

## Arquitectura de Intranet/Extranet para Sistemas Corporativos Basados en Web

### Tabla de Contenidos

4. Arquitectura de Intranet/Extranet para Sistemas Corporativos Basados en Web.....	2
4.1 Internet.....	2
4.2 Internet vs Intranet.....	3
4.3 Intranet.....	4
4.4 ¿Porqué usar Intranet?.....	6
Características y Beneficios:.....	6
Nuevo Paradigma de la Información:.....	6
Publicación en Base a la Demanda:.....	7
Reducción de Costes:.....	7
Desarrollo de Aplicaciones Cliente/Servidor:.....	8
4.5 Extranet.....	9
4.6 Seguridad de las Intranets / Extranet.....	9
Enrutadores para filtrar.....	10
Firewalls.....	11
Servidores sustitutos.....	12
Anfitriones bastión.....	13



## 4. Arquitectura de Intranet/Extranet para Sistemas Corporativos Basados en Web

### 4.1 Internet

Internet es una red global en la cual, cada ordenador actúa como un cliente y un servidor. Internet consta de varios componentes conectados:

- **Backbones:** líneas de comunicación de alta velocidad y ancho de banda que unen hosts o redes.
- **Redes:** grupos de hardware y software de comunicación dedicados a la administración de la comunicación a otras redes. Todas las redes tienen conexiones de alta velocidad para dos o más redes.
- **Proveedores del Servicio de Internet (ISPs):** son computadoras que tienen acceso a la Internet. Varios proveedores de servicios en línea como Compuserve, MPSNet y Spin, actúan como ISPs proporcionando acceso a Internet a todos sus suscriptores.
- **Hosts:** ordenadores cliente/servidor. En ellos es donde los usuarios ven la interacción con la Internet. Cada computadora que se conecta directamente a una red es un host. Todos los hosts tienen una dirección de red única. Esta es comúnmente conocida como la dirección IP.

La manera en que Internet permite a los ordenadores conectarse es similar a como trabaja una red de área local (LAN). En una red simple, se tienen dos computadoras y una conexión de datos. Las computadoras se comunican enviando un paquete a través de la conexión. Un paquete es una unidad de datos que viaja entre hosts de una red específica. Un paquete consiste de dos secciones (Esto se verá con más exactitud en el siguiente módulo del curso):

- **Encabezado:** contiene la localización de la dirección física y otros datos de red.
- **Datos:** contiene un datagrama.



Los dos protocolos de Internet que trabajan en conjunto para la transmisión de datos son:

- Transmission Control Protocol (TCP)
- Internet Protocol (IP)

En conjunto estos protocolos son conocidos como TCP/IP.

Los ordenadores también pueden comunicarse con otros ordenadores fuera de la LAN. Al conjunto de LANs se les conoce como redes de área amplia (WAN). Los ruteadores y gateways proveen las conexiones entre diferentes LANs. Si las LANs son del mismo tipo, se usa un ruteador. Si las LANs utilizan diferentes protocolos de comunicación, o topologías, los gateways son usados para convertir los paquetes en el formato requerido. Cuando un gateway recibe un paquete, el gateway utiliza la información de la dirección y el encabezado del datagrama para determinar la localización del destinatario de los datos. El gateway reempaqueta el datagrama en el formato, del paquete adecuado, hacia la siguiente conexión. Los datos pueden cruzar varias LANs antes de llegar a su destino.

Internet es considerada una red de área amplia, independiente a la topología. Esta independencia de las diversas topologías de LAN la realiza el protocolo estándar IP. El encabezado del paquete IP contiene una dirección de cuatro octetos que identifican a cada una de los equipos. Cuando un paquete es enviado hacia un host, el ordenador determina si el paquete es local o remoto (dentro o fuera de la LAN). Si el paquete es local, el mismo lo transmite; si es remoto lo envía hacia un gateway el cual determina la dirección final. La información de la dirección también determina cómo será ruteado el paquete a través de Internet. Normalmente el gateway utiliza la localización del destinatario para determinar la mejor ruta para enviar el paquete. Si alguna red intermedia llegara a estar demasiado ocupada o no disponible, el gateway dinámicamente selecciona una ruta alterna. Una vez que el paquete es enviado, cada red que reciba el paquete, repite el proceso redirigiendolo cuando sea necesario. Este proceso de repite hasta que el paquete llega a su destino. Diferentes paquetes pueden tomar diferentes rutas, aún cuando contengan información del mismo archivo o mensaje. Los datos del paquete son reensamblados en el destinatario.



## 4.2 Internet Vs Intranet

El uso más común de las tecnologías de Internet, por los negocios y organizaciones, es interno a sus redes de área local o de área amplia. Una LAN o WAN que utilice las tecnologías de Internet es llamada una Intranet. Las Intranets brindan a los usuarios la capacidad de compartir dinámicamente recursos internos de la misma forma que los usuarios de Internet lo hacen. Las diferencias de Intranet sobre Internet son:

- Privacidad: La información es solo interna, solo visible por los miembros de una compañía, mientras que Internet no es limitada para ningún tipo de colectivo.
- Control y Administración: Mientras que Internet en si misma no se puede ni controlar ni administrar, por lo menos de una forma global, en la Intranet si que se administran y controlan no solo los contenidos de la Intranet sino también más factores como puede ser los grupos de usuarios admitidos, etc.
- Mejor rendimiento: El acceso a la información en Intranet es aún más rápida si cabe que en Internet y además la información requerida está centralizada y siempre se encuentra actualizada, cosa que en Internet no se da en la mayoría de los casos.
- Ámbito de alcance: Intranet es una red dentro de una organización mientras que Internet es la “red de redes” y es a nivel mundial.

## 4.3 Intranet

Como hemos hablado antes Intranet es una red de ordenadores conectados por medio del protocolo de comunicación TCP/IP, es decir aplica la tecnología de Internet a la tecnología de redes Lan, lo cual permite dentro de una empresa u organización, que se enlacen a todos los miembros de una organización proporcionándoles un acceso fácil a la información y convirtiendo el uso de los recursos y aplicaciones en un proceso más amigable, funcional y productivo.



Para usar una Intranet, las computadoras cliente normalmente necesitan de los siguientes requisitos mínimos:

- TCP/IP instalado, el cual se puede encontrar por defecto tanto en sistemas operativos Windows como en cualquier distribución de Linux.
- Un navegador de Web instalado como el Internet Explorer o Netscape Navigator en sistemas operativos Windows o como Konqueror y Mozilla en las distribuciones Linux.
- Un servidor de Web como el Internet Information Server (IIS) en los sistemas operativos Windows o como Apache en distribuciones Linux.
- Herramientas de desarrollo de páginas Web para la Intranet, donde existen multitud de herramientas para esta función tanto para Windows como Linux, aunque la más usada es la de Microsoft Frontpage.

Una Intranet es una infraestructura de comunicación. La Intranet esta basada en los estándares de comunicación de Internet y el en los del World Wide Web. Por lo tanto, las herramientas usadas para crear una Intranet son idénticas a las mismas de Internet y las aplicaciones Web. La diferencia principal de la Intranet es que al acceso a la información publicada esta restringido y solo será visible a clientes dentro del grupo de la Intranet.

Otras herramientas que no básicas en una Intranet pero que la pueden complementar son:

- Herramientas de indexación:

Para la indexación de páginas Web. Cuando un documento en el servidor de páginas Web es modificado, el sistema de archivos notifica al servidor de indexación del cambio. Dicho servidor puede no indexar el documento instantáneamente. La indexación ocurre en background cuando hay suficientes recursos disponibles en la computadora sin afectar el rendimiento del sistema. Cuando el Index Server dice que puede indexar los cambios, abre el documento e inicia el proceso de indexación. El proceso de indexación consiste de tres pasos principales:

1. Filtrado: Los filtros de acuerdo al formato del archivo extraen las cadenas de texto, reconocen los cambios de idioma y manejan los objetos incrustados.
2. Word Breaking: Según el idioma dividen las cadenas de caracteres en palabras válidas de acuerdo a la estructura y sintaxis del idioma.
3. Normalización. La normalización depura las palabras emitidas por el word breaker, involucra detalles como el uso de mayúsculas y minúsculas, la puntuación y elimina las palabras "ruidosas" (preposiciones, conjunciones, artículos, etc.).

- **Servidor de Correo Electrónico:** basado en los estándares de Internet. Provee administración de buzones de usuarios, es escalable, tiene capacidades de ruteo y funciones de autenticación. También aprovecha puertos y threads, para soportar múltiples conexiones simultáneas. Debe ser compatible con productos basados en SMTP y POP3. Por ejemplo el MCIS Mail server de Windows.
- **Servidores de Noticias.**
- **Bases de datos:** Para la gestión y administración de los contenidos a compartir para el trabajo en grupo dentro de la compañía, como pueden ser por ejemplo el caso de Oracle y Sql para Windows y MySQL en Linux.
- **Herramientas de seguridad:** Porque al abrir una compuerta al mundo exterior (Extranet) puede resultar peligroso y hay que implementar toda una política de seguridad, que implementa funciones como las del cortafuegos (firewall), encriptación y autenticación, antivirus, monitorización de la Intranet, etc.
- **Lenguajes de desarrollo:** A todo esto solo cabe añadir que Java se ha posicionado como la mejor plataforma de desarrollo de Intranets sobre todo para Windows, mientras que en sistemas operativos cabe destacar el lenguaje Perl.



#### 4.4 ¿Porqué Usar Intranet?

Una Intranet básica puede ser instalada en horas o días y puede servir como un "depósito de información" para la compañía completa.

##### **Características y Beneficios:**

La Intranet tiene las siguientes características:

- Rápido Diseño.
- Escalabilidad.
- Fácil navegación.
- Accesible para la mayoría de las plataformas de cómputo.
- Integra la estrategia de cómputo distribuido.
- Adaptable a los sistemas de información propietarios.
- Uso de multimedia.

Los beneficios para la empresa son:

- Requiere poca inversión para su inicio
- Ahorra tiempo y costos en comparación de la distribución de información tradicional (papel).
- Su estrategia de cómputo distribuido utiliza los recursos de cómputo mas efectivamente.
- Tiene una interfaz sencilla y flexible (vínculos).
- Independiente de la plataforma.



### **Nuevo Paradigma de la Información:**

La Intranet propone el concepto de usar el Explorador de Internet como la interfaz de información universal. Las ventajas de este nuevo paradigma son:

- Reduce el tiempo de aprendizaje de los usuarios.
- Simplifica la instalación de aplicaciones.
- Presenta diferentes tipos de información: texto, gráficas, sonido y vídeo.
- Actúa como "front-end" para las aplicaciones cliente-servidor.
- Permite el acceso a bases de datos.

### **Publicación en Base a la Demanda:**

Una de las principales motivaciones para la adopción de la Intranet es que permite a las organizaciones evolucionar de una estrategia de publicación calendarizada a publicación en base a la demanda.

Tradicionalmente, las compañías publican una vez al año el manual del empleado. cualquier cambio de último momento o ajuste importante, sería actualizado hasta el siguiente año. La Intranet ofrece dos soluciones a este problema:

1. El empleado decide cuando consultar la información.
2. La información puede actualizarse instantáneamente.

### **Reducción de Costes:**

El modelo de publicación tradicional incluye varios pasos:

1. Creación del documento.
2. Migración del a una publicación electrónica.
3. Producción del original.
4. Revisión.
5. Producción del original corregido.





6. Duplicación.

7. Distribución.

El modelo de publicación con la Intranet incluye:

1. Creación del documento.

2. Migración de los sistemas actuales al ambiente de Intranet.

En este último modelo la revisión se convierte en parte del proceso de actualización y la información es usado cuando se necesita.

#### **Desarrollo de Aplicaciones Cliente/Servidor:**

Las aplicaciones cliente/servidor tradicionalmente manejan dos o tres capas:

1. Front End

2. Middleware

3. Back End

Actualmente el desarrollo del Front End se realiza por medio de herramientas como Visual Basic, Delphi, C++ y se instala en cada una de las computadoras. Actualizar o añadir nuevos módulos a las aplicaciones es costoso y lento. Además las aplicaciones se deben compilar para cada plataforma.

Con el nuevo paradigma del explorador de Internet como cliente universal este problema es eliminado por varios factores:

- Las aplicaciones residen en las páginas Web.
- Los objetos y componentes se instalan automáticamente o de manera muy sencilla.
- Existen exploradores para todos los sistemas operativos.



## 4.5 Extranet

Extranet es la extensión de una Intranet de una Corporación más allá de esta. Es decir deja de ser exclusivamente para el uso de la organización y amplía este concepto a los clientes y los proveedores con los que cuenta la organización.

A pesar de la diferencia entre la Intranet y la Extranet, en las arquitecturas de ambas no existe tal diferencia y son implementadas con las mismas herramientas, aunque sus usuarios finales serán gente externa a la Corporación.

## 4.6 Seguridad De Las Intranets / Extranet

Cualquier Intranet es vulnerable a los ataques de personas que tengan el propósito de destruir o robar datos empresariales. La naturaleza sin limites de Internet y los protocolos TCP/IP exponen a una empresa a este tipo de ataques. Las Intranets requieren varias medidas de seguridad, incluyendo las combinaciones de hardware y software que proporcionan el control del tráfico; la encriptación y las contraseñas para convalidar usuarios; y las herramientas del software para evitar y curar de virus, bloquear sitios indeseables, y controlar el tráfico. En esta sección veremos la seguridad desde un punto de vista aplicado a la Intranet aunque para conocer el tema más profundamente consultar el módulo de seguridad posterior a este.

El término genérico usado para denominar a una línea de defensa contra intrusos es firewall. Un firewall es una combinación de hardware / software que controla el tipo de servicios permitidos hacia o desde la Intranet.

Los servidores sustitutos son otra herramienta común utilizada para construir un firewall. Un servidor sustituto permite a los administradores de sistemas seguir la pista de todo el tráfico que entra y sale de una Intranet.

Un firewall de un servidor bastión se configura para oponerse y evitar el acceso a los servicios no autorizados. Normalmente está aislado del resto de la Intranet en su propia subred de perímetro. De este modo si el servidor es "allanado", el resto de la Intranet no estará en peligro. Los sistemas de autenticación son una parte importante en el diseño de la seguridad de cualquier Intranet. Los sistemas de autenticación se emplean para asegurar que cualquiera de sus recursos, es la persona que dice ser. Los sistemas de autenticación normalmente utilizan nombres de usuario, contraseñas y sistemas de encriptación.



El software para el bloqueo de sitios basado en el servidor de sitios basado en el servidor puede prohibir a los usuarios de una Intranet la obtención de material indeseable. EL software de control rastrea dónde ha ido la gente y qué servicios han usado, como HTTP para el acceso a la Web. El software para detectar virus basado en el servidor puede comprobar cualquier archivo que entra en la Intranet para asegurarse que está libre de virus.

Una manera de asegurarse de que las personas impropias o los datos erróneos no pueden acceder a la Intranet es usar un enrutador para filtrar. Este es un tipo especial de enrutador que examina la dirección IP y la información de cabecera de cada paquete que entra en la Intranet, y sólo permite el acceso a aquellos paquetes que tengan direcciones u otros datos, como e-mail, que el administrador del sistema ha decidido previamente que pueden acceder a la Intranet.

### **Enrutadores para filtrar**

Los enrutadores para filtrar, algunas veces denominados enrutadores de selección, son la primera línea de defensa contra ataques a la Intranet. Los enrutadores para filtrar examinan cada paquete que se mueve entre redes en una Intranet. Un administrador de Intranets establece las reglas que utilizan los enrutadores para tomar decisiones sobre qué paquetes deberían admitir o denegar.

Las distintas reglas se pueden establecer para paquetes que entran y que salen de modo que los usuarios de Intranets puedan acceder a los servicios de Internet, mientras que cualquiera en Internet tendría prohibido el acceso a ciertos servicios y datos de la Intranet. Los enrutadores para filtrar pueden llevar el registro sobre la actividad de filtración. Comúnmente, siguen la pista a los paquetes sin permiso para pasar entre Internet y la Intranet, que indicarían que una Intranet ha estado expuesta al ataque.

Las direcciones de origen se leen desde la cabecera IP y se comparan con la lista de direcciones de origen en las tablas de filtros. Ciertas direcciones pueden ser conocidas por ser peligrosas y al incluir en la tabla permiten el enrutador denegar ese tráfico. El enrutador examina los datos en la cabecera IP que envuelve los datos y la información de cabecera de la pila de transporte. Eso significa que cualquier paquete contendrá datos, y dos conjuntos de cabeceras: una para la pila de transporte y otra para la pila de Internet. Los enrutadores para filtrar examinan todos estos datos y cabecera para decidir si permiten pasar a los paquetes. Los enrutadores pueden tener reglas diferentes para las subredes ya que pueden necesitar distintos niveles de seguridad. Una subred que contenga información privada financiera o competitiva puede tener muchas restricciones. Una subred de ingeniería puede tener menos restricciones en actividad que entran o salen.

Un enrutador para filtrar puede permitir a los usuarios tener acceso a servicios como Telnet y FTP, mientras que restringe el uso de Internet de estos servicios para acceder a la Intranet. Esta misma técnica se puede emplear para evitar que los usuarios internos accedan a datos restringidos de una Intranet. Por ejemplo, puede permitir a los miembros financieros el uso abierto de FTP mientras que deniega las peticiones FTP del departamento de ingeniería en el departamento de finanzas. Cierta tipo de servicios son más peligrosos que otros. Por ejemplo, FTP se utiliza

para recibir archivos pero puede traer archivos que contengan un virus. Telnet y el comando *roglin* (que es como Telnet pero con mayor riesgo de burlar la seguridad) están prohibidos por las reglas en la tabla de filtros que evalúan este tipo de servicio por el número del puerto de origen o destino. Trucar direcciones es un método de ataque común. Para trucar direcciones, alguien externo a la Intranet falsifica una dirección de origen de modo que el enrutador le parezca que la dirección de origen es realmente de alguien de dentro de la Intranet. El intruso espera engañar al enrutador para filtrar, para que le permita un mayor acceso a la Intranet que el que le permite una dirección externa original. Una vez que el enrutador se convenció de que el intruso estaba ya dentro de la Intranet, los archivos privados podrían enviarse potencialmente fuera de la Intranet. Los enrutadores pueden manejar direcciones truncadas. Se puede establecer una regla que comunique al enrutador examinar la dirección de origen en cada cabecera IP que entre, pero que no salga. Si la dirección de origen es interna, pero el paquete proviene del exterior, el enrutador no admitirá el paquete.

## Firewalls

Los firewalls protegen a las Intranets de los ataques iniciados contra ellas desde Internet. Están diseñados para proteger a una Intranet del acceso no autorizado a la información de la empresa, y del daño o rechazo de los recursos y servicios informáticos. También están diseñados para impedir que los usuarios internos accedan a los servicios de Internet que puedan ser peligrosos, como FTP.

Las computadoras de las Intranets sólo tienen permiso para acceder a Internet después de atravesar un firewall. Las peticiones tienen que atravesar un enrutador interno de selección, llamado también enrutador interno para filtrar o enrutador de obstrucción. Este enrutador evita que el tráfico de paquetes sea "husmeado" remotamente. Un enrutador de obstrucción examina la información de todos los paquetes como cuál es su origen y cuál su destino. El enrutador compara la información que encuentra con las reglas en una tabla de filtros, y admite, o no, los paquetes basándose en esas reglas. Por ejemplo, algunos servicios, como *roglin*, no pueden tener permiso para ejecutarse. El enrutador no permite tampoco que cualquier paquete se envíe a localizaciones específicas del Internet sospechosas. Un enrutador también puede bloquear cada paquete que viaje entre Internet y la Intranet, excepto el e-mail. Los administradores de sistemas qué paquetes admitir y cuáles denegar. Cuando una Intranet está protegida por un firewall, están disponibles los servicios internos usuales de la red, como el e-mail, el acceso a las bases de datos corporativas y a los servicios de la Web, y el uso de programas para el trabajo en grupo.

Los firewall seleccionados de la subred tiene una manera más para proteger la Intranet: un enrutador exterior de selección, también denominado enrutador de acceso. Este enrutador selecciona paquetes entre Internet y la red de perímetro utilizando el mismo tipo de tecnología que el enrutador interior de selección. Puede seleccionar paquetes basándose en las mismas reglas que aplica el enrutador interior de selección y puede proteger a la red incluso si el enrutador interno falla. Sin embargo, también puede tener reglas adicionales para la selección de paquetes diseñadas eficazmente para proteger al anfitrión bastión. Como un modo adicional para proteger a una Intranet del ataque, el anfitrión bastión se coloca en una red de perímetro, una subred, dentro del firewall. Si el anfitrión bastión estuviera en la Intranet en vez de en una red de perímetro y fuera, el intruso podría obtener acceso a la Intranet. Un anfitrión

bastión es el punto de contacto principal para las conexiones provenientes de Internet para todos los servicios como el e-mail, el acceso FTP, y cualquier otros datos y peticiones. El anfitrión bastión atiende todas esas peticiones, las personas en la Intranet sólo se ponen en contacto con este servidor, y no contactan directamente con otros servidores de Intranets. De este modo, los servidores de Intranets están protegidos del ataque. Los anfitriones bastión también pueden configurarse como servidores sustitutos.

### **Servidores sustitutos**

Una parte integral de muchos de los sistemas de seguridad es el servidor sustituto. Un servidor sustituto software y un servidor que se coloca en un firewall y actúa como intermediario entre computadoras en una Intranet e Internet. Los servidores sustitutos a menudo se ejecutan en anfitriones bastión. Solo el servidor sustituto en vez de las muchas computadoras individuales en la Intranet, interactúan con Internet, de este modo la seguridad se puede mantener porque el servidor puede estar más seguro que los cientos de computadoras individuales en la Intranet. Los administradores de Intranets pueden configurar servidores sustitutos que puedan utilizarse para muchos servicios, como FTP, la Web y Telnet. Los administradores de Intranets deciden que servicios de Internet deben atravesar un servidor sustituto, y cuales no. Se necesita software específico del servidor sustituto para cada tipo diferente de servicio Internet.

Cuando una computadora en la Intranet realiza una petición a Internet, como recuperar una página Web desde un servidor Web, la computadora interna se pone en contacto con el servidor Internet, El servidor Internet envía la página Web al servidor sustituto, que después la mandará a la computadora de la Intranet. Los servidores sustitutos registran todo en tráfico entre Internet y la Intranet, por ejemplo, un servidor sustituto de Telnet podría seguir la pista de cada pulsación de una tecla en cada sección Telnet en la Intranet, y también podría seguir la pista de cómo reacciona al servidor externo en Internet con esas pulsaciones. Los servidores sustitutos pueden anotar cada dirección IP, fecha y hora de acceso, URL, número de bytes recibidos, etc. Esta información se puede utilizar para analizar cualquier ataque iniciado contra la red. También puede ayudar a los administradores de Intranets a construir mejor acceso y servicios para los empleados. Algunos servidores sustitutos tienen que trabajar con clientes sustitutos especiales. Una tendencia más popular es usar clientes con servidores sustitutos ya configurados como Netscape. Cuando se emplea este paquete ya hecho, debe configurarse especialmente para trabajar con servidores sustitutos desde el menú de configuración. Después el empleado de la Intranet usa el software cliente como de costumbre. El software cliente sabe salir hacia un servidor sustituto para obtener datos, en vez de hacia Internet.

Los servidores sustitutos pueden hacer algo más que hacer llegar las peticiones entre una Intranet e Internet. También pueden hacer efectivos los diseños de seguridad. Por ejemplo podría configurarse para permitir en envío de archivos desde Internet a una computadora de la Intranet, pero impedir que se manden archivos desde la red empresarial a Internet, o viceversa. De este modo, los administradores de Intranets pueden impedir que cualquier persona externa a la corporación reciba datos corporativas vitales. O pueden evitar que los usuarios de la Intranet reciban archivos que puedan contener virus. Los servidores sustitutos también se pueden utilizar para acelerar la actuación de algunos servicios de Internet almacenando datos. Por ejemplo, un servidor Web sustituto podría

almacenar muchas paginas Web, a fin de que cuando alguien desde la Intranet quisiera obtener alguna de esas páginas Web, accediera ella directamente desde el servidor sustituto a través de líneas de la Intranet de alta velocidad, en lugar de tener que salir a través de Internet y obtener la página a menor velocidad desde las líneas de Internet.

### **Anfitriones bastión**

Un anfitrión bastión (llamado también servidor bastón) es una de las defensas principales en el firewall de una Intranet. Es un servidor fuertemente fortificado que se coloca dentro del firewall, y es el punto de contacto principal de la Intranet e Internet. Al tener como punto de contacto principal un servidor aislado, duramente defendido, el resto de los recursos de la Intranet pueden proteger de los ataques que se inician en Internet.

Los anfitriones bastión se construyen para que cada servicio posible de la red quede inutilizado una vez dentro de ellos, lo único que hace el servidor es permitir el acceso específico de Internet. Así que, por ejemplo, no debería haber ninguna cuenta de usuarios en un servidor bastión, para que nadie pudiera entrar, tomar el control y después obtener acceso a la Internet. Incluso el Sistema de Archivos de Red (NFS), que permite a un sistema el acceso a archivos a través de una red en un sistema remoto, debería inhabilitarse para que los intrusos no pudieran acceder al servidor bastión es instalarlo en su propia subred como parte del firewall de una Intranet. Al colocarlos en su propia red, si son atacados, ningún recurso de la Intranet se pone en peligro.

Los servidores bastión registran todas las actividades para que los administradores de Intranets puedan decir la red ha sido atacada. A menudo guardan dos copias de los registros del sistema por razones de seguridad: en caso de que se destruya o falsifique un registro, el otro siempre disponible como reserva. Un modo de guardar una copia segura del registro es conectar el servidor bastión mediante un puerto de serie con una computadora especializada, cuyo único propósito es seguir la pista del registro de reserva.

Los monitores automatizados son programas incluso más sofisticados que el software de auditoria. Comprueban con regularidad los registros del sistema del servidor bastión, y envían una alarma si encuentra un patrón sospechoso. Por ejemplo, se puede enviar una alarma si alguien intenta más de tres conexiones no exitosas. Algunos servidores bastión incluyen programas de auditoria, que examinan activamente si se ha iniciado un ataque en su contra. Hay varias maneras de hacer una auditoria: una manera de revisar esto es utilizar un programa de control que compruebe si algún software en el servidor bastión se ha modificado por una persona no autorizada. El programa de control calcula un número basándose en el tamaño de un programa ejecutable que hay en el servidor. Después calcula con regularidad el número de control para ver si ha cambiado desde la última vez que lo hizo. Si ha cambiado, significa que alguien ha alterado el software, lo que podría indicar un ataque externo.

Cuando un servidor bastión recibe una petición de un servidor como puede ser enviar una pagina Web o repartir e-mail, el servidor no administra la petición él mismo; en su lugar, envía la petición al servidor de Intranets apropiado. EL servidor de Intranets maneja la petición, y después devuelve la información al servidor bastión; y será ahora cuando envíe la información requerida al solicitarme en Internet.

Puede haber más de un anfitrión bastión en un firewall; y cada uno puede administrar varios servicios de Internet para la Intranet. Algunas veces, un anfitrión bastión se puede utilizar como maquina victima: un servidor despojado de casi todos los servicios excepto de uno especifico de Internet. Las máquinas victimas pueden emplearse para ofrecer servicios de Internet que son difíciles de manejar o cuyas limitaciones sobre la seguridad no se conocen aún, utilizando un enrutador sustituto o uno para filtrar. Los servidores se colocan en la máquina victima en vez de en un anfitrión bastión con otros servicios. De ese modo, si se irrumpe en el servidor, los otros anfitriones bastión no estarán afectados.

