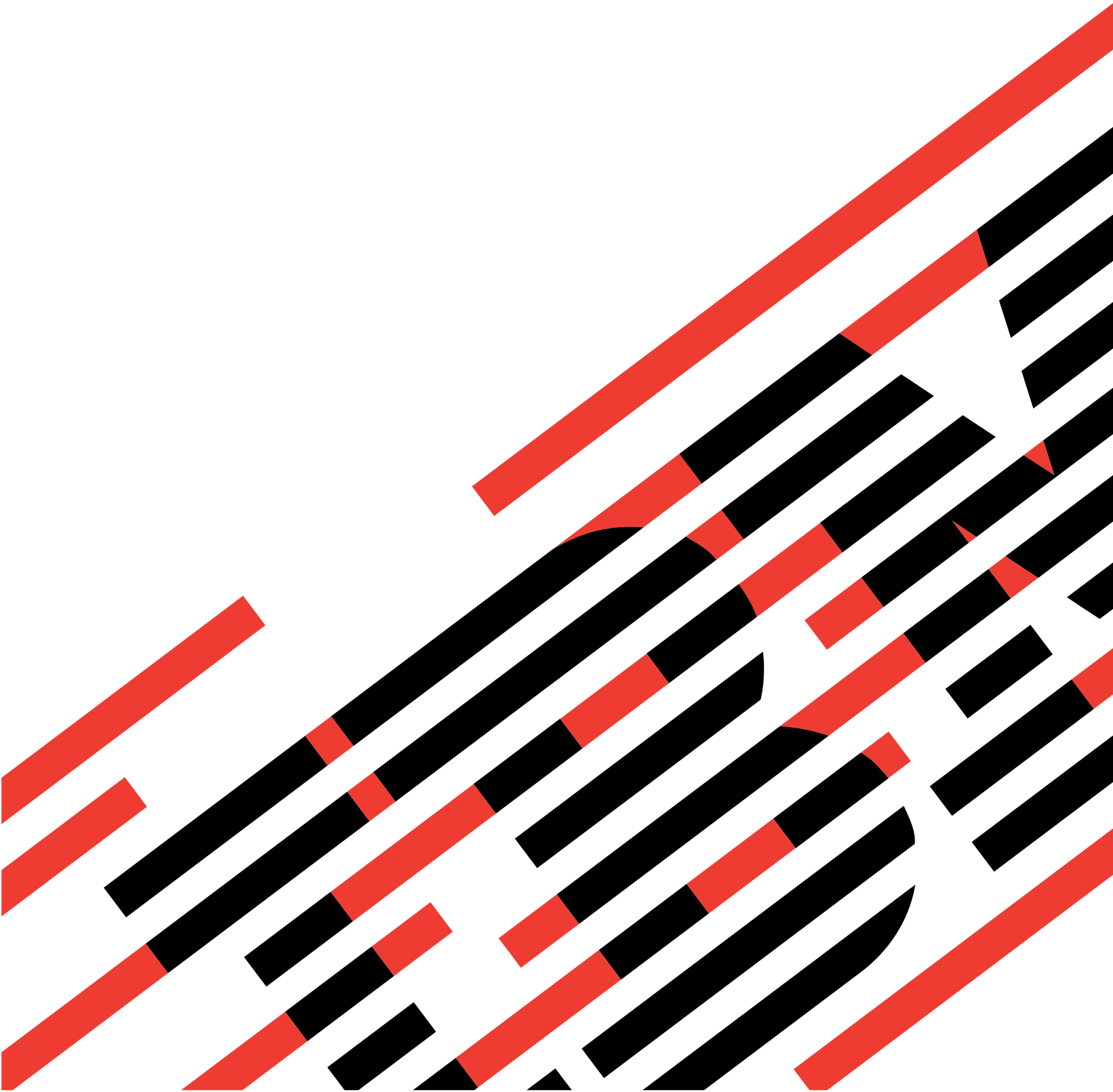
IBM

eserver

iSeries

IBM SecureWay: iSeries 400 e Internet



IBM

@server

iSeries

IBM SecureWay: iSeries 400 e Internet

Contenido

Parte 1. IBM SecureWay: iSeries e Internet

El acceso a Internet desde la LAN es un paso adelante en la evolución de la red para el que deberá volver a evaluar los requisitos de seguridad. Afortunadamente, el sistema iSeries 400 tiene integradas soluciones de software y una arquitectura de seguridad que le permitirá diseñar una buena defensa contra los intrusos y las brechas de seguridad potenciales de Internet. El uso correcto de estas ofertas de seguridad del sistema iSeries permitirá a los clientes, empleados y socios comerciales obtener la información que necesiten para trabajar en un entorno seguro.

Puede utilizar la información contenida en este documento para conocer cuáles son las amenazas de seguridad más conocidas y cómo se relacionan estos riesgos con Internet y sus objetivos de e-business. Asimismo, puede aprender a evaluar estos riesgos y a sopesarlos con las ventajas de utilizar las distintas opciones de seguridad que ofrece el iSeries. Por último, puede determinar cómo desea utilizar esta información para desarrollar un plan de seguridad de la red que se ajuste a las necesidades de su compañía, y asegurar así su política de seguridad.

Si desea obtener más información sobre los riesgos de seguridad de Internet y las soluciones de seguridad del iSeries que podrá utilizar para proteger los sistemas y recursos, consulte la siguiente información:

- **Novedades de la versión V5R1**
  Utilice esta información para conocer los cambios y adiciones que se han realizado en la versión V5R1 de las ofertas de seguridad de Internet para el iSeries.
- **Imprimir este tema**
  Utilice esta información para acceder a una versión de este tema en Adobe Acrobat e imprimirlo.
- **El sistema iSeries y la seguridad en Internet**
  Utilice esta información para obtener una visión general de las ventajas de la seguridad del iSeries para e-business y las ofertas de seguridad del iSeries que están disponibles.
- **Planificar la seguridad para Internet**
  Esta información le enseñará a crear una política de seguridad que responda a sus necesidades de seguridad para e-business y para Internet.
- **Niveles de seguridad del sistema iSeries para la disponibilidad básica de Internet**
  Esta información le permitirá determinar qué medidas de seguridad del sistema debe tener instaladas antes de conectarse a Internet.
- **Opciones de seguridad de la red**
  Utilice esta información para conocer las medidas de seguridad que se deben implantar a nivel de red para proteger los recursos internos.
- **Opciones de seguridad de aplicaciones**
  Con esta información podrá conocer los riesgos de seguridad de Internet más comunes para muchos de los servicios y aplicaciones de Internet, así como las medidas que se pueden tomar para gestionar los riesgos.
- **Opciones de seguridad de la transmisión**
  Aquí hallará información sobre las medidas de seguridad que puede implantar para proteger los datos mientras fluyen a través de una red que no sea de confianza, como Internet. Conozca las medidas de seguridad de las conexiones SSL (capa de sockets segura), Client Access Express y VPN (redes privadas virtuales).

- **opciones de seguridad del iSeries para Internet**
  Esta descripción resumida de las opciones de seguridad del iSeries le servirá de ayuda para elegir las ofertas que le permitirán proteger los sistemas y recursos según el uso que tenga previsto hacer de Internet y los planes que tenga para el e-business.

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

Capítulo 1. Novedades de la versión V5R1

En la versión V5R1, se han añadido varias mejoras y complementos a las ofertas de seguridad del iSeries 400. En la siguiente lista se describen algunas de las mejoras de seguridad y funciones más importantes:

- **Mejoras del gestor de certificados digitales (DCM)**
  Ahora puede utilizar DCM para crear y gestionar certificados que le permitirán firmar los objetos digitalmente y asegurar su integridad, así como proporcionar la prueba del origen de los objetos. También podrá crear y gestionar los correspondientes certificados de verificación de firma que le permitirán a usted o a otras personas autenticar la firma de un objeto firmado para garantizar que los datos del objeto no se han cambiado, como prueba de verificación del origen del objeto. Podrá asimismo utilizar DCM o las correspondientes API, para firmar un objeto o verificar la firma de un objeto.
- **Sistema operativo con firma digital**
  A partir de la versión V5R1, el OS/400 y los LPP de IBM estarán digitalmente firmados por IBM. Los usuarios podrán verificar que los programas de IBM no han sido modificados desde que IBM los firmó. La verificación de la firma digital se puede realizar en el momento de restaurar el sistema o ejecutando el mandato CHKOBJITG. También encontrará varias API que permiten a los clientes y a los business partners firmar digitalmente y verificar sus aplicaciones.
- **Nuevas reglas para las contraseñas de perfil de usuario (QPWDLVL 2 y 3)**
  Ha aumentado la longitud de la contraseña de perfil de usuario, que ahora permite entre 1 y 128 caracteres. Las contraseñas son sensibles a las mayúsculas/minúsculas y permiten blancos intercalados; por ejemplo: "Esta es mi nueva contraseña". Los blancos finales se eliminan, y una contraseña no puede estar formada solo por blancos.
- **Mejoras realizadas en las contraseñas de perfil de usuario**
  Puede emplear el nuevo valor QPWDLVL del sistema para establecer una de las 4 opciones de control del nivel de contraseña del sistema:
  - PWDLVL 0: este valor permite que las contraseñas tengan una longitud de 10 bytes, así como retener las contraseñas de Netserver. Este es el valor por omisión.
  - PWDLVL 1: este valor permite que las contraseñas tengan una longitud de 10 bytes y elimina las contraseñas de Netserver.
  - PWDLVL 2: este valor permite que las contraseñas tengan una longitud de 128 caracteres, así como retener las contraseñas que estén en conformidad con el formatos anterior y el nuevo.
  - PWDLVL 3: este valor permite que las contraseñas tengan una longitud de 128 caracteres y elimina las contraseñas con formatos anteriores.
- **Soporte de coprocesador criptográfico PCI IBM 4758–023 para un almacenamiento de claves más seguro**
  Si el sistema tiene instalado un coprocesador criptográfico PCI IBM 4758–023, podrá utilizarlo para almacenar las claves de certificados digitales de forma más segura. Si utiliza DCM para crear o renovar certificados, puede elegir entre almacenar la clave directamente en el coprocesador o bien utilizar la clave maestra del coprocesador para cifrar la clave privada y almacenarla en un archivo de almacén de claves especial. Asimismo, si utiliza el coprocesador para el almacenamiento de claves, podrá mejorar el rendimiento de SSL (capa de sockets segura) de las aplicaciones habilitadas para SSL. Esto se debe a que el coprocesador se encarga de la tarea de descifrar la clave privada para

presentarla al establecimiento de enlace de SSL. También podrá realizar el equilibrado de la carga del proceso de establecimiento de enlace de SSL entre múltiples tarjetas 4758.

- **Soporte de certificados VPN (redes privadas virtuales)**
  Antes de la versión V5R1, los servidores IKE (intercambio de claves de Internet) de VPN podían autenticarse mutuamente utilizando una clave precompartida. El uso de una clave precompartida es menos seguro, porque hay que comunicar manualmente la clave al administrador situado en el otro extremo de la red VPN. Por ello, hay una posibilidad de que esta clave quede expuesta a otros usuarios durante el proceso de comunicarla. En la versión V5R1, podrá evitar este riesgo utilizando certificados digitales para autenticar los extremos, en lugar de emplear una clave precompartida. Puede usar el gestor de certificados digitales (DCM) para gestionar los certificados que utiliza el servidor IKE para establecer una conexión VPN dinámica.
- **Mejoras realizadas en las aplicaciones habilitadas para SSL (capa de sockets segura)**
  En la V5R1 se han realizado varias mejoras de SSL. Ahora puede configurar el servidor FTP (protocolo de transferencia de archivos) del iSeries para que utilice SSL con el fin de obtener sesiones de comunicaciones seguras. También puede configurar el servidor FTP con objeto de que utilice certificados digitales para la autenticación de los clientes. Además, en la versión V5R1, el OS/400 proporciona soporte para el cifrado AES de 128 bits. AES es un nuevo algoritmo de cifrado más rápido que sustituye al algoritmo DES.
- **Mejoras realizadas en el protocolo simple de transferencia de correo (SMTP)**
  Ahora, SMTP proporciona soporte de lista negra basado en Asunto, Remitente y Dirección IP.
- **Asistente de configuración de Internet**
  El reconocido asistente de configuración de Internet, que en el último release estaba disponible como archivo descargable, ahora está disponible directamente dentro de Operations Navigator. Este asistente le permite configurar una conexión Internet para el sistema iSeries y protegerla con reglas de filtrado generadas automáticamente.
- **Mejoras realizadas en la retención de datos para la creación de programas**
  Los programas creados para los sistemas iSeries de la versión V5R1 o posterior contienen información que permite volver a crear los programas en el momento de restaurarlos, si fuera necesario. La información que se necesita para volver a crear el programa permanece junto con el programa, incluso cuando se ha eliminado la observabilidad del programa. Si se detecta un error de validación del programa en el momento de restaurarlo, el programa se volverá a crear para corregir el error de validación del programa. La acción de volver a crear el programa en el momento de restaurarlo no es nueva para el iSeries de la versión V5R1. En los releases anteriores, los errores de validación del programa que aparecían en tiempo de restauración daban como resultado que se volviera a crear el programa, si era posible (si existía la observabilidad en el programa que se estaba restaurando). La diferencia con los programas del iSeries de la versión V5R1 o posterior es que la información que se necesita para volver a crear el programa permanece, incluso si se ha eliminado la observabilidad del programa. Así, cualquier programa de la versión V5R1 o posterior en el que se detecte una anomalía de validación se volverá a crear durante la restauración, y se eliminará la alteración que produjo la anomalía de validación.

Capítulo 2. Imprimir este tema

Puede ver o bajar una versión PDF de este documento para consultarlo o imprimirlo. Para ver los archivos PDF debe tener instalado el producto Adobe Acrobat Reader. Puede bajar una copia del producto de la página de presentación de Adobe. 

Para ver o bajar la versión PDF, seleccione IBM SecureWay: iSeries e Internet (416 KB o 60 páginas).

Para guardar un PDF en la estación de trabajo con objeto de verlo o imprimirlo:
1. Abra el PDF en el navegador (pulse el enlace anterior).
2. En el menú del navegador, pulse **Archivo**.
3. Pulse **Guardar como...**
4. Navegue hasta el directorio en el que desee guardar el PDF.
5. Pulse **Guardar**.

Capítulo 3. iSeries 400 y la seguridad en Internet

Como propietario del iSeries 400 a quien le interesan las distintas opciones de conexión de los sistemas a Internet, una de las primeras preguntas que se planteará es ″¿Cómo puedo empezar a utilizar Internet en mis negocios?″. La segunda pregunta será ″¿Qué debo saber sobre la seguridad e Internet?″. El objetivo de este manual es ayudarle a responder a la segunda pregunta.

La respuesta a la pregunta ″¿Qué debo saber sobre la seguridad e Internet?″ es que depende de cómo desee utilizar Internet. Los problemas de seguridad relacionados con Internet son muchos. Los problemas relevantes para usted dependerán del uso que desee hacer de Internet. El primer uso que se hace de Internet suele ser 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, debería 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. Consulte la página Escenario: planes de la compañía JKL Toy para el e-business cuando vaya a elaborar su propio plan de utilización de Internet. (Nota: si no está familiarizado con la terminología de seguridad y de Internet, consulte la terminología de seguridad común mientras trabaja con esta documentación).

Una vez determinado el uso que desee 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 se elijan en el desarrollo de 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 sistema iSeries 400

Además de las distintas ofertas de seguridad específicas para proteger el sistema en Internet, el iSeries 400 incluye características de seguridad del sistema muy potentes, como son:

- 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 un sistema iSeries, un archivo no puede hacerse pasar por un programa, ni un programa puede cambiar otro programa. Las características de seguridad del iSeries 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 asesor de seguridad, de Technical Studio,  para determinar qué recomendaciones de seguridad se ajustan a sus necesidades.

Ofertas de seguridad avanzada del iSeries

El sistema iSeries también ofrece varias ofertas de seguridad específicas que le permitirán mejorar la seguridad del sistema cuando se conecte a Internet. Dependiendo del uso que haga de Internet, podrá 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 OS/400, disponible en la interfaz Operations Navigator.
- Reglas de paquetes, que es una característica integrada del OS/400, disponible en la interfaz Operations Navigator. Esta característica permite configurar filtros de paquetes IP y reglas NAT (conversión de direcciones de red) para controlar el flujo del tráfico TCP/IP dentro y fuera del sistema iSeries.
- Seguridad de comunicaciones de las aplicaciones SSL (capa de sockets segura), que permite 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 navegadores web, pero se pueden habilitar otras aplicaciones para que utilicen SSL. Ahora son numerosas las aplicaciones del servidor iSeries que están habilitadas para SSL, incluidas IBM HTTP Server para iSeries, Client Access Express, FTP (protocolo de transferencia de archivos), Telnet, entre otras muchas.

Una vez determinado el uso que desea hacer de Internet, así como las cuestiones de seguridad y las ofertas, funciones y herramientas de seguridad disponibles, ya estará preparado para desarrollar una política y unos objetivos de seguridad. Son varios los factores que afectarán a las opciones que elija al desarrollar la política de seguridad. Cuando amplíe su organización para llevarla Internet, la política de seguridad será la piedra angular para garantizar la seguridad de su sistema.

Nota: Si desea obtener información más detallada sobre cómo empezar a utilizar Internet en sus negocios, consulte en Information Center estos temas y libros rojos de IBM en línea:

- *Conexión a Internet*
- *AS/400 Internet Security: Protecting Your AS/400 from HARM on the Internet* (SG24-4929). 

Capítulo 4. Planificar la seguridad en Internet

Cuando elabore planes para el uso que se va a hacer de Internet, deberá planificar detenidamente 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 los resultados obtenidos, podrá evaluar con precisión sus necesidades de seguridad.

Por ejemplo, debe documentar y describir aspectos como los siguientes:
- La configuración de la red actual.
- Información de configuración del servidor de correo electrónico y DNS.
- La conexión con el proveedor de servicios de Internet (ISP).
- Qué servicios de Internet desea utilizar.
- Qué servicios desea proporcionar 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 cuáles las medidas necesarias para minimizarlos.

Por ejemplo, supongamos que le interesa que los usuarios internos utilicen Telnet para conectarse a los sistemas principales de una ubicación de investigación especial. Los usuarios internos necesitan este servicio para mejorar el desarrollo de nuevos productos de la compañía. Sin embargo, está preocupado por el flujo a través de Internet de datos confidenciales sin protección. Si la competencia captura estos datos y se aprovecha de ellos, 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 adicionales de seguridad debe implementar para garantizar la confidencialidad de los datos en este uso (habilitación de la capa de sockets segura (SSL)).

Para obtener ayuda en la elaboración de planes relacionados con el uso de Internet y la seguridad, consulte los siguientes temas:
- **La seguridad basada en la defensa por capas**, que proporciona información sobre los problemas asociados a la elaboración de un plan de seguridad global.
- **Política y objetivos de seguridad**, que proporciona información para ayudarle a entender mejor los problemas que implica la elaboración de un plan de seguridad global.
- **Escenario: planes de la compañía JKL Toy para el e-business**, que proporciona un modelo práctico del uso de Internet y de los planes de seguridad de una compañía típica, que podrá utilizar a la hora de crear su propio modelo.

Aunque el producto ha dejado de suministrarse, aún puede serle de utilidad adaptar y emplear las hojas de trabajo de planificación de IBM Firewall para AS/400 para documentar sus planes. Estas hojas de trabajo pueden ayudarle a reunir información detallada importante sobre el uso que tenga previsto hacer de Internet y la configuración de la red interna, así como para evaluar las necesidades de seguridad. Puede acceder a estas hojas de trabajo en el tema Iniciación al cortafuegos de V4R5 iSeries Information Center. . Independientemente de si decide utilizar o no un cortafuegos, gran parte de la información que necesita para planificar la estrategia de seguridad en Internet es la misma.

La 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. 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 iSeries 400, si se configuran correctamente, permiten minimizar muchos riesgos. No obstante, cuando se conecta el sistema iSeries a Internet, se deben 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 una gran variedad de 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 sencillamente el tráfico de la red para intentar conocer algunos secretos. Estos ataques se pueden basar en la red (rastreando 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 intentará adivinar o robar las contraseñas o bien utilizará 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 proporcionar medidas que ofrezcan protección en las siguientes capas del modelo informático de red tradicional. En general, la seguridad debe planificarse desde el nivel más básico (seguridad del sistema) al nivel más complejo (seguridad de transacciones).

Seguridad a nivel del 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 completa de seguridad de Internet debe ser configurar debidamente los valores básicos de seguridad del sistema iSeries.

Seguridad a nivel de red
Las medidas de seguridad de la red controlan el acceso al sistema iSeries y a otros sistemas de la red. Cuando conecta la red a Internet, debe asegurarse de que tiene implantadas las debidas medidas de seguridad 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 y debe 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 de la conexión del direccionador del ISP y las precauciones del servicio 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 tome precauciones 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 decida utilizar deberán cubrir 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 servidores que están fuera de su control. A menos que implante medidas de seguridad como las de configurar las aplicaciones para que utilicen SSL (capa de sockets segura), 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.

Política y objetivos de seguridad

La política de seguridad

Cada servicio de Internet que utilice o preste supone riesgos para el sistema iSeries 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 cubren 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 está intentando burlar sus defensas.

Para desarrollar una política de seguridad, debe definir claramente sus objetivos de seguridad. Una vez creada la 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. Puede encontrar un ejemplo de política de seguridad para la compañía JKL Toy en el tema ″Seguridad básica del sistema y planificación″, en iSeries Information Center.

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 varias 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 iSeries. 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 pueden 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, podrá 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:
  - Proteger los datos para que no se puedan "husmear" ni interpretar, los 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 de los sistemas iSeries, la integridad del sistema es el componente de seguridad más vigilado, porque es una parte fundamental de la arquitectura del iSeries. Por ejemplo, la arquitectura del iSeries

dificulta enormemente a los intrusos la imitación o el cambio de un programa del sistema operativo cuando se utiliza el nivel de seguridad 40 ó 50.

No repudio
El No repudio es la prueba de que se ha producido una transacción o de que se ha enviado o recibido un mensaje. La utilización de los certificados digitales y de la criptografía de claves públicas para ″firmar″ transacciones, mensajes y documentos da soporte al No repudio. El remitente y el destinatario están de acuerdo en que el intercambio ha tenido 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) 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.

El conocimiento de los objetivos de seguridad le ayudará a crear una política de seguridad que dé respuesta a todas sus necesidades de seguridad de Internet y de la red. El tema Escenario: planes de la compañía JKL Toy para el e-business le será de utilidad para aprender a definir sus objetivos y a crear la política de seguridad. El plan de seguridad y el uso de Internet que hace la compañía del escenario es representativo de la mayoría de las implementaciones del mundo real.

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

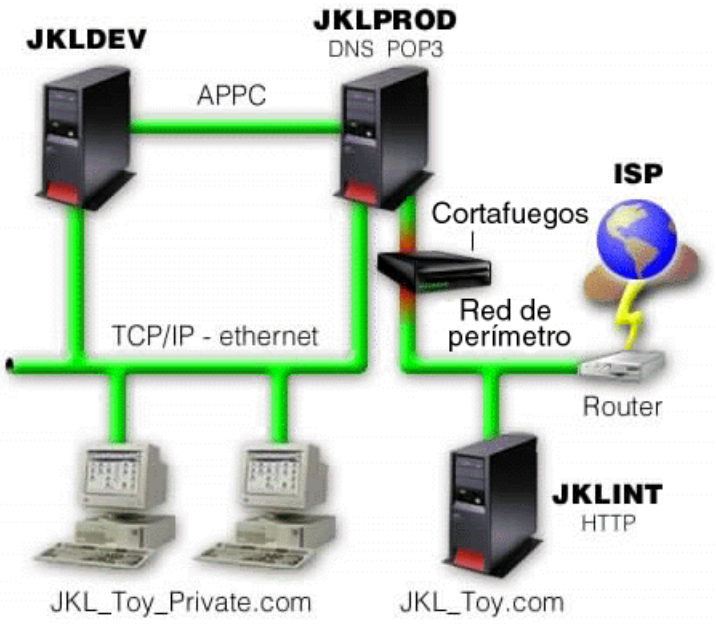
Este escenario describe una empresa típica, la compañía JKL Toy, que ha decidido ampliar sus objetivos comerciales mediante el uso de Internet. Aunque la compañía es ficticia, sus planes de utilizar Internet para el e-business y las necesidades de seguridad resultantes son representativos de muchas de las compañías del mundo real.

La compañía JKL Toy es un empresa fabricante de juguetes, pequeña pero en rápida expansión, con productos como cuerdas de saltar, cometas o peluches de leopardo. El presidente de la compañía está contento con el crecimiento de la empresa y con las posibilidades que el nuevo sistema iSeries le ofrece para aliviar la carga de dicho crecimiento. Sharon Jones, directora de contabilidad, es la responsable de la administración y la seguridad del sistema iSeries.

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 coporativa 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 será la responsable de actualizar la política de seguridad de la compañía y 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 de los sistemas iSeries, 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. La figura siguiente ilustra la configuración de red/Internet de la compañía.



Como se muestra en el diagrama, la compañía JKL Toy tiene dos sistemas iSeries primarios. Uno de ellos se utiliza para el desarrollo (JKLDEV) y el otro para las 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. Por ello, ha optado por añadir un nuevo sistema iSeries (JKLINT) para ejecutar 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. Al designar este nuevo sistema iSeries como servidor solo de Internet, la compañía también disminuye la complejidad de la gestión de la seguridad de la red.

La compañía no ejecutará aplicaciones críticas del negocio en el nuevo sistema iSeries. Durante esta etapa de elaboración de planes para el e-business, el nuevo sistema solo proporcionará 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 ataques posibles. 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 (por ejemplo, un sitio web de comercio electrónico o el acceso a una extranet) se implantarán medidas de seguridad más avanzadas.

Capítulo 5. Niveles de seguridad para la disponibilidad básica de Internet

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 total de Internet debe ser configurar debidamente los valores de la seguridad básica del OS/400. Debe realizar las siguientes acciones para garantizar que la seguridad del sistema cumple los requisitos mínimos:

- 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 lo recomendable para proteger el sistema en entornos de alto riesgo como Internet.

  Nota: Si tiene un sistema orientado básicamente a las transacciones o una aplicación que realiza un uso intensivo del sistema de archivos integrado, el nivel de seguridad 50 puede disminuir el rendimiento del sistema o de la aplicación.

  Si desea obtener más información sobre cada nivel de seguridad del iSeries, consulte Consejos y herramientas para proteger el sistema iSeries.

  Nota: Si está ejecutando un nivel de seguridad menor que 50, es posible que tenga que actualizar los procedimientos de funcionamiento o las aplicaciones. Consulte la información del manual Referencia de seguridad de iSeries , antes de pasar a un nivel de seguridad más alto.
- 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 Operations Navigator o el asesor de seguridad de Technical Studio para comparar sus valores con los 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 omisión a todos los usuarios el uso (PUBLIC *EXCLUDE) 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 objeto en el sistema. Puede encontrar más información acerca de cómo trabajar con las autorizaciones sobre objetos en el capítulo de iSeries Navigator de Consejos y herramientas para proteger el sistema iSeries .

Como ayuda para configurar estos requisitos mínimos de seguridad del sistema, puede utilizar el **asesor de seguridad** (disponible en el sitio web Technical Studio) o el **asistente de seguridad** (disponible en la interfaz iSeries Navigator). El asesor de seguridad de Technical Studio proporciona un conjunto de

recomendaciones de seguridad a partir de sus respuestas a una serie de preguntas. Luego podrá utilizar las recomendaciones para configurar los valores de seguridad del sistema que necesite. El asistente de seguridad también proporciona recomendaciones a partir de sus respuestas a una serie de preguntas. A diferencia de lo que sucede con el asesor de seguridad, podrá hacer que el asistente utilice las recomendaciones para configurar automáticamente los valores de seguridad del sistema.

Las características de seguridad inherentes del iSeries, cuando estén debidamente configuradas y gestionadas, le proporcionarán capacidad para minimizar numerosos riesgos. No obstante, cuando conecte el sistema iSeries a Internet, tendrá que proporcionar medidas de seguridad adicionales para garantizar la seguridad de la red interna. Tras haberse asegurado de que el iSeries 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.

Capítulo 6. Opciones de seguridad de la 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 implementar 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.

Asimismo, el proveedor de servicios de Internet (ISP) puede y debe proporcionar una parte importante del plan de seguridad de la red. El sistema de seguridad de la red debe precisar las medidas de seguridad que proporcionará el proveedor de servicios de Internet (ISP), como pueden ser las reglas de filtrado para la conexión del direccionador del ISP o las precauciones 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**. Dado que los riesgos potenciales de Internet se pueden producir en una gran variedad de niveles, deberá poner a punto medidas de seguridad que ofrezcan múltiples capas de defensa contra los riesgos.

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 el 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.

Conviene que se plantee seriamente la posibilidad de utilizar un producto cortafuegos como línea principal de defensa siempre que conecte el sistema iSeries o la red interna a Internet. Aunque ya no se puede adquirir el producto IBM Firewall para AS/400 y tampoco está disponible el soporte para este producto, existen en el mercado numerosos cortafuegos que podrá utilizar.

Si desea obtener más información sobre cómo hacer la transición desde un producto IBM Firewall para AS/400 existente a otros productos o a las características de seguridad de red nativas del iSeries, consulte el libro rojo All You Need to Know When Migrating from IBM Firewall for AS/400 (SG24-6152).

Como los productos cortafuegos del mercado proporcionan una amplia gama de tecnologías de seguridad de red, la compañía JKL Toy ha decidido utilizar uno en el escenario de seguridad del e-business para proteger su red. No obstante, su cortafuegos no ofrece ninguna protección para el nuevo servidor Internet de iSeries. Por lo tanto, la compañía ha optado por implementar la característica de reglas de paquetes del iSeries para crear reglas de filtrado y de NAT con objeto de controlar el tráfico del servidor Internet.

Acerca de las reglas de paquetes del iSeries

Las reglas de filtrado de paquetes permiten proteger los sistemas informáticos rechazando o aceptando los paquetes IP según los criterios que se definan. Las reglas de NAT permiten ocultar la información interna del sistema a los usuarios

externos, sustituyendo una dirección IP por otra dirección IP pública. 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 iSeries.

Consulte el tema Elegir las opciones de seguridad de la red de iSeries si necesita ayuda para decidir qué enfoque es más adecuado para sus necesidades de seguridad.

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. El cortafuegos:
- Permite a los usuarios de la red interna utilizar los recursos situados fuera de la red.
- Impide 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 considerablemente 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 cortafuegos

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 pueden 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
  - Dividir servicios de nombres de dominio (DNS)
  - 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 servidor 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, el cortafuegos permite 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 (vea la figura de más abajo). 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 obtener acceso a los sistemas internos.

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

Aunque el cortafuegos 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 el 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 del iSeries

Las reglas de paquetes del iSeries es una característica integrada del OS/400 que está disponible en la interfaz Operations Navigator. La característica de reglas de paquetes le permite configurar dos tecnologías de seguridad de red centrales para que controlen el flujo del tráfico TCP/IP para proteger el sistema iSeries:
- Conversión de direcciones de red (NAT)
- Filtrado de paquetes IP

La NAT y el filtrado IP están integrados en el sistema OS/400, por lo que suponen una forma económica de asegurar 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, dependiendo de las necesidades de seguridad y de los objetivos.

Nota: No conviene que se centre solamente en el ahorro de costes si está planificando la seguridad de un sistema de producción iSeries. En tales situaciones, la seguridad del sistema debe prevalecer sobre el coste. Para asegurar la protección máxima del sistema de producción, debe plantearse la posibilidad de usar un cortafuegos.

¿Qué son la NAT y el filtrado de paquetes IP y cómo funcionan conjuntamente?

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 iSeries 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.

El 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 Operations 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:
- 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 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. Una vez grabada la información en un diario del sistema, no se puede modificar la entrada del archivo de anotaciones. Por lo tanto, el archivo de anotaciones es una herramienta ideal para auditar la actividad de la red.

Elegir opciones de seguridad de red para el iSeries

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 iSeries 400, puede optar por 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 OS/400. Esta

implementación está formada por la característica de reglas de paquetes (que incluye el filtrado IP y la NAT) y la característica de servidor proxy HTTP para iSeries.

La elección de la característica de reglas de paquetes o de un cortafuegos dependerá del entorno de red, de los requisitos de acceso y de las necesidades de seguridad. Conviene que se plantee **seriamente** la posibilidad de utilizar un cortafuegos como línea principal de defensa siempre que conecte el sistema iSeries 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 OS/400 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.

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 sortea con éxito el cortafuegos y consigue acceder a él, el atacante no podrá hacer gran cosa. Mientras que si un atacante consigue sortear las funciones de seguridad de TCP/IP del iSeries, 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 hacer estragos en el sistema o para obtener acceso a otros sistemas de la red interna.

Así que, ¿existe algún caso en el que sea aceptable usar las características de seguridad de TCP/IP del iSeries? 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 de 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 usar la tecnología TCP/IP del OS/400**	**Es mejor usar un cortafuegos totalmente funcional**
Filtrado de paquetes IP	• Para proporcionar protección **adicional** a un solo sistema iSeries, 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 iSeries funciona como pasarela (direccionador 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 una extranet en la que el sistema iSeries funciona como pasarela.	• 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 usar la tecnología TCP/IP del OS/400	Es mejor usar un cortafuegos totalmente funcional
Conversión de direcciones de red (NAT)	• 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.	• 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	• Para funcionar a modo de proxy en las **ubicaciones remotas** de una red corporativa cuando el cortafuegos central proporciona acceso a Internet.	• Para funcionar a modo de proxy en toda una red corporativa cuando se accede a **Internet**.

Si desea obtener más información sobre cómo utilizar las características de seguridad de TCP/IP del OS/400, consulte las siguientes fuentes de información:

- Reglas de paquetes (filtrado y NAT).
- Documentation Center de HTTP Server.
- AS/400 Internet Security Scenarios: A Practical Approach (SG24-5954).

Capítulo 7. Opciones de seguridad 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 tome precauciones 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 cubrir 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.

Si desea obtener más información sobre cómo proteger algunas de las aplicaciones más comunes de Internet, revise las páginas siguientes:

Seguridad del servicio web

Cuando proporciona acceso a los visitantes de su sitio web, no le interesará exponer a la vista de todos la información sobre cómo está configurado el sitio ni el código que se utiliza para generar la página. Lo que desea es que la visita a su página sea rápida, fácil y sin fisuras, y que todo el trabajo se realice internamente. Como administrador, le conviene asegurarse de que las medidas de seguridad no afecten negativamente al sitio web. Si utiliza el iSeries 400 como servidor web, tenga en cuenta los siguientes puntos:

- El administrador del servidor debe definir las directivas del servidor antes de que un cliente pueda interaccionar con el servidor HTTP. Existen dos métodos para crear comprobaciones de seguridad: directivas generales del servidor y directivas de protección del servidor. Las peticiones dirigidas al servidor web deben cumplir todas y cada una de las restricciones impuestas por estas directivas antes de que el servidor acepte dichas peticiones.
- Puede crear y editar estas directivas utilizando las páginas web Admin del servidor para configurarlo. Las directivas del servidor le permiten controlar el comportamiento global del servidor web. Las directivas de protección del servidor permiten especificar y controlar los modelos de seguridad utilizados por el servidor para los URL específicos que maneja el servidor.
- Para configurar el servidor, puede utilizar las directivas MAP o PASS y las páginas web Admin del servidor.
  - Utilice las directivas MAP o PASS para enmascarar los nombres de archivo del servidor web del iSeries. En concreto, hay directivas de servidor PASS y directivas de servidor MAP que controlan los directorios cuyos URL sirve el servidor web. Asimismo, puede encontrar una directiva de servidor EXEC que controla las bibliotecas en las que residen los programas CGI-BIN.

Definirá directivas de protección para cada URL del servidor. No todos los URL requieren una directiva de protección. Pero si desea controlar cómo se accede o quién accede a un recurso del URL, necesitará una directiva de protección para dicho URL.

– Además, puede utilizar las páginas web Admin del servidor para configurar el servidor, en lugar de utilizar el mandato WRKHTTPCFG (Trabajar con configuración de HTTP) y escribir las directivas. La tarea de trabajar con las directivas de protección mediante la interfaz de línea de mandatos puede ser muy complicada. Por lo tanto, le recomendamos que emplee las páginas web Admin para asegurarse de que configura correctamente las directivas.

HTTP proporciona capacidad para visualizar datos, pero no para alterar los datos que hay en un archivo de base de datos. Sin embargo, algunas de las aplicaciones que escriba necesitarán actualizar un archivo de base de datos. Para ello, puede utilizar los programas CGI-BIN. Por ejemplo, supongamos que desea crear formularios que, una vez cumplimentados por el usuario, actualicen una base de datos del iSeries. Como administrador de seguridad, tendría que supervisar las autorizaciones de ese perfil de usuario y las funciones que realicen los programas CGI. Asimismo, se aseguraría de evaluar qué objetos confidenciales podrían tener una autorización de uso público inadecuada.

Nota: CGI (interfaz de pasarela común) es un estándar del sector para el intercambio de información entre un servidor web y los programas informáticos externos. Los programas pueden estar escritos en cualquier lenguaje de programación que esté soportado en el sistema operativo en el que se está ejecutando el servidor web.

Además de emplear programas CGI en las páginas web, podría entersarle utilizar Java. Antes de añadir Java a las páginas web, conviene que sepa cómo funciona la Seguridad Java.

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

El servidor proxy recibe las peticiones HTTP de los navegadores web y las reenvía a los servidores web. Los servidores web que reciben estas peticiones solo se enteran de la dirección IP del servidor proxy. No pueden determinar los nombres ni las direcciones de los PC que originaron las peticiones. El servidor proxy puede manejar las peticiones de URL para HTTP, FTP (protocolo de transferencia de archivos), Gopher y WAIS.

También podrá utilizar el soporte de proxy HTTP de IBM HTTP Server para iSeries  con objeto de consolidar el acceso web. El servidor proxy también puede anotar todas las peticiones de URL con el fin de hacer un seguimiento. Así, usted podrá revisar los archivos de anotaciones para supervisar el uso y el mal uso de los recursos de la red.

Hallará más información sobre este tema en el manual *Consejos y herramientas para proteger el sistema iSeries*. 

Seguridad Java en Internet

La programación Java se está extendiendo cada vez más en los entornos informáticos actuales. Por ejemplo, es posible que esté utilizando los productos IBM Toolbox para Java o IBM Development Kit para Javaen su sistema para desarrollar nuevas aplicaciones. Por lo tanto, debe estar preparado para manejar los problemas de seguridad relacionados con 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 que protege a los programadores contra la utilización de objetos de forma no intencionada. 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 deben aplicarse las mismas reglas de seguridad que las que se aplican con otros lenguajes en el iSeries 400.

Applets Java

Los applets Java son pequeños programas Java que se pueden incluir en las páginas HTML. Como los applets se ejecutan en el cliente, su acción queda restringida al cliente. Sin embargo, un applet Java tiene potencial para acceder al iSeries 400. (Un programa ODBC o un programa APPC (comunicaciones avanzadas programa a programa) que funcione en un PC de la red también puede acceder al iSeries). En general, los applets Java solo pueden establecer una sesión con el servidor en el que se originaron. Por lo tanto, el applet Java únicamente puede acceder al iSeries desde un PC conectado si el applet se ha originado en el iSeries (por ejemplo, en el servidor web).

Un applet puede intentar conectarse a un puerto TCP/IP del servidor. No hace falta que se comunique con un servidor de software escrito en Java. No obstante, para los servidores que se hayan escrito con IBM Toolbox para Java, el applet debe proporcionar un ID de usuario y una contraseña cuando vuelve a establecer conexión con el servidor. En este manual, los servidores que se describen son todos servidores iSeries. (No es necesario que un servidor escrito en Java utilice IBM Toolbox para Java). Normalmente, la clase IBM Toolbox para Java solicita al usuario un ID de usuario y una contraseña en la primera conexión.

El applet únicamente puede ejecutar funciones en el sistema iSeries si el perfil de usuario tiene autorización sobre esas 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. Cuando el sistema procesa las peticiones procedentes de los applets, no utiliza el valor de capacidad limitada del perfil del usuario.

El visor de applets permite comprobar un applet en el sistema servidor; no obstante, no está sujeto a las restricciones de seguridad del navegador. Por lo tanto, solo debe utilizar el visor de applets para comprobar sus propios applets, nunca para ejecutar los applets que proceden de fuentes externas. Los applets Java se 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 objeto de establecer su autenticidad. El applet firmado puede escribirse en las unidades locales del PC, aunque el valor por omisión del navegador no lo permita. El applet firmado también se puede escribir en unidades correlacionadas del iSeries, ya que estas aparecen en el PC como si fuesen unidades locales.

Nota: El comportamiento descrito anteriormente se cumple en general en Netscape Navigator y MS Internet Explorer. Lo que suceda en realidad dependerá de la configuración y la administración de los navegadores que se utilicen.

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

A partir de la versión V4R4, puede utilizar IBM Toolbox para Java para configurar un entorno SSL (capa de sockets segura). 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 usar 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 funcionalidad de un servidor web sin cambiar el código del servidor web. El servidor IBM WebSphere Application Server que se suministra con IBM HTTP Server para iSeries proporciona soporte para utilizar servlets en los sistemas iSeries.

Debe utilizar la seguridad de recursos en los objetos servlet que utiliza el servidor. 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 de HTTP Server. Por ejemplo, no permita que los servlets se ejecuten únicamente bajo el perfil del servidor web. Aparte de esto, deberá controlar quién puede ejecutar el servlet (palabras clave enmascaradas en la directiva de protección) utilizando grupos de servidores HTTP y listas de control de acceso (ACL). Asimismo, debe utilizar las funciones de seguridad que ofrecen las herramientas de desarrollo de servlets, como las de WebSphere Application Server para iSeries.

Consulte estos recursos para obtener más información sobre las medidas de seguridad generales para Java:
- La seguridad Java de IBM Developer Kit para Java.
- Clases de seguridad de IBM Toolbox para Java.
- Consejos y herramientas para proteger el sistema iSeries  .

Autenticación y autorización Java de los recursos

IBM Toolbox para Java contiene clases de seguridad que facilitan la verificación de la identidad del usuario y asignan opcionalmente esa identidad a la hebra de sistema operativo correspondiente a una aplicación o servlet que se esté ejecutando en un sistema iSeries. Las comprobaciones ulteriores de la seguridad de recursos se producirán bajo la identidad asignada. Si desea obtener más información sobre estas clases de seguridad, consulte los Servicios de autenticación de IBM Toolbox para Java.

IBM Developer Kit para Java proporciona soporte para JAAS (servicio de autenticación y autorización Java), que es una ampliación 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). Si desea obtener más información sobre el uso de J2SDK, consulte JAAS (servicio de autenticación y autorización Java).

Proteger las aplicaciones Java con SSL

Puede utilizar la capa de sockets segura (SSL) para proteger las comunicaciones de las aplicaciones del iSeries 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 habilitarlo para las otras aplicaciones.

Si desea obtener más información sobre la administración de SSL (capa de sockets segura) para las aplicaciones Java, consulte los siguientes temas de Information Center:
- Entorno SSL (capa de sockets segura) de IBM Toolbox para Java.
- IBM Developer Toolkit para Java para garantizar la seguridad de una aplicación Java con SSL.

Seguridad del correo electrónico

La utilización del correo electrónico en Internet o en otras redes que no sean de confianza supone riesgos de seguridad contra los que el uso de un cortafuegos tal vez no pueda proteger. 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 muy importante ser prudente a la hora de enviar información confidencial por correo electrónico. El correo electrónico viaja a través de numerosos servidores 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 para intentar inundarlo. Sin la seguridad adecuada, el servidor de

destino puede experimentar una denegación de servicio porque el disco de almacenamiento del servidor queda lleno de mensajes inútiles. O bien, el servidor deja 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 servidores 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 del 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 clase 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 obtener más información sobre la seguridad de Domino en los sistemas iSeries, consulte las siguientes referencias:

- Biblioteca de referencia de Lotus Domino. 
- Sitio web de asistencia al usuario de Lotus Notes. 
- Lotus Notes and Domino R5.0 Security Infrastructure Revealed  (SG24-5341).

- Lotus Domino for AS/400 Internet Mail and More  (SG24-5990).

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 opción posible es configurar una conexión de red privada virtual (VPN). A partir de la versión V4R4, puede utilizar el sistema iSeries para configurar diversas conexiones VPN, incluso entre clientes remotos y el sistema iSeries. 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.

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. También puede utilizar la función de mandatos remotos para enviar mandatos al servidor. Por lo tanto, el protocolo de transferencia de archivos es muy útil para trabajar con los sistemas remotos o para mover archivos entre sistemas. Sin embargo, el uso del protocolo de transferencia de archivos por Internet o por otras redes que no sean de confianza le expone a algunos riesgos de seguridad. Debe conocer estos riesgos para garantizar que su política de seguridad tiene previsto cómo minimizarlos.

- 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). Como los usuarios de FTP no están restringidos a los menús, podrían 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 iSeries 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 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 proporcionan los programas de menús. Es probable que muchos usuarios deseen restringir aún más los controles de acceso a FTP. Esta opción solo se aplica a FTP, no a otras interfaces como ODBC, DDM o 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.

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.

A partir de la versión V5R1, 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.

Si desea obtener más información sobre el uso del protocolo de transferencia de archivos (FTP), sus riesgos y las medidas de seguridad disponibles, consulte estas fuentes de información:
- Implementar la seguridad de FTP.
- FTP anónimo.
- Seguridad de FTP.
- Consejos y herramientas para proteger el sistema iSeries .

Capítulo 8. Opciones de seguridad de la transmisión

Recuerde que el escenario de la compañía JKL Toy tiene dos sistemas iSeries 400 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 iSeries 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 el nuevo sistema iSeries 400 como servidor solo de Internet, la compañía también disminuye la complejidad de la gestión de 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 implementar soluciones de seguridad más potentes. Para combatir estos riesgos, deberá implantar medidas de seguridad que protejan la transmisión de los datos mientras viajan por Internet.

Los riesgos asociados al movimiento de la información entre sistemas que no sean de confianza se pueden minimizar con dos ofertas de seguridad específicas a nivel de transmisión para los sistemas iSeries: las comunicaciones seguras con la capa de sockets segura (SSL) y las conexiones de redes privadas virtuales (VPN).

Proteger las aplicaciones con SSL

El protocolo SSL (capa de sockets segura) constituye de hecho un estándar del sector para proteger la comunicación 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 iSeries, algunas de las aplicaciones son:

- IBM HTTP Server para iSeries (original y powered by Apache)
- Servidor FTP
- Servidor Telnet
- Arquitectura de bases de datos relacionales distribuidas (DRDA) y servidor de gestión de datos distribuidos (DDM)
- Management Central
- Servidor de servicios de directorios (LDAP)
- Aplicaciones Client Access Express, incluido Operations Navigator y las aplicaciones escritas para el conjunto de interfaces de programación de aplicaciones (API) de Client Access Express
- 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 permiten habilitar SSL en las aplicaciones. En el tema Las API de SSL (capa de sockets segura) 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) del iSeries

Puede utilizar las conexiones VPN del sistema iSeries para establecer un canal de comunicaciones seguro entre dos extremos. 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?

Estos dos métodos de seguridad 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. Los factores que conviene tener en cuenta son: 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 todavía hay algunas aplicaciones que no pueden aprovechar las ventajas de SSL, muchas otras, como Telnet y Client Access Express, tienen capacidad SSL incorporada. Por otro lado, 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. Podría crear una conexión VPN de pasarela a pasarela para la parte de la red que le interese. De esta manera portegería el tráfico, pero la conexión sería transparente para los servidores y clientes individuales situados a cada lado de la conexión.

Utilización de 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. Los sistemas iSeries 400 permiten crear y gestionar fácilmente certificados digitales para los sistemas y usuarios con el Gestor de certificados digitales (DCM), una característica integrada del OS/400.

Además, puede configurar algunas aplicaciones, como IBM HTTP Server para iSeries, para que utilicen certificados digitales como método más potente de autenticación de clientes, 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. Una tercera parte de confianza, denominada **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 muy poca información, como las que tal solo exigen un nombre distinguido. Nombre distinguido es el nombre de la persona o del servidor 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. El propietario de un certificado puede utilizar estas claves para ″firmar″ y cifrar datos como, por ejemplo, mensajes y documentos, que se envían entre los usuarios y los servidores. Las firmas digitales aseguran la fiabilidad del origen de un elemento y protege su integridad.

Aunque todavía hay algunas aplicaciones que no pueden aprovechar las ventajas de SSL, muchas otras, como Telnet y Client Access Express, tienen capacidad SSL incorporada. Si desea obtener más información sobre el uso de SSL con las aplicaciones del iSeries, consulte el tema **Proteger las aplicaciones con SSL** en iSeries Information Center.

SSL para garantizar un acceso seguro a Telnet

A partir de la versión V4R4, puede configurar el servidor Telnet para que utilice la capa de sockets segura (SSL) con el fin de asegurar las sesiones de comunicaciones de 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. Una vez establecida 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 del iSeries con 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. Podrá inhabilitar los puertos utilizando el mandato ADDTCPPORT. Una vez desactivado el puerto, el servidor proporciona sesiones Telnet no SSL a los clientes, y las sesiones Telnet SSL quedan inhabilitadas.

Si desea obtener más información sobre Telnet y algunos consejos relacionados con la seguridad para Telnet con y sin SSL, consulte estas fuentes de información:

- El tema Telnet, en Information Center, proporciona la información necesaria para utilizar Telnet en el sistema iSeries.
- Seguridad de Telnet, que proporciona información sobre el uso conjunto de SSL y Telnet para proteger las sesiones de comunicaciones Telnet.
- Consejos y herramientas para proteger el sistema iSeries  proporciona información detallada sobre la seguridad de Telnet en la sección TCP/IP.

SSL para Client Access Express seguro

A partir de la versión V4R4, puede configurar los servidores de Client Access Express para que utilicen la capa de sockets segura (SSL) con el fin de proteger las sesiones de comunicaciones de Client Access Express. Por ejemplo, la compañía JKL Toy, a medida que ha ido creciendo, ha añadido al personal varios agentes comerciales como viajantes. Los agentes comerciales necesitan acceder desde su oficina a la información del sistema de producción del iSeries para conocer, por ejemplo, el estado la disponibilidad de los juguetes y las fechas de fabricación. Como estos datos son confidenciales, la compañía JKL Toy solo permite a los agentes comerciales acceder a esta información a través de Client Access Express seguro.

La utilización de SSL garantiza el cifrado de todo el tráfico de las sesiones de Client Access Express. De esta forma se impide que se lean los datos mientras se transmiten entre los sistemas principales local y remoto.

Si desea obtener más información sobre el uso de Client Access Express con SSL, consulte las siguientes fuentes de información:

- Administración de la capa de sockets segura (SSL)
- Seguridad de Client Access Express y Operations Navigator
- SSL de IBM Developer Kit para Java
- SSL de IBM Toolbox para Java

Redes privadas virtuales (VPN) para proteger las comunicaciones privadas

Con el aumento del uso de redes privadas virtuales (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 sistemas iSeries, y el uso de una conexión VPN podría garantizar la seguridad que necesitan para comunicarse entre las dos redes. La creación de una VPN es más rentable que utilizar las tradicionales líneas alquiladas.

Las conexiones VPN le permiten controlar y proteger las conexiones con las sucursales, con los empleados móviles, con los suministradores y con los socios comerciales, entre otros.

Algunos de los usuarios que se podrían 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 del 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, puede estar enviando datos corporativos confidenciales a través de redes públicas, lo que expone 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, una conexión VPN tal vez no pueda cifrar los datos 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 sistemas principales 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. Afortunadamente, 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 la 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 iSeries 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.

Capítulo 9. Terminología de seguridad de Internet

Para establecer las bases para tratar la seguridad en Internet, empezaremos por definir algunos términos básicos de Internet. Si ya está familiarizado y conoce lo suficiente Internet, puede saltarse esta sección.

Autenticación
Autenticación es la verificación de que un cliente o un servidor remoto es realmente el que dice ser. La autenticación garantiza que se puede confiar en el similar remoto al que se está conectando.

Cracker
Pirata informático que actúa con malas intenciones.

Criptografía
Ciencia que garantiza la seguridad de los datos. La criptografía permite almacenar información o comunicarse con otras partes sin que haya terceros no involucrados que puedan entender la información almacenada o la comunicación. El cifrado transforma el texto inteligible en un conjunto de datos ininteligibles (texto cifrado). El descifrado restaura el texto inteligible a partir de los datos ininteligibles. Ambos procesos implican un algoritmo o una fórmula matemática y una secuencia secreta de datos (la clave).

Hay dos tipos de criptografía:
- En la criptografía de clave compartida/secreta **(simétrica)**, una clave es un secreto compartido entre las dos partes de la comunicación. El cifrado y el descifrado utilizan la misma clave.
- En la criptografía de clave pública **(asimétrica)**, el cifrado y el descifrado utilizan claves diferentes. Una de las parte tiene dos claves: una clave pública y otra privada. Las dos claves están relacionadas matemáticamente, pero es virtualmente imposible deducir la clave privada a partir de la clave pública. Un mensaje cifrado con la clave pública de un usuario solo se puede descifrar con la clave privada asociada. Por otro lado, un servidor o un usuario pueden utilizar una clave privada para ″firmar″ un documento y utilizar una clave pública para descifrar una firma digital. De esta forma se verifica el origen del documento.

Certificado digital
Certificado digital es un documento digital que valida la identidad del propietario del certificado, de manera muy parecida a como lo hace un pasaporte. Una parte de confianza, denominada autoridad certificadora (CA), emite certificados digitales para los usuarios y los servidores. La confianza en la CA es la base de la confianza en el certificado como credencial válida. Puede utilizar los certificados como:
- Identificación: quién es el usuario.
- Autenticación: garantiza que el usuario es quien dice ser.
- Integridad: determina si el contenido de un documento ha sido alterado, verificando la ″firma″ digital del remitente.
- No repudio: garantiza que un usuario no puede declarar que no ha realizado una acción. Por ejemplo, que el usuario no pueda negar que ha autorizado una compra electrónica con una tarjeta de crédito.

Firma digital
Una firma digital en un documento electrónico es equivalente a una firma personal en un documento escrito. La firma digital es una prueba del origen del documento. El propietario del certificado ″firma″ un documento utilizando la clave privada asociada al certificado. El destinatario del documento utiliza la correspondiente clave pública para descifrar la firma, que verifica al remitente como el origen.

Gestor de certificados digitales (DCM)
El gestor de certificados digitales (DCM) permite a OS/400 ser una autoridad certificadora (CA) local. El DCM le permitirá crear certificados digitales para que los utilicen los servidores o los usuarios. Puede importar certificados digitales emitidos por otras CA. También puede asociar un certificado digital a un perfil de usuario de OS/400. Asimismo, puede utilizar DCM para configurar las aplicaciones para que utilicen la capa de sockets segura (SSL) y garantizar así la seguridad de las comunicaciones.

Nombre distinguido
Nombre distinguido es el nombre de la persona o del servidor para el que la autoridad certificadora (CA) emite un certificado digital. El certificado proporciona este nombre para indicar la propiedad del certificada. En función de la política de la CA que emite el certificado, el nombre distinguido puede incluir información de autorización adicional.

Servidor de nombres de dominio (DNS)
Sistema principal de Internet que convierte los nombres de Internet en direcciones IP, a menudo interaccionando con otros servidores DNS de Internet. Por ejemplo, muchos servidores DNS podrían reconocer

```
vnet.ibm.com
```

pero quizá solo unos pocos conocen la dirección IP completa de:

```
system1.vnet.ibm.com
```

Cuando se conecta a Internet, el cliente de Internet utiliza un servidor de nombres de dominio para determinar la dirección IP del sistema principal con el que desea comunicarse.

Cifrado
El cifrado transforma los datos dándoles un formato que resulta ilegible para las personas que no tengan el método de descifrado correcto. Aún así, las partes no autorizadas pueden interceptar la información. Sin embargo, sin el método de descifrado correcto, la información será incomprensible.

Extranet
Red comercial privada de varias organizaciones cooperativas situadas fuera del cortafuegos corporativo. El servicio de una extranet utiliza la infraestructura de Internet existente, incluidos los servidores estándar, los clientes de correo electrónico y los navegadores web. De esta forma, la extranet resulta más económica que crear y mantener una red propia. Permite a los socios comerciales, proveedores y clientes con intereses comunes utilizar Internet en sentido amplio para fomentar estrechas relaciones comerciales y un vínculo de comunicaciones más fuerte.

Cortafuegos
Barrera lógica entre la red interna y una red externa, como puede ser Internet. El cortafuegos está formado por uno o más sistemas de hardware y software. Controla el acceso y el flujo de la información entre sistemas seguros o de confianza y sistemas no seguros o que no son de confianza.

Pirata informático (hacker)
Persona no autorizada que intenta forzar la entrada al sistema.

Enlaces de hipertexto
Forma de presentar la información en línea con conexiones (llamadas enlaces de hipertexto) entre un fragmento de información (llamado nodo de hipertexto) y otro.

Lenguaje de códigos de hipertexto (HTML)
Lenguaje que se utiliza para definir documentos de hipertexto. El HTML le pemitirá indicar cuál ha de ser el aspecto del documento (resaltado y estilo) y cómo se debe enlazar con otros documentos u objetos.

Protocolo de transporte de hipertexto (HTTP)
Método estándar para acceder a los documentos de hipertexto.

Internet
La ""red de redes"" mundial que conecta a todas las redes entre sí. También es una suite de aplicaciones cooperativas que permite comunicarse entre sí a los sistemas conectados a la ″red de redes″. Internet proporciona información navegable, transferencia de archivos, conexión remota, correo electrónico, noticias y otros servicios. A Internet se la conoce a menudo como “la Red”.

Cliente de Internet
Programa (o usuario) que utiliza Internet para realizar peticiones y recibir resultados de un programa servidor de Internet. Hay distintos programas de cliente que permiten solicitar distintos tipos de servicios de Internet. Uno de los tipos de programas de cliente son los navegadores web. Otro es el protocolo de transferencia de archivos (FTP).

Sistema principal de Internet
Sistema que está conectado a Internet o a una intranet. Un sistema principal de Internet puede ejecutar más de un programa servidor de Internet. Por ejemplo, el sistema principal de Internet podría ejecutar un servidor FTP para responder a las peticiones de las aplicaciones de clientes de FTP. Ese mismo sistema principal puede ejecutar un servidor HTTP para responder a las peticiones de clientes que utilizan navegadores web. Los programas servidores se ejecutan normalmente como programas de fondo (por lotes) en el sistema principal.

Intercambio de claves de Internet (IKE)
El protocolo IKE, cuando se utiliza con IPSec, da soporte a la negociación automática de las asociaciones de seguridad, así como a la generación y la renovación automáticas de claves criptográficas. En general, se utiliza IKE como parte de una red privada virtual.

Nombre de Internet
Alias de una dirección IP. Una dirección IP tiene un formato numérico largo y es difícil de recordar; por ejemplo, 10.5.100.75. Puede asignar esta dirección IP a un nombre de Internet como, por ejemplo,

```
system1.vnet.ibm.com
```

Un nombre de Internet también se llama nombre de dominio totalmente calificado. Si observa un anuncio que dice “Visite nuestra página inicial”, la ″dirección de la página inicial″ incluye el nombre de Internet, no la dirección IP, porque el nombre de Internet es más fácil de recordar.

Un nombre de dominio totalmente calificado está formado por varias partes. Por ejemplo,

system1.vnet.ibm.com

tiene las siguientes partes:

com: Todas las redes comerciales. Esta parte del nombre de dominio viene asignada por la autoridad de *Internet* (una organización externa). Se asignan distintos caracteres para los distintos tipos de red (por ejemplo, com para las instituciones comerciales y edu para las instituciones docentes).

ibm: Identificador de la organización. Esta parte del nombre de dominio también viene asignada por la autoridad de Internet y es exclusiva. Solo hay una organización en todo el mundo que pueda tener el identificador

ibm.com

vnet: Agrupación de sistemas dentro de

ibm.com

Este identificador se asigna de forma interna. El administrador de ibm.com puede crear una o más agrupaciones.

system1:
Nombre de un sistema principal de Internet dentro del grupo vnet.ibm.com.

Servidor de Internet
Programa (o conjunto de programas) que acepta las peticiones que los correspondientes programas de cliente realizan por Internet y luego les responde también por Internet. Un servidor de Internet es como un sitio web al que un cliente de Internet puede acceder o visitar. Cada programa servidor da soporte a servicios diferentes, como pueden ser los siguientes:

- Navegación (una "página inicial" y enlaces a otros documentos y objetos).
- Transferencia de archivos. El cliente puede solicitar, por ejemplo, la transferencia de archivos del servidor al cliente. Los archivos podrían ser actualizaciones de software, listas de productos o documentos.
- Comercio electrónico, como la capacidad de solicitar información o cursar pedidos de productos.

Proveedor de servicios de Internet (ISP)
Organización que proporciona conexión a Internet de forma parecida a como su compañía telefónica local le proporciona conexión a la red telefónica mundial.

Intranet
Red interna de la organización, que utiliza herramientas de Internet, como puede ser un navegador web o FTP.

Dirección IP
Una dirección IP (protocolo de Internet) es la forma en que se reconoce a los usuarios de una red TCP/IP (Internet es una red TCP/IP de tamaño muy grande). Un servidor de Internet normalmente tiene asignada una dirección IP exclusiva. Un cliente de Internet podría utilizar una dirección IP temporal, aunque exclusiva, asignada por el ISP.

Datagrama IP
Unidad de información que se envía a través de una red TCP/IP. Un

datagrama IP (al que también se llama paquete) contiene datos e información de cabecera, como puede ser la dirección IP del origen y del destino.

Filtros IP
El filtrado de IP proporciona el mecanismo de protección básico del cortafuegos. Permite determinar qué tráfico pasa a través de él, tomando como base los detalles de la sesión IP. De esta forma, la red segura queda protegida contra los intrusos que utilizan técnicas poco sofisticadas (por ejemplo, la exploración de servidores seguros) o incluso técnicas más sofisticadas (por ejemplo, la usurpación de direcciones IP). La característica de filtrado debe considerarse como la base sobre la que se construyen las demás herramientas. Proporciona la infraestructura para el funcionamiento de las demás herramientas y deniega el acceso a todos los intrusos, aunque no puede con los crackers más ambiciosos.

IPSec Conjunto de protocolos que dan soporte al intercambio seguro de paquetes en la capa IP. IPSec es un conjunto de estándares que el iSeries y muchos otros sistemas emplean para llevar a cabo redes privadas virtuales (VPN).

Usurpación IP
Intento de acceder al sistema simulando ser un sistema (dirección IP) de confianza. El intruso configura un sistema con una dirección IP de confianza. Los fabricantes de direccionadores han diseñado protecciones en los sistemas para detectar y rechazar los intentos de usurpación.

Conversión de direcciones de red (NAT)
Proporciona una alternativa más transparente a los servidores proxy y SOCKS. También simplifica la configuración de la red, ya que permite conectar redes con estructuras de sistemas de direcciones incompatibles. La NAT proporciona dos funciones principales. Puede proteger un servidor web público que desee hacer funcionar desde dentro de la red interna. Para ofrecer esta protección, la NAT permite ocultar la dirección ″verdadera″ del servidor detrás de una dirección que está a disposición del público. Asimismo, proporciona un mecanismo para que los usuarios internos puedan acceder a Internet manteniendo ocultas las direcciones IP internas privadas. La NAT ofrece también protección cuando se permite a los usuarios internos acceder a los servicios de Internet, porque existe la posibilidad de ocultar sus direcciones privadas.

No repudio
No repudio es la 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 da soporte al No repudio.

Paquete
Datagrama que incluye información sobre el protocolo de línea, como puede ser Ethernet, Token-Ring o Frame-Relay.

Proxy El servidor proxy es una aplicación TCP/IP que reenvía las peticiones y respuestas entre los clientes de la red interna segura y los servidores de la red no de confianza. El servidor proxy desglosa la conexión TCP/IP para ocultar la información de la red interna (como las direcciones IP internas). Los sistemas principales situados fuera de la red detectarán el servidor proxy como el origen de la comunicación.

Infraestructura de claves públicas (PKI)
Sistema de certificados digitales, de autoridades certificadoras (CA) y de

otras autoridades de registro que verifican y autentican la validez de cada una de las partes implicadas en una transacción de Internet.

Capa de sockets segura (SSL)
Creado por Netscape, el protocolo SSL es en la práctica el estándar del sector para el cifrado de sesiones entre clientes y servidores. SSL utiliza el cifrado de claves simétricas para cifrar la sesión entre un servidor y un cliente (usuario). El cliente y el servidor negocian esta clave de sesión durante un intercambio de certificados digitales. Se crea una clave diferente para cada sesión SSL de servidor y cliente. Por lo tanto, aunque hubiera usuarios no autorizados que interceptaran y descifraran una clave de sesión (lo que es poco probable), no podrían utilizarla para entrometerse en las sesiones SSL actuales, pasadas o futuras.

Husmear
Práctica de supervisar o entrometerse en las transmisiones electrónicas. La información que se envía por Internet puede pasar a través de varios direccionadores antes de alcanzar su destino. Los fabricantes de direccionadores, los ISP y los desarrolladores de sistemas operativos han trabajado muy duro para que no se pueda husmear en la red central de Internet. Cada vez son menos frecuentes los intentos satisfactorios de la acción de husmear. La mayoría de las veces solo ocurre en las LAN privadas conectadas a Internet, no en la propia red central de Internet. Sin embargo, no se debe descartar esta posibilidad, ya que la mayoría de las transmisiones de TCP/IP no están cifradas.

SOCKS
SOCKS es una arquitectura de cliente/servidor que transporta tráfico TCP/IP a través de una pasarela segura. Un servidor SOCKS ejecuta casi los mismos servicios que un servidor proxy.

Usurpación
Atacantes camuflados como sistemas de confianza que intentan persuadirle para que les envíe información secreta.

TCP/IP
Es el principal protocolo de comunicaciones que se utiliza en Internet. TCP/IP son las siglas de Transmission Control Protocol/Internet Protocol, que es el protocolo de control de transmisión/protocolo Internet. También se puede utilizar TCP/IP en la red interna.

Caballo de Troya
Caballo de Troya es un programa informático que tiene en aparencia una una función útil e inocente. No obstante, contiene funciones ocultas que utilizan las autorizaciones aprobadas asignadas al usuario cuando este inicia el programa. Por ejemplo, podría copiar información de autorización interna del sistema y enviarla al originador del caballo de Troya.

Red privada virtual (VPN)
Ampliación de la intranet privada de una empresa. Puede utilizarse a través de una red pública como Internet, creando una conexión segura privada, fundamentalmente a través de un "túnel" privado. Las VPN transportan información de forma segura por Internet conectando otros usuarios al sistema. Entre estos se encuentran:
- Usuarios remotos
- Oficinas filiales
- Socios comerciales y suministradores

Navegador web
La aplicación de cliente HTTP. Un navegador web interpreta el lenguaje

HTML para mostrar documentos de hipertexto del usuario. Para acceder a un objeto con hiperenlace, el usuario puede seleccionar un área del documento actual. Esta área se llama a menudo una **zona activa**. Internet Connection Web Explorer y Netscape Navigator son ejemplos de navegadores web.

World Wide Web (WWW)
Malla de servidores y clientes interconectados que utilizan el mismo formato estándar para crear documentos (HTML) y acceder a documentos (HTTP). La malla de enlaces, de servidor a servidor y de documento a documento, se llama metafóricamente **la Web**.

Impreso en España