www.monografías.com

Intranet

Una Intranet es una red privada que la tecnología Internet usó como arquitectura elemental. Una red interna se construye usando los protocolos TCP/IP para comunicación de Internet, que pueden ejecutarse en muchas de las plataformas de hardware y en proyectos por cable. El hardware fundamental no es lo que construye una Intranet, lo que importa son los protocolos del software. Las Intranets pueden coexistir con otra tecnología de red de área local. En muchas compañías, los “sistemas patrimoniales” existentes que incluyen sistemas centrales, redes Novell, mini - computadoras y varias bases de datos, se están integrando en un Intranet. Una amplia variedad de herramientas permite que esto ocurra. El guión de la Interfaz Común de Pasarela (CGI) se usa a menudo para acceder a bases de datos patrimoniales desde una Intranet. El lenguaje de programación Java también puede usarse para acceder a bases de datos patrimoniales.

Con el enorme crecimiento de Internet, un gran numero de personas en las empresas usan Internet para comunicarse con el mundo exterior, para reunir información, y para hacer negocios. A la gente no le lleva mucho tiempo reconocer que los componentes que funcionan tan bien en Internet serían del mismo modo valioso en el interior de sus empresas y esa es la razón por la que las Intranets se están haciendo tan populares. Algunas corporaciones no tienen redes TCP/IP: el protocolo requerido para acceder a los recursos de Internet. Crear una Intranet en la que todas las informaciones y recursos se puedan usar sin interrupciones tiene muchos beneficios. Las redes basadas en TCP/IP facilitan las personas el acceso a la red remotamente,

desde casa o mientras viajan. Contactar con una Intranet de este modo es muy parecido a conectar con Internet, La operabilidad interna entre redes es otro suplemento sustancial. Los sistemas de seguridad separan una Intranet de Internet. La red interna de una compañía está protegida por firewall: combinaciones de hardware y software que sólo permiten a ciertas personas acceder a ella para propósitos específicos. Se puede utilizar para cualquier cosa para la que se empleaban las redes existentes. La facilidad que tiene para publicar información en la WWW las ha convertido en lugares utilizados para enviar información de empresa como las noticias y procedimientos de la compañía. Las bases de datos empresariales con procesadores sencillos usan la Web y lenguajes de programación como Java.

Las Intranets permiten a los usuarios trabajar juntos de un modo más sencillo y efectivo. EL programa conocido como trabajo en grupo es otra parte importante de las redes internas. Nos permite colaborar en proyectos, compartir información, llevar a cabo conferencias visuales, y establecer procedimientos seguros para el trabajo de producción. EL software del servidor y del cliente gratuito y la multitud de servicios como los grupos de noticias, estimulan la expansión de Internet. La consecuencia de ese crecimiento avivó y provocó el desarrollo de las Intranets.

UNA VISION GLOBAL DE UNA INTRANET

Una Intranet es una red privada empresarial o educativa que utiliza los protocolos TCP/IP de Internet para su transporte básico. Los protocolos pueden ejecutar una variedad de Hardware de red, y también, pueden coexistir con otros protocolos de red, como IPX. Aquellos empleados que están dentro de una Intranet pueden acceder a los amplios recursos de Internet, pero aquellos en Internet no pueden entrar en la Intranet, que tiene acceso restringido.

Una Intranet se compone frecuentemente de un numero de redes diferentes dentro de una empresa que se comunica con otra mediante TCP/IP. Estas redes separadas se conocen a menudo como sub - redes. El software que permite a la gente comunicarse entre ella vía e-mail y tablones de mensaje públicos, y colaborar en la producción usando software de grupos de trabajo, está entre los programas de Intranets más poderoso. Las aplicaciones que permiten a los distintos departamentos empresariales enviar información, y a los empleados rellenar formularios de la empresa (como las hojas de asistencia) y utilizar la información corporativa financiera, son muy populares. La mayoría del software que se utiliza en las Intranets es estándar: software de Internet como el Netscape, Navigator y los navegadores Explorer para Web de Microsoft. Y los programas personalizados se construyen frecuentemente usando el lenguaje de programación de Java y el de guión de CGI.

Las Intranets también se pueden utilizar para permitir a las empresas llevar a cabo transacciones de negocio a negocio como: hacer pedidos, enviar facturas, y efectuar pagos. Para mayor seguridad, estas transacciones de Intranet a Intranet no necesitan nunca salir a Internet, pero pueden viajar por líneas alquiladas privadas. Son un sistema poderoso para permitir a una compañía hacer negocios en línea, por ejemplo, permitir que alguien en Internet pida productos. Cuando alguien solicita un producto en Internet, la información se envía de una manera segura desde Internet a la red interna de la compañía, donde se procesa y se completa el encargo. La información enviada a través de una Intranet alcanza su lugar exacto mediante los enrutadores, que examinan la dirección IP en cada paquete TCP(IP y determinan su destino. Después envía el paquete al siguiente direcciónador. Si este tiene que entregarse en una dirección en la misma sub - red de la Intranet desde la que fue enviado, llega directamente sin tener que atravesar otro enrutador. Si tiene que mandarse a otra sub – red de trabajo en la Intranet, se enviará a otra ruta. Si el paquete tiene que alcanzar un destino externo a la Intranet a la Intranet en otras palabras, Internet se envía a un enrutador que conecte con Internet.

Para proteger la información corporativa delicada, y para asegurar que los piratas no perjudican a los sistemas informáticos y a los datos, las barreras de seguridad llamadas firewalls protegen a una Intranet de Internet. La tecnología firewall usa una combinación de enrutadores, servidores y otro hardware y software para permitir a los usuarios de una Intranet utilizar los recursos de Internet, pero evitar que los intrusos se introduzcan en ella. Mucha Intranets tienen que conectarse a “sistemas patrimoniales”: el hardware y las bases de datos que fueron creadas antes de construir la Intranet. A menudo los sistemas patrimoniales usan tecnologías más antigua

no basada en los protocolos TCP/IP de las Intranets. Hay varios modos mediante los que las Intranets se pueden unir a sistemas patrimoniales. Un método común es usar los guiones CGI para acceder a la información de las bases de datos y poner esos datos en texto HTML formateado. Haciéndolos asequibles a un navegador para Web.

COMO FUNCIONA TCP/IP E IPX EN LAS INTRANETS

Lo que distingue una Intranet de cualquier otro tipo de red privada es que se basa en TCP/IP: los mismos protocolos que se aplican a Internet. TCP/IP se refiere a los dos protocolos que trabajan juntos para transmitir datos: el Protocolo de Control de Transmisión (TCP) y el Protocolo Internet (IP). Cuando envías información a través de una Intranet, los datos se fragmentan en pequeños paquetes. Los paquetes llegan a su destino, se vuelven a fusionar en su forma original. El Protocolo de Control de Transmisión divide los datos en paquetes y los reagrupa cuando se reciben. El Protocolo Internet maneja el encaminamiento de los datos y asegura que se envían al destino exacto.

En algunas empresas, puede haber una mezcla de Intranets basadas en TCP/IP y redes basadas en otra tecnología, como NetWare. En este caso, la tecnología TCP/IP de una Intranet se puede utilizar para enviar datos entre NetWare y otras redes, usando una técnica llamada IP canalizado. Las redes NetWare usan el protocolo IPX(Intercambio de Paquetes en Internet) como medio de entregar datos y las redes TCP/IP no pueden reconocer este protocolo. Cuando un paquete IP mediante un servidor NetWare especifico y que se dedica a ofrecer el mecanismo de transporte del IP para los paquetes IPX.

Los datos enviados dentro de una Intranet deben separase en paquetes menores de 1.500 caracteres. TCP divide los datos en paquetes. A medida que crea cada paquete, calcula y añade un número de control a éstos. El número de control se basa en los valores de los bytes, es decir, la cantidad exacta de datos en el paquete.

Cada paquete, junto al número de control, se coloca en envases IP o “sobre” separados. Estos envases contienen información que detalla exactamente donde se van a enviar los datos dentro de la Intranet o de Internet. Todos los envases de una clase de datos determinada tienen la misma información de direccionamiento así que se pueden enviar a la misma localización para reagruparse.

Los paquetes viajan entre redes Intranets gracias a enrutadores de Intranets. Los enrutadores examinan todos los envases IP y estudian sus direcciones. Estos direccionadores determinan la ruta más eficiente para enviar cada paquete a su destino final. Debido a que él trafico en una Intranet cambia frecuentemente, los paquetes se pueden enviar por caminos diferentes y puedan llegar desordenados. Si el enrutador observa que la dirección está localizada dentro de la Intranet, el paquete se puede enviar directamente a su destino, o puede enviarse a otro enrutador. Si la dirección se localiza fuera de Internet, se enviará a otro enrutador para que se pueda enviar a través de ésta.

A medida que los paquetes llegan a su destino, TCP calcula un número de control para cada uno. Después compara este número de control con el número que se ha enviado en el paquete. Si no coinciden, CP sabe que los datos en el paquete se han degradado durante él envió. Después descarta el paquete y solicita la retransmisión del paquete origina.

TCP incluye la habilidad de comprobar paquetes y determinar que se han recibido todos. Cuando se reciben os paquetes no degradaos, TCP los agrupa en su forma original, unificada. La información de cabecera de los paquetes comunica el orden de su colocación.

Una Intranet trata el paquete IP como si fuera cualquier otro, y envía el paquete a la red NetWare receptora, un servidor TCP/IP NetWare abre el paquete IP descarta el paquete IP, y lee el paquete IPX original. Ahora puede usar el protocolo IPX para entregar los datos en el destino exacto.

COMO FUNCIONA EL MODELO OSI

La organización Internacional para la Normalización (ISO) ha creado el modelo de referencia “Interconexión de Sistemas Abiertos” (OSI), que describe siete pilas de protocolos para comunicaciones informáticas. Estas pilas no conocen o no se preocupan de lo que hay en pilas

adyacentes. Cada pila, esencialmente, sólo ve la pila recíproca en el otro lado. La pila destinada a enviar la aplicación observa y se comunica con la pila de aplicación en el destino. Esa conversación tiene lugar sin considerar, por ejemplo, qué estructura existe en la pila física, como Ethernet o Token Ring. TCP combina las pilas de aplicación, presentación y sesión del modelo OSI en una que también se llama pila de aplicación.

COMO SE PROCESAN LOS PAQUETES TCP/IP

Los protocolos como TCP/IP determinan cómo se comunican las computadoras entre ellas por redes como Internet. Estos protocolos funcionan conjuntamente, y se sitúan uno encima de otro en lo que se conoce comúnmente como pila de protocolo. Cada pila del protocolo se diseña para llevar a cabo un propósito especial en la computadora emisora y en la receptora. La pila TCP combina las pilas de aplicación, presentación y sesión en una también denominada pila de aplicación.

En este proceso se dan las características del envasado que tiene lugar para transmitir datos:

- La pila de aplicación TCP formatea los datos que se están enviando para que la pila inferior, la de transporte, los pueda remitir. La pila de aplicación TCP realiza las operaciones equivalentes que llevan a cabo las tres pilas de OSI superiores: aplicaciones, presentación y sesión.
- La siguiente pila es la de transporte, que es responsable de la transferencia de datos, y asegura que los datos enviados y recibidos son de hecho los mismos, en otras palabras, que no han surgido errores durante él envió de los datos. TCP divide los datos que obtiene de pila de aplicación en segmento. Agrega una cabecera contiene información que se usará cuando se reciban los datos para asegurar que no han sido alterados en ruta, y que los segmentos se pueden volver a combinar correctamente en su forma original.
- La tercera pila prepara los datos para la entrega introduciéndolos en data gramas IP, y determinando la dirección Internet exacta para estos. El protocolo IP trabaja en la pila de Internet, también llamada pila de red. Coloca un envase IP con una cabecera en cada segmento. La cabecera IP incluye información como la dirección IP de las computadoras emisoras y receptoras, la longitud del data grama y el orden de su secuencia. El orden secuencial se añade porque el data grama podría sobrepasar posiblemente el tamaño permitido a los paquetes de red, y de este modo necesitaría dividirse en paquetes más pequeños. Incluir el orden secuencial les permitiría volverse a combinar apropiadamente.

COMO FUNCIONAN LOS PUENTES

Los puentes son combinaciones de hardware y software que conectan distintas partes de una red, como las diferentes secciones de una Intranet. Conectan redes de área local (LAN) entre ellas. Sin embargo, no se usan generalmente para conectar redes enteras entre ellas, por ejemplo: para conectar una Intranet con Internet; o una Intranet con otra, o para conectar una sub – red completa con otra. Para hacer eso, se usan piezas de tecnología más sofisticada llamadas enrutadores.

Cuando hay gran cantidad de trafico en una red de área local Ethernet, los paquetes pueden chocar entre ellos, reduciendo la eficacia de la red, y atrasando el tráfico de la red. Los paquetes pueden colisionar porque se encamina mucho trafico entre todas las estaciones de trabajo en la red.

Para reducir la proporción de colisiones, una LAN se puede subdividir en dos o más redes. Por ejemplo, una LAN se puede subdividir en varias redes departamentales. LA mayoría del tráfico en cada red departamental se queda dentro de la LAN del departamento, y así no necesita viajar a través de todas las estaciones de trabajo en todas las LAN de la red. De este modo, se reducen las colisiones. Los puentes se usan para enlazar las LAN. El único tráfico que necesita cruzar puentes es el que navega con rumbo a otra LAN. Cualquier trafico con la LAN no necesita cruzar un puente.

Cada paquete de datos en una Intranet posee más información que la del IP. También incluye información de direccionamiento requerida para otra arquitectura de red básica, como Ethernet. Los puentes comprueban esta información de la red externa y entregan el paquete en la dirección exacta en una LAN.

Los puentes consultan una tabla de aprendizaje que contiene las direcciones de todos los nodos de la red. Si un puente descubre que un paquete pertenece a su LAN, mantiene el paquete en la LAN. Si descubre que la estación de trabajo está en otra LAN, envía el paquete. El puente actualiza constantemente la tabla de aprendizaje a medida que controla y encamina el tráfico.

Los puentes pueden conectar redes de área local de varias formas diferentes. Pueden conectar LAN usando conexiones en serie por líneas telefónicas tradicionales y módems, por líneas ISDN, y por conexiones directas por cable. Las unidades CSU / DSU se usan para conectar puentes con líneas telefónicas mediante conductividad remota.

Los puentes y enrutadores se combinan algunas veces en un solo producto llamado brouter. Un brouter ejecuta las tareas de ambos. Si los datos necesitan sólo enviarse a otra LAN en la red o sub – red, solamente actuará como un puente, entregando los datos basados en la dirección Ethernet. Si el destino es otra red, actuará como un enrutador, examinando los paquetes IP y encaminando los datos basados en la dirección IP.

COMO FUNCIONAN LOS ENRUTADORES DE LAS INTRANETS

Los enrutadores son los guardias de tráfico de las Intranets. Se aseguran que todos los datos se envían donde se supone que tienen que ir y de que lo hacen por la ruta más eficaz. Los enrutadores también son herramientas útiles para sacar el mejor rendimiento de la Intranet. Se emplean para desviar el tráfico y ofrecer rutas. Los enrutadores utilizan la encapsulación para permitir el envío de los distintos protocolos a través de redes incompatibles.

Los enrutadores abren el paquete IP para leer la dirección de destino, calcular la mejor ruta, y después enviar el paquete hacia el destino final. Si el destino está en la misma parte de una Intranet, el enrutador enviará el paquete directamente a la computadora receptora. Si el paquete se destina a otra Intranet o sub – red (o si el destino está en Internet), el enrutador considera factores como la congestión de tráfico y él numero de saltos – términos que se refiere al número de enrutadores o pasarelas en una ruta dada. El paquete IP lleva consigo un segmento que cuenta los saltos y un enrutador no usará una red que exceda de un número de saltos predeterminado. Las rutas múltiples – dentro de un número aceptable de saltos, son convenientes para ofrecer variedad y para asegurar que los datos se pueden transmitir. Por, ejemplo, si una ruta directa entre Madrid y Barcelona no estuviera disponible, los enrutadores sofisticados enviarán los datos a Barcelona por otro enrutador probablemente en otra ciudad en la Intranet, y esto sería transparente para los usuarios.

Los enrutadores tienen dos o más puertos físicos: los de recepción (de entrada) y los de envío (de salida). En realidad, cada puerto es bidireccional y puede recibir o enviar datos. Cuando se recibe un paquete en un puerto de entrada, se ejecuta una rutina de software denominada proceso de encaminamiento. Este proceso investiga la información de cabecera en el paquete IP y encuentra la dirección a la que se están enviando los datos. Luego compara esta dirección con una base de datos llamada tabla de encaminamiento que posee información detallando a que puertos deberían enviarse los paquetes con varias direcciones IP. Basándose en lo que encuentra en la tabla de encaminamiento, envía el paquete en un puerto de salida específico. Este puerto de salida envía después los datos al siguiente enrutador o al destino.

A veces. Los paquetes se mandan a un puerto de entrada de un enrutador antes de que pueda procesarlos. Cuando esto ocurre, los paquetes se envían a un área de contención especial llamada cola de entrada, un área de RAM en el enrutador. Esa cola de entrada específica está asociada con un puerto de entrada concreto. Un enrutador puede tener más de una cola de entrada, si varios puertos de entrada están enviando paquetes más aprisa que el enrutador puede procesarlos. Cada puerto de entrada procesará los paquetes de la cola en el orden en que se recibieron.

Si él tráfico a través del enrutador es muy denso, el número de paquetes en la cola puede ser mayor que su capacidad. (La capacidad de la cola se denomina longitud). Cuando esto ocurre,

es posible que los paquetes se abandonen y de este modo no serán procesados por el enrutador, y no se enviarán a su destino. Aunque esto no significa que se tenga que perder la información. El protocolo TCP se diseño para tener en cuenta que los paquetes pueden perderse de camino a su destino final. Si nos envían todos los paquetes al receptor, TCP en la computadora receptora identifica y pide que se vuelvan a enviar los paquetes perdidos. Seguirá solicitando él reenvió de los paquetes hasta que reciban todos. Los enrutadores sofisticados pueden manejarse y los problemas diagnosticarse y resolverse usando software especial, como SNMP(Protocolo Simple de Administración de Red). TCP puede decidir que decisiones tiene que tomar porque hay varias banderas en el paquete, como el número de saltos en IP, que comunica a TCP lo que necesita para saber cómo actuar. Por ejemplo, la bandera ack, indica que esta respondiendo (reconociendo) a una comunicación previa.

Se utilizan varios tipos de tablas en ruta. En el tipo de Intranet más simple denominada tabla de encaminamiento mínimo. Cuando una Intranet se compone de una sola red TCP/IP o a Internet, se puede usar encaminamiento mínimo. En encaminamiento mínimo, un programa llamado ifconfig crea automáticamente la tabla, que contiene únicamente unas pocas entradas básicas. Puesto que hay muy pocos lugares a los que se pueden enviar los datos, sólo se necesita configurar un número mínimo de enrutadores.

Si una Intranet tiene solamente un número limitado de redes TCP/IP, se puede utilizar una tabla de encaminamiento estático. En este caso, los paquetes con direcciones específicas se envían a enrutadores específicos. Los enrutadors no desvían paquetes para modificar el tráfico variable de la red. El encaminamiento estático debería utilizarse cuando sólo hay una ruta para cada destino. Una tabla de encaminamiento estático permite a un administrador de Intranets añadir o eliminar entradas en ésta.

Las tablas de encaminamiento dinámico son las más sofisticadas. Deberían usarse cuando hay más de una manera para enviar datos desde un enrutador al destino final, y en Intranets más complejas. Estas tablas cambian constantemente a medida que varía el trafico de la red y las condiciones, así que siempre encaminan datos del modo más eficiente posible, teniendo en cuanta el estado actual del tráfico de la Intranet.

Las tablas de encaminamiento dinámico se construyen utilizando protocolos de encaminamiento. Estos protocolos son medios por los que se comunican los enrutadores, ofreciendo información sobre la manera más eficaz de encaminar datos dado el estado actual de la Intranet. Un enrutador con una tabla de encaminamiento dinámico puede desviar datos a una ruta de apoyo si la ruta primaria es reducida. También puede determinar siempre el método más eficiente de encaminar datos hacia su destino final. Los enrutadores exponen sus direcciones IP y conocen las direcciones IP de sus vecinos. Los enrutadores pueden usar esta información en un algoritmo para calcular la mejor ruta para enviar paquetes.

El protocolo de encaminamiento más común que realiza estos cálculos se conocen como RIP (Protocolo de Información de Encaminamiento). Cuando RIP determina la ruta más eficaz para enviar datos el camino con el menor número de saltos. Asume que cuantos menos saltos haya, más eficaz un número de saltos mayor que 16, descartará la ruta.

El Protocolo de Pasarela Exterior (EGP) se usa en Internet donde se puede tener que atravesar muchos más enrutadores antes de que un paquete alcance su destino final.

El factor a tener en cuenta sobre Intranets y Tecnología de encaminamiento es que no es una situación “o se da una u otra”, sino que pueden utilizar muchos tipos de tecnologías de encaminamiento, dependiendo de las necesidades de esa parte particular de la red. Algunas partes pueden ser capaces de emplear enrutadores con tablas de encaminamiento estático, mientras que otras partes pueden necesitar tablas de encaminamiento dinámico.

COMO SE REPARTE EL E-MAIL DENTRO DE UNA INTRANET

Probablemente la parte más usada de una Intranet que no tiene nada que ver con bases de datos de la empresa, páginas Web ostentosas. O contenido multimedia es el uso del correo electrónico. Las Intranets empresariales pueden emplear diferentes programas e-mail, como cc: Mail Microsoft Mail o Lotus Notes, entre otros. Pero la Arquitectura más común que sirve de base

al uso del e-mail de las redes internas es el protocolo llamado Protocolo simple de Transferencia de Correo, o SMTP.

Como se utiliza SMTP para repartir correo dentro de una Intranet:

- Como sucede con muchas aplicaciones de Intranets y de Internet, SMTP usa una arquitectura cliente / servidor. Cuando alguien quiere crear un mensaje, usa un agente usuario de correo o agente usuario (MUA o UA), software cliente que se ejecuta en un computador, para crear un fragmento de correo electrónico. Este MUA puede ser cualquiera de los programas e-mail, y puede ejecutarse en varias computadoras diferentes, incluyendo PC, Macintosh,, y estaciones de trabajo UNÍS; Pegasus, Eudora. cc: Mail y Microsoft Mail para PC; y Eudora para Macintosh.
- Después de finalizar el mensaje, el MUA lo manda a un programa que s esta ejecutando en un servidor llamado agente de transferencia de correo (MTA) examina la dirección del receptor de mensaje. Si el receptor del mensaje está en la Intranet, el MTA envía el mensaje a otro programa servidor en la red interna denominado agente de entrega de correo (MDA). Si el receptor está ubicado en Internet o en otra red interna, el archivo llegará al receptor a través de Internet. El MDA examina la dirección del receptor, y envía el correo a la bandeja de entrada d el apersona adecuada.
- Algunos sistemas de correo emplean otro protocolo e-mail llamado el Protocolo de Oficina de Correos (POP) conjuntamente con SMTP. Con POP, el e-mail no se entrega directamente en tu computadora. En lugar de eso, el correo se echa a un buzón en el servidor. Para conseguir el coreo, alguien accede al servidor usando una contraseña y un nombre de usuario, y recupera el mensaje con un agente de correo.
- El receptor del correo puede utilizar ahora un agente usuario de correo para leer el mensaje, archivarlo y responderlo.
- SMTP sólo puede manejar la transferencia de e-mail de archivos de textos ASCII sencillos. Para enviar archivos binarios como hojas de cálculos, dibujos y documentos de procesador de texto, primero deben convertirlos en un formato ASCII codificándolos. Los archivos se pueden codificar usando varios métodos que incluyen codificación y Base64. Algunos software e-mail codificará automáticamente archivos binarios. Cuando alguien recibe un archivo codificado, lo descodifica y después puede usar o examinar el archivo binario. Además muchos paquetes e-mail descodifican automáticamente archivos codificados.

COMO SE REPARTE E-MAIL ENTRE INTRANETS

A menudo el e-mail creado en una Intranet no se entregará a una computadora de la Intranet, sino a alguien en Internet, sino a alguien en Internet, en otra Intranet, o un servidor en línea como América Online, Microsoft Netword, o CompuServe. Aquí están los pasos que un mensaje típico tiene que seguir cuando se envía de una Intranet a otra red o Intranet.

- Un mensaje e-mail se crea usando SMTP. Como ocurre con toda la información enviada a través de Internet, el mensaje es dividido por el Protocolo TCP de Internet en paquetes IP. La dirección la examina el agente de transferencia de correo de la Intranet. Si la dirección se encuentra en otra red, el agente de transferencia de correo enviará el correo a través de la Intranet mediante enrutadores al agente de transferencia de correo en la red receptora.
- Antes de que se pueda enviar el correo a través de Internet, puede que primero tenga que atravesar un firewall, una computadora que protege a la Intranet para que los intrusos no puedan acceder a ella. El firewall sigue la pista de los mensajes y los datos que entran y salen de la Intranet.

- El mensaje deja la Intranet y se envía a un enrutador Internet. El enrutador examina la dirección, determina dónde debería mandarse el mensaje, y después lo pone en camino.
- La red receptora obtiene el mensaje e-mail. Aquí utiliza una pasarela para convertir los paquetes IP en un mensaje completo. Después la pasarela traduce el mensaje al protocolo particular que emplea la red (como el formato de correo de Compu-Serve), y lo pone en camino. Puede que el mensaje también tenga que atravesar un firewall en la red receptora.
- La red receptora examina la dirección e-mail y envía el mensaje al buzón especifico donde el mensaje está destinado a ir, o emplea el Protocolo de Oficina de Correo (POP) para entregarlo a un servidor de correo.
- Las pasarelas realmente pueden modificar los datos (si se necesita) para la conectividad. Para el e-mail, puede convertir el protocolo Compu-Serve en SMTP. Las pasarelas también se utilizan para conectar PC con sistemas centrales IBM, por ejemplo, ASCII con EBCDIC.

COMO FUNCIONA UNA INTRANET

El centro de una Intranet es la World Wide Web. En muchos casos gran parte de la razón por la que se creó una Intranet en primer lugar es que la Web facilita la publicación de la información y formularios por toda la compañía usando el Lenguaje de Marcado de Hipertexto (HTML). La Web permite la creación de páginas iniciales multimedia, que están compuesta de texto, gráficos, y contenidos multimedia como sonido y vídeo. Los enlaces de hipertexto te permiten saltar desde un lugar en la Web a otro, lo que significa que puedes saltar a lugares dentro de una Intranet o fuera en Internet desde una pagina inicial.

- Las Intranets están basadas en la arquitectura cliente / servidor. EL software cliente-un navegador para Web, se ejecuta en una computadora local, y el software servidor en una Intranet anfitriona. El software cliente esta disponible para PC, Macintosh y estaciones de trabajo UNÍS. El software servidor se ejecuta en UNÍS, Windows NT y otros sistemas operativos. El software cliente y el software servidor no necesitan ejecutarse en el mismo sistema operativo. Para una Intranet, primero pone en marcha tu navegador para Web. Si estás conectado directamente con tu Intranet, el programa TCP/IP que necesitas para ejecutar el navegador ya estará instalado en tu computadora.
- Cuando se ponen en marcha los navegadores, visitarán una cierta localización predeterminada. En una Intranet, esa localización puede ser una página Web departamental o una página Web por toda la compañía. Para visitar un sitio diferente, escribe la localización de la Intranet que quieres visitar, o pulsa en un enlace para dirigirte allí. El nombre para cualquier localización Web es el URL(localizador uniforme de recursos). Tu navegador para Web envía la petición URL usando http(Protocolo de Transferencia de Hipertexto) que define el modo en el que se comunican el navegador para Web y el servidor Web.
- Si la petición es de una pagina localizada en la Intranet, los navegadores envían la petición a esa página Web de la Intranet. Puede estar disponible una conexión de alta velocidad, puesto que las Intranet pueden construirse usando cables de alta velocidad, y todo el tráfico dentro de la Intranet se puede conducir por esos cables. La conexión Internet puede ser mucho más lenta debido a la cantidad de tráfico de Internet, y porque puede haber varias conexiones de baja velocidad que la petición desde la Intranet tendrá que atravesar. Los paquetes que componen la petición se encaminan hacia un enrutador de la Intranet, que envía en turnos la petición al servidor Web.
- El servidor Web recibe la petición usando http, la petición es para un documento especifico. Devuelve la página inicial, documento u objetivo al navegador para Web cliente. La información se muestra ahora en la pantalla de la computadora en el navegador Web. Después de enviar el objeto al navegador para Web, la conexión http se cierra para hacer un uso más eficaz de los recursos de la red.

- Los URL constan de varia partes. La primera parte, el http://, detalla qué protocolo Internet hay que usar. El segmento www.zdnet.com" varia en longitud e identifica el servidor Web con el que hay que contactar. La parte final identifica un directorio especifico en el servidor, y una página inicial, documento, u otro objeto de Internet o de la Intranet.

URL

http://www.zdnet.com/logo/index.html

COMO FUNCIONAN LOS SERVIDORES DE SISTEMAS DE NOMBRES DE DOMINIO EN LAS INTRANETS

- Cuando hay que conectar con un URL particular, la dirección con el URL debe ser igual que la dirección IP verdadera. Tu navegador para Web irá primero a un servidor DNS local en la Intranet de la empresa para obtener esta información si la dirección IP es local, el servidor DNS podrá resolver el URL con la dirección IP. Este enviará la dirección IP auténtica a tu computadora.
- Tu navegador para Web tiene ahora la dirección IP verdadera del lugar que estás intentando localizar. Utiliza esa dirección IP y contacta con el sitio. EL sitio te envía la información que has solicitado.
- Si la información que has solicitado no está en tu Intranet, y si tu servidor DBS local no tiene la dirección IP, el servidor DNS de Intranets debe obtener la información desde un servidor DNS en Internet. EL servidor DNS de Intranets contacta con lo que se denomina servidor de dominio raía, que se mantiene por un grupo llamado InterNiC. EL servidor raíz e dominio l dice al servidor de Intranets qué servidor primario de nombres y qué servidor secundario de nombres tiene la información sobre el URL solicitado.
- El servidor de Intranets contacta ahora con el servidor primario de nombres. Si la información no se puede encontrar en el servidor primario de nombres, el servidor DNS de Intranets contacta con el servidor secundario. Uno de esos servidores de nombres tendrá la información exacta. Después devolverá la información al servidor DNS de Intranets.
- El servidor DNS de Intranets te devuelve la información, tu navegador para Web usa ahora la dirección IP para contactar con el sitio exacto.

Cuando alguien en una Intranet quiere contactar con una localización, por ejemplo, visitar un sitio Web, escribirá una dirección, como www.metahouse.com. Aunque de hecho, Internet no utiliza realmente estas direcciones alfanuméricas. En lugar de eso, emplea direcciones IP, que son direcciones numéricas, en cuatro números de 8 bits separados por puntos, como 123.5.56.255. Un servidor DNS, llamado también un servidor de nombres, empareja, direcciones alfanuméricas con sus direcciones IP, y te permite contactar con la localización exacta.

COMO FUNCIONA JAVA

Al usar Java, los programadores pueden vincular datos corporativos desde una Intranets, permitiendo el uso de sistemas patrimoniales como bases de datos. Los programadores, editores y artistas pueden también utilizar Java para crear programación multimedia. Además Java será capaz de crear programas personalizados de Intranets de todo tipo desde informática para grupos de trabajo a comercio electrónico.

Java es similar al lenguaje informático C++, y está orientado a objeto, l que significa que se pueden crear programas usando muchos componentes preexistentes, en lugar de tener que escribir todo el programa desde el principio. Esto será una gran ayuda para las Intranets, puesto que permitirá a los programadores de la empresa compartir componentes y de ese modo construir aplicaciones personalizadas mucho más aprisa.

Java es un lenguaje compilado, lo que significa que después de que el programa Java se escribe, debe ejecutarse a través de un compilador para transformar el programa en un lenguaje

que pueda entender la computadora. Sin embargo Java se diferencia de otros lenguajes compilados. En otros lenguajes compilados, los compiladores específicos de la computadora crean un código ejecutable distinto para todos los computadores diferentes en los que se puede ejecutar el programa. Por el contrario, en Java se crea una sola versión compilada del programa llamada: código de bytes Java. Los interpretes en los distintos computadores entienden el código de bytes Java y ejecutan el programa. De este modo, un programa Java se puede crear una vez, y usarse después en muchos tipos diferentes de computadora. Los programas Java diseñados para ejecutarse dentro un navegador para Web se denominan apliques. Los apliques son un subconjunto de Java y por razones de seguridad no pueden leer o escribir archivos locales, mientras que Java lo puede hacer. Los navegadores que admiten Java posen interpretes del código de bytes Java.

Después de que un aplique Java está compilado en códigos de bytes, se copia en un servidor Web de Intranets y el enlace necesario se introduce en HTML.

Cuando alguien en una Intranets visita una pagina inicial con un aplique Java en ella, el aplique se recibe automáticamente en su computadora. EL aplique no espera la invitación. Por eso hay tanta preocupación por los virus que se están incrustando en los apliques. Para ejecutar el aplique Java, necesitaras un navegador para Web que tenga un interprete de código de bytes que pueda ejecutar apliques Java.

Puesto que los apliques Java son programas que se pueden ejecutar en tu computadora, teóricamente podrían ser portadores de un virus como cualquier otro programa informático. Para asegurar que ningún virus puede infectar tu computadora cuando recibe un aplique Java, el aplique pasa primero a través de la verificación. Sin embargo, los apliques no se pueden leer o escribir en archivos locales que están normalmente involucrados en ataques víricos, así que esto debería reducir substanciales el riesgo de infección.

Después de que los códigos de bytes se hayan verificado, él interprete Java en el navegador los introduce en una área restringida en la memoria de tu computadora y los ejecuta. Se toman medidas adicionales para que ningún virus pueda perjudicarle.

El aplique Java está ejecutado. Los apliques pueden interrogar a las bases a datos presentando una lista de preguntas o cuestionarios al usuario. Pueden favorecer la búsqueda de sitios en la Intranet creando mecanismos de búsqueda lo más sofisticados posible con HTML. Más importante, puesto que los ciclos CPU del cliente se usan más que los del servidor, todo tipo de multimedia, incluyendo animación e interactividad, es posible con los apliques Java.

Java tendrá Interfaces para Programas de Aplicación (API) y otro tipo de software "enganchado" para permitir a los programadores de Intranets integrar más fácilmente programas de Intranets como los navegadores para Web en bases de datos y redes corporativas existentes.

SUBDIVIDIR UNA INTRANET

Cuando las Intranets sobrepasan un cierto tamaño, o se extienden por varias localizaciones geográficas, empiezan a ser difícil manejarlas como una sola red. Para resolver el problema, la Intranet se puede subdividir en varias sub – redes, subsecciones de una Intranet que las hacen más fáciles de administrar. Para el mundo exterior, la Intranet aparece todavía como su fuera una sola red.

- Si estas construyendo una Intranet y quieres que este conectada con Internet, necesitarías una dirección IP única para tu red, que será manejada por los Servicios Internic de Registro. Puedes disponer de tres clases de redes: Clase A, Clase B o Clase C. Generalmente, la clasificación de Clase A es mejor para las redes más grandes, mientras que la Clase C es mejor para las más pequeñas. Una red de Clase A puede estar compuesta de 127 redes y un total de 16.777.214 nodos en la red. Una red de Clase B puede estar compuesta de 16.383 redes y un total de 65.383 nodos. Una red de Clase C puede estar compuesta de 2.097.151 redes y 254 nodos.
- Cuando se le asigna una dirección a una Intranet, se asigna los dos primeros números IP de la dirección Internet numérica (llamados el campo de la netid) y los

dos números restantes(llamados el campo de la hostid) se dejan en blanco, para que la propia Intranet los pueda asignar, como 147.106.0.0. El campo de la hostid consiste en un número para una sub – red y un número de anfitrión.

- Cuando una Intranet se conecta con Internet, un enrutador realiza el trabajo de enviar los paquetes desde Internet a la Intranet.
- Cuando las Intranets crecen, por ejemplo, si hay un departamento ubicado en otro edificio, ciudad o país, se necesita algún método para manejar el trafico de red. Puede ser poco practico y físicamente imposible encaminar todos los datos necesarios entre muchas computadoras diferentes extendidos por un edificio o por el mundo. Se necesita crear una segunda red denominada sub – red de trabajo o sub – red.
- Para tener un enrutador que dirija todo él trafico de entrada para un Intranet subdividida, se utiliza el primer byte del campo de la hostid. Los bits que se usan para distinguir sub – redes se llaman números de sub – red.
- Cada computadora en cada sub – red recibe su propia dirección IP, como en una Intranet normal. La combinación del campo de la netid el número de sub – red, y finalmente un número de anfitrión, forman la dirección IP.
- El enrutador debe ir informado de que el campo de la hostid en las sub – redes tien que tratarse de modo diferente que los campos del ahostid no subdivididos, si no en así, no podrá encaminar adecuadamente los datos. Para hacer esto, se emplea una mascara de sub – red. Una mascara de Sub – red es un número de 32 bits como 255.255.0.0, que se utiliza conjuntamente con los números en el campo dela hostid. Cuando se efectúa un calculo usando la mascara de sub – red y la dirección IP, el enrutador sabe donde encamina el correo. La mascara de sub – red está incluida en los archivos de configuración de la red de los usuarios.

COMO FUNCIONA LA CONVERSIÓN DE REDES IPX EN UNA INTRANET

La mayoría de las Intranets no están construidas desde cero. Muchas son redes existentes, como Novell NetWare, que tienen que convertirse en una Intranet. A menudo, el primer paso en el movimiento hacia una Intranet puede introducirse en la propia red existente. Depuse, la tecnología de Intranets puede introducirse en la propia red y convertirse en una Intranet.

Cuando una computadora en la red quiere conectar con Internet y solicitar información de ella, se envía una petición a un navegador en la Intranet. Este navegador enviará la petición al destino exacto en Internet. En la red NetWare, el sistema operativo NetWare se utiliza para manejar él trafico de la red y la administración. Como método para encaminar paquetes a través de la red, NetWare emplea al protocolo IPX (Intercambio de Paquetes Internet). Aunque IPX se denomina intercambio de paquetes Internet, no ofrece realmente acceso a Internet o transporta la información de Internet. Las estaciones de trabajo pertenecientes a la red NetWare, y los servidores en la red, necesitan tener cargado IPX en la memoria para usar la red.

Para que las estaciones de trabajo en la red Novell consiga acceder a Internet o a la Intranet, necesitan ejecutar los protocolos TCP/IP que forman la base de Internet. Para hacer eso, debe instalarse una pila TCP/IP en cada computadora que permitirá la entrada a la Intranet. Esto significa que cada computadora tendrá instalado IPX y una pila TCP/IP, para permitir el acceso a Internet y a la red Ethernet. Básicamente, esto da como resultado “RAM de bote en bote” y es uno de los dolores de cabeza más fuertes para cualquiera que intente ejecutar ambas pilas de protocolos. Una unidad de servicio de canal/Unidad de Servicio de Datos (CSU/DSU) realiza la conexión física entre el enrutador de la Intranet y el Proveedor de Servicio Internet (IPS). EL ISP ofrece la autentica conexión Internet y servicios. Varias líneas digitales pueden conectar la CSU/DSU con el ISP, incluyendo una línea alquilada de 56 Kbps, una línea T1 de alta velocidad, o incluso una líneat3 de mayor velocidad. La información solicitada se devuelve a través del CSU/DSU y del enrutador, y después se encamina a la computadora que pidió la información. Si la información está ubicada en una Intranet dentro de la compañía, el enrutador enviará la petición al anfitrión exacto, que después devolverá la información al solicitante. Algunos productos como

NetWare/IP permitirán a las computadoras acceder a servicios de NetWare y a Internet. Esto significa que no tienen que ejecutar los protocolos IPX y TCP/IP, eliminando los problemas de memoria producidos por las múltiples pilas.

SEGURIDAD DE LAS INTRANETS

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 encripción y las contraseñas para convalidar usuarios; y las herramientas del software para evitar y curar de virus, bloquear sitios indeseables, y controlar el tráfico.

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 sub – red 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.

COMO FUNCIONAN LOS 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 enrutadoes pueden tener reglas diferentes para las sub - redes ya que pueden necesitar distintos niveles de seguridad. Una sub – red que contenga información privada financiera o competitiva puede tener muchas restricciones. Una sub – red 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. Cierto 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 él numero 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 bromista 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 bromista 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.

COMO FUNCIONAN LOS 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 trafico 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 especificas 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 sub – red 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 plica 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 sub – red, 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.

COMO FUNCIONAN LOS 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 bastón. 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 especifico 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 Interner 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.

COMO FUNCIONAN LOS 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 especifico de Internet. Así que, por ejemplo, no debería haber ninguna cuenta de usuarios en n 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 sub – red 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.

COMO FUNCIONA LA ENCRIPTACIÓN

Un medio de asegurar una Intranet es usar la encriptación: alterar datos para que sólo alguien con acceso a códigos específicos para descifrar pueda comprender la información. La encriptación se utiliza para almacenar y enviar contraseña para asegurarse de que ningún fisgón pueda entenderla. La encriptación se emplea también cuando se envían datos entre Intranets en Redes Privadas Muy Seguras (VSPN). Además la encriptación se usa para dirigir el comercio en Internet y proteger la información de la tarjeta de crédito durante la transmisión.

Las claves son el centro de la encriptación. Las claves son formulas matemáticas complejas (algoritmos), que se utilizan para cifrar y descifrar mensajes. Si alguien cifra un mensaje sólo otra persona con la clave exacta será capaz de descifrarlo. Hay dos sistemas de claves básicos: criptografía de claves secretas y de claves públicas. Se emplea un algoritmo para realizar una función de rehecho. Este proceso produce un resumen del mensaje único al mensaje. El resumen del mensaje se cifra con la clave privada del emisor que da lugar a una “huella digital”.

El estándar de Encriptación de Datos (DES) es un sistema de claves secretas (simétrico); no hay componente de clave privada. El emisor y el receptor conocen la palabra secreta del

código. Este método no es factible para dirigir negocios por Internet. RSA es un sistema de claves públicas (asimétrico), que utiliza pares de claves para cifrar y descifrar mensajes. Cada persona tiene una clave pública, disponible para cualquiera en un anillo de claves públicas, y una clave privada, guardada sólo en la computadora. Los datos cifrados con la clave privada de alguien sólo pueden descifrarse con su clave pública, y los datos cifrados con su clave pública sólo pueden descifrarse con su clave privada. Por tanto, RSA necesita un intercambio de claves públicas, esto se puede realizar sin necesidad de secretos ya que la clave pública es inútil sin la clave privada.

PGP, Privacidad de las buenas, un programa inventado por Philip Zimmermann, es un método popular empleado para cifrar datos. Utiliza MD5 (resumen del mensaje 5) y los sistemas cifrados de RSA para generar los pares de claves. Es un programa muy extendido que se puede ejecutar en plataformas UNÍX, DOS y Macintosh. Ofrece algunas variaciones de funcionalidad, como la comprensión, que otros sistemas cifrados no brindan. Los pares de claves múltiples se pueden generar y ubicar en anillos de claves públicas y privadas.

COMO FUNCIONAN LAS CONTRASEÑAS Y LOS SISTEMAS DE AUTENTICACION

Una de las primeras líneas de defensa de una Intranet es usar la protección de las contraseñas. Varias técnicas de seguridad, incluyendo la encriptación, ayudan a asegurarse de que las contraseñas se mantienen a salvo. También es necesario exigir que las contraseñas se cambien frecuentemente, que no sean adivinadas fácilmente o palabras comunes del diccionario, y que no se revelen simplemente. La autenticación es el paso adicional para verificar que la persona que ofrece la contraseña es la persona autorizada para hacerlo.

El servidor cifra la contraseña que recibe del usuario, utilizando la misma técnica de encriptación empleada para cifrar la tabla de contraseñas del servidor. Compara la contraseña cifrada del usuario con la contraseña cifrada en la tabla. Si los resultados encajan, el usuario tiene permiso para entrar en el sistema. Si los resultados no encajan, el usuario no tiene permiso.

Las contraseñas de la gente y los nombres de usuario en una Intranet se almacena dentro de un formulario de tablas de un archivo que se encuentra en un servidor que verifica las contraseñas. A menudo, el nombre del archivo es password y el directorio en el que se encuentra es etc. Dependiendo de la técnica de autenticación de contraseñas que se use, el archivo puede estar cifrado o no.

Un método para reconocer a un usuario es a través del Protocolo de Autenticación de Contraseñas (PAP). PAP no asigna la encriptación, pero la tabla de contraseñas en el servidor está normalmente cifrada. Cuando alguien quiere entrar a la red o a un recurso de la red protegido con una contraseña, se le pide el nombre de usuario y la contraseña. El nombre de usuario y la contraseña se envía después al servidor.

El sistema del Protocolo de Autenticación para Cuestionar el Handshake (CHAP) es un sistema de respuesta. El CHAP requiere una tabla de contraseñas no cifrada. Cuando alguien entra en un sistema con CHAP, el servidor genera una clave al azar que se envía al usuario para que cifre su contraseña.

La computadora del usuario emplea esta clave para cifrar su contraseña. Después la contraseña cifrada se devuelve al servidor. El servidor se remite a la tabla de contraseñas para la clave al azar, y cifra la contraseña con la misma clave que se envió al usuario. El servidor compara después la contraseña cifrada con la del usuario con la contraseña cifrada que creó. Si encajan, el usuario tiene permiso de entrada.

La clave de diferencia de CHAP en que el servidor continúa preguntando a la computadora del usuario a lo largo de la sesión. Además, se envía distintas preguntas que deben ser cifradas y devueltas por la computadora, sin intervención humana. De este modo CHAP limita tu ventana de vulnerabilidad. Una sesión no puede piratearse, puesto que el pirata no sería admitido una vez que la computadora no respondiera correctamente a los desafíos que se suceden periódicamente.

Sin importar qué tipo de sistemas de contraseñas se utilice, ni la tabla de contraseñas está cifrada o no, lo importante es proteger la tabla de contraseñas. El archivo debe protegerse contra el acceso FTP y debería haber acceso restringido al archivo para que sólo el administrador o alguien bajo el control del administrador pueda acceder a él.

COMO FUNCIONA EL SOFTWARE PARA EXAMINAR VIRUS EN UNA INTRANET

Los virus son el mayor riesgo en la seguridad de las Intranets. Pueden dañar datos, ocupar y consumir recursos, e interrumpir operaciones. Los archivos de programas eran la principal fuente de problemas en el pasado, pero los nuevos virus de "macro" se pueden esconder en archivos de datos e iniciarse, por ejemplo, cuando se ejecutan una macro en un programa de procesamiento de texto. El software para examinar virus basado en el servidor y el basado en el cliente poseen dispositivos que ayudan a proteger a la Intranet.

Un virus se esconde dentro de un programa. Hasta que ejecutes el programa infectado, el virus permanece inactivo, entonces el virus entra en acción. Algunas veces, lo primero que se hará infectar otros programas del disco duro copiándose de ellos.

Algunos virus colocan mensajes denominados V-marcadores o marcadores de virus dentro de programas que están infectados y ayudan a manejar las actividades víricas. Cada virus tiene un marcador de virus especifico asociado con él. Si un virus se encuentra con uno de estos marcadores en otro programa, sabe que el programa ya está infectado y de ese modo no se reproduce allí. Cuando un virus no encuentra ningún archivo sin marcar en una computadora, eso puede indicar al virus que no hay que infectar más archivos. En este momento, el virus empieza a estropear la computadora y sus datos. Los virus no pueden corromper los archivos de programas o de datos ya que cuando se ejecutan funcionan extrañamente, no funcionan o causan daños. Pueden destruir todos los archivos de tu computadora necesita cuando se conecta y provocar otro tipo de averías.

El software para examinar virus se ejecuta en un servidor dentro del firewall de una Intranet. El software no comprueba la posible existencia de virus en cada paquete que entra en la Intranet, ya que eso sería imposible. En su lugar, sólo comprueba aquellos paquetes enviados con los tipos de servicios y protocolos Internet que indican que un archivo puede encontrarse en el proceso de transferencia desde Internet, comúnmente, e-mail (que se envía mediante SMTP, (Protocolo Simple de Transferencia de Correo), el Protocolo de Transferencia de Archivos (FTP) y la World Wide Web (http; Protocolo Transferencia de Hipertexto). EL software emplea la tecnología de filtrado de paquetes para determinar qué paquetes se están enviando con estos protocolos.

Cuando el software encuentra paquetes que se envían con SMTP, FTP o HTTP, sabe que debe examinarlos más a fondo, para ver si tienen virus. El software para examinar virus funciona de varias maneras. Un método de detección es comprobar archivos para revelar marcadores de virus que indican la presencia de un virus. Los paquetes que no están utilizando SMTP, FTP o http (como TNP) se admiten y el software no realiza ninguna acción en ellos.

Si se encuentra que el archivo está libre de virus, se le permite pasar. Si se encuentra que tiene virus, no se le permitirá entrar en la Intranet.

El software antivirus también debería ejecutarse en computadoras individuales dentro de la Intranet porque es posible que se pueda introducir un virus en la Intranet por disquetes, por ejemplo. Además de la protección contra virus, puede detectar virus y extirpar cualquier virus que encuentre.

BLOQUEAR SITIOS INDESEABLES DESDE UNA INTRANET

El software para el bloqueo de sitios examina el URL de cada petición que sale de la Intranet. Los URL más propensos a no ser aceptados accederán a la Web (http); grupos de noticias (ntp), ftp (ftp); gopher (gopher) y las conversaciones de Internet (irc). EL software toma cada uno de estos cinco tipos de URL y los pone en sus propias "cajas" separadas. El resto de la información de la Intranet que sale tiene permiso para pasar.

Cada URL en cada caja se comprueba en una base de datos de los URL de los sitios censurables. Si el software de bloqueo encuentra que algunos de los URL provienen de sitios desagradables, no permitirá que la información pase a la Intranet. Los productos como SurfWatch como prueban miles de sitios y enumeran varios miles en sus bases de datos que se han encontrado molestos.

El software para bloquear sitios comprueba después el URL con una base de datos de palabras (como "sexo") que puede indicar que el material que se solicita puede ser censurable. Si

el software de bloqueo encuentra un patrón que encaje, no permitirá que la información pase a la Intranet.

El software para bloquear sitios puede entonces emplear un tercer método para comprobar los sitios desagradables; un sistema de clasificación llamado PICS (Plataforma para la Selección de Contenido en Internet). Si el software para el bloqueo de sitios encuentra, basándose en el sistema de clasificación, que el URL es para un sitio que puede contener material censurable, no permitirá el acceso a ese sitio.

Debido a que Internet está creciendo tan deprisa, las bases de datos de sitios censurables podrían llegar a ser anticuados. Para resolver el problema, la base de datos se actualiza cada mes. El software para el bloqueo de sitios conectará automáticamente con un sitio en Internet, y recibirá la base de datos de sitios desagradables más nueva a través de ftp.

Los administradores de Intranets pueden encontrar sitios no enumerados en la base de datos y no filtrados por el software para bloquear sitios que ellos quieren bloquear. Para bloquear manualmente el acceso a esos sitios, pueden añadirlos simplemente a la base de datos.

COMO FUNCIONA EL SOFTWARE DE SUPERVISIÓN DE INTRANETS

El software utiliza filtrado de paquetes, muy parecidos a lo que hacen los enrutadores para filtrar. Ambos observan los datos en la cabecera de cada paquete IP que entra y sale de la Intranet. Sin embargo, se diferencian en que los enrutadores para filtrar deciden si admiten o no a los paquetes. El software de supervisión simplemente deja pasar a los paquetes y sigue la pista a la información de los paquetes además delos datos como la dirección del emisor y destino, el tamaño del paquete, el tipo de servicio de Internet implicado (como la WEB o FTP) y la hora del día en la que se recogen en una base de datos.

Mientras que todos los paquetes deben pasar a través del servidor, el software no introduce necesariamente la información de cada paquete en la base de datos. Por ejemplo, la información acerca de los paquetes http (World Wide Web), los paquetes del protocolo de transferencia de archivos (FTP), los paquetes del protocolo de transferencia de archivos (FTP), los paquetes e-mail (SMTP), los paquetes delos grupos de noticias (TNP) y los paquetes Telnet pueden seguirse, mientras que los paquetes de sonido fluido pueden ignorarse.

El software incluido con el programa del servidor permite a los administradores de redes examinar y analizar el tráfico de la Intranet y de Internet en un grado extraordinario. Puede mostrar la cantidad total del tráfico de la red por día y por horas, por ejemplo, y mostrar a cualquier hora a qué sitios de Internet se estaban transfiriendo. Puede incluso mostrar qué sitios estaban visitando los usuarios individuales en la Intranet, y los sitios más populares visitados en forma gráfica.

Algún software va más allá del análisis y permite a los administradores de Intranets cambiar el tipo de acceso a Internet de los usuarios de la Intranet, basándose en el tráfico, uso y otros factores. El software permitirá también a los administradores de Intranets prohibir que se visiten ciertos sitios de la Intranet.

REDES VIRTUALES SEGURAS

Una Red Privada Virtual Segura (VSPN) o Red Privada Virtual (VPN) permite a los empresarios, siempre y cuando cada uno posea una Intranet, enviarse comunicaciones seguras por Internet y saber que nadie más será capaz de leer los datos. Esencialmente, crea un canal privado y seguro entre sus respectivas Intranets, incluso aunque los datos enviados entre ellas viajen por la Internet publica. Esto significa que las compañías no tienen que alquilar líneas caras entre ellas para mandar datos a través de n enlace seguro. Esta tecnología también se puede emplear para permitir a una compañía enlazar sucursales sin tener que alquilar líneas caras y saber que los datos se pueden leer por la gente de la VSPN.

VISION GLOBAL DE LOS PROGRAMAS PARA TRABAJO EN GRUPO

Una de las razones más importantes por las que las empresas instalan una Intranet es para permitir a sus empleados trabajar mejor juntos. EL tipo de software más potente que deja a la gente trabajar juntas está incluido en el extenso apartado de programas para trabajo en grupo y

admite que los usuarios empleen la conferencia visual, comparta documentos, participen en discusiones y trabajen juntos de otro modo.

COMO FUNCIONAN LAS HERRAMIENTAS DE BÚSQUEDA DE LAS INTRANETS

Las herramientas de búsqueda y de catalogación, como agentes, arañas, tractores y autómatas, algunas veces denominadas motores de búsqueda, se pueden utilizar para ayudar a la gente a encontrar información y se emplean para reunir información acerca de documento disponibles en una Intranet. Estas herramientas de búsqueda son programas que buscan paginas Web, obtienen los enlaces de hipertexto en esas paginas y clasifican la información que encuentran para construir una base de datos. Cada moto de búsqueda tiene su propio conjunto de reglas. Algunos siguen cada enlace en todas las paginas que encuentran, y después en turno examinan cada enlace en cada una de esas paginas iniciales nuevas, etc. Algunos ignoran enlaces que dirigen a archivos gráficos, archivos de sonido y archivos de animación; algunos enlaces a ciertos recursos como las bases de datos WAIS; y a algunos se les dan instrucciones para buscar las páginas iniciales más visitadas.

COMO FUNCIONAN LAS TRANSACIONES FINANCIERAS EN UNA INTRANET

Las Intranet se utilizan no sólo para coordinar negocios y hacerlos más eficaces, sino también como un lugar para hacerlos - recibir y rellenar pedidos de bienes y servicios. Aunque para que esto ocurra, se debe diseñar una manera segura para enviar la información de la tarjeta de crédito por la notoriamente insegura Internet. Hay muchos métodos para hacer esto pero probablemente el que más se utilizará será un estándar llamado: el protocolo para la Transacción Electrónica Segura (SET), que ha sido aprobado por VISA, MasterCard, American Express, Microsoft y Nestcape, entre otras compañías. Es un sistema que permitirá a la gente con tarjetas bancarias hacer negocios seguros por las Intranets.

CONCLUSION

Con la evolución que cada día sufre los sistemas de computación, su fácil manejo e innumerables funciones que nos ofrece, su puede decir que igualmente se ha incrementado el numero de usuarios que trabajan con computadoras, no sin antes destacar él Internet; una vía de comunicación efectiva y eficaz, donde nos une a todos por medio de una computadora.

Utilizando la Red de Area Local en una estructura interna y privada en una organización, seguidamente se construye usando los protocolos TCP/IP. Permite a los usuarios trabajar de una forma sencilla y efectiva, al mismo tiempo brinda seguridad en cuanto a la información ya que esta protegida por firewall: combinaciones de hardware y software que solo permite a ciertas personas acceder a ella para propósitos específicos.

Por otra parte el Intranet nos permite trabajar en grupo en proyectos, compartir información, llevar a cabo conferencias visuales y establecer procedimientos seguros para el trabajo de producción.

La Intranet es una red privada, aquellos usuarios dentro de una empresa que trabajan con Intranet pueden acceder a Internet, pero aquellos en Internet no pueden entrar en la Intranet de dicha empresa. El software que se utilizan en los Intranets es estándar: software de Internet como él Netscape, Navigator y los Navegadores Explorer para Web de Microsoft, facilitan en intercambios de información entre varios departamentos para poder llevar a cabo sus objetivos. Los programas personalizados se construyen frecuentemente usando el lenguaje de programación de Java y el guión de C.P.I. (Interfaz Común de Pasarela) permitiendo hacer negocios en línea, la información enviada a través de una Intranets alcanza su lugar exacto mediante los enrutadores.

Para proteger la información corporativa delicada las barreras de seguridad llamadas firewall (esta tecnología usa una combinación de enrutadores, que permite a los usuarios e Intranet utilizan los recursos de Internet, para evitar que los intrusos se introduzcan en ella).

Construyendo los protocolos TCP/IP (son los que diferencian a la Intranet de cualquier otra red privada) las cuales trabajan juntos para transmitir datos. (TCP: Protocolo de Control de Transmisión y el I.P: Protocolo de Internet), estos protocolos manejan el encadenamiento de los datos y asegura que se envían al destino exacto, funciona conjuntamente y se sitúan uno encima

de otro en lo que se conoce comúnmente Peta de Protocolo, esta formatea los datos que se están enviando para que la pila inferior, la de transporte, los pueda remitir.

Cuando hay una gran cantidad de trafico en una Red de Area Local, los paquetes de datos pueden chocar entre ellos, reduciendo en eficacia de la Red. Por tal motivo se utilizan combinaciones de Hardware y Software denominados Puentes que conectan con enrutadores en un solo producto llamado brouter, que ejecuta la tarea de ambos. Los enrutadores son los que aseguran que todos los datos se envíen donde se supone tienen que ir y de que lo hacen por la ruta más eficaz, desviando él trafico y ofreciendo rutas, cuentan con dos más puertos físicos. Los de recepción (de entrada) y los de envío (de salida), cada puerto es bidireccional y puede recibir o enviar datos.

Saliendo un poco en cuanto a Procesamiento de Datos podemos destacar dentro del Intranet el Uso de Correo Electrónico, utilizando a la vez el Protocolo Simple de Transmisión de Correo (CMTP), emplea una arquitectura cliente / servidor; el receptor del correo puede utilizar ahora un agente usuario de correo para leer el mensaje, archivarlo y responderlo. Frecuentemente el e-mail generado por Intranet no se entregará a una computadora de la Intranet, sino a alguien en Internet, en otra Intranet. EL mensaje deja la Intranet y se envía a un enrutador Internet. EL enrutador examina la diversión, determina donde debería mandarse el mensaje, y después lo pone en camino.

El motivo por el cual una Intranet es porque a Web facilita la publicación de la información y formularios usando el Lenguaje de Hipertexto (HTML), permite tambien la creación de paginas inicales multimedias, que estan compuestas por textos, video, animación, sonido e imagen.

Los programadores pueden vincular datos corporativos desde una Intranet, permitiendo el uso de sistemas patrimoniales como base de datos en el Java, el cual es similar al lenguaje informático C++, es compilado, lo que significa que después de que el programa Java se escribe, debe ejecutarse a través de un compilador para transformar el programa en el lenguaje que pueda entender la computadora.

La Intranet se puede subdividir en varios niveles al momento de sobrepasar su tamaño y al ser difícil de manejar, para resolver el problema se crea subsecciones de una Intranet que las hacen más fáciles de hoslid: los bits que se usan para distinguir sub – redes se llaman números de sub – red.

Al mismo tiempo la Intranet cuenta con firewall que es la combinación de hardware / software que controla el tipo de servidores permitidos hacia o desde la Intranet, esta línea de defensa es por los ataques de aquellas personas que tengan el propósito de destruir o robar datos en una empresa ya que la Internet se expone a este tipo de ataques. Otra manera de emitirlos es usando un enrutador para filtrar, encaminar la dirección IP, y la información de cabecera de cada paquete que entra con la Intranet y solo permite el acceso aquellos paquetes que tengan direcciones u otros datos, que el administrador del sistema ha decidido previamente que puedan acceder a la Intranet.

Seguidamente para asegurar una Intranet se debe usar la encriptación el cual se utiliza para almacenar y enviar contraseñas o códigos específicos para asegurase que ninguna persona pueda entenderla. La clave son el centro de la encriptación. Las contraseñas deben cambiar frecuentemente, que no sean adivinadas fácilmente y tienen que ser elaboradas por personas autorizadas.

Por otra parte tenemos los vienes en la Intranet, son el mayor riesgo en la seguridad, pueden dañar datos, ocupar y consumir recursos e interrumpir operaciones. Estos virus se esconden dentro de un programa, hasta que no se ejecute ese programa el virus es inactivo, al ejecutarse entra en acción infectando en el disco duro copiándose de ellas. El software se ejecuta en un servidor de firewall para examinar al virus, también utiliza filtrado de paquetes, muy parecidos a lo que hacen los enrutadores para filtrar.

El software de supervisión simplemente deja pasar a los paquetes y sigue la pista a la información de los paquetes. Igualmente incluidos con el programa del servidor permite a los administradores de redes examinar y analizar él trafico de la Intranet y de Internet en un grado extraordinario. Algún software va más allá del análisis y permite a los administradores de Intranets

cambiar el tipo de acceso a Internet de los usuarios de la Intranet, basándose en el tráfico, uso y otros factores.

Finalmente podemos decir que las Intranets permiten a los empresarios que a sus empleados trabajen en grupo, tal motivo se debe al extenso aportado de programas para trabajo en grupo y admite que los usuarios empleen la conferencia visual, compartan documentos, participen en discusiones y trabajen juntos de otro modo, no solo para coordinar negocios y hacerlos más eficaces, sino también como un lugar para hacerlo – recibir y rellenar pedidos de bienes y servicios.

BIBLIOGRAFIA

- GRALLA, P.(1996). Como Funcionan las Intranets. (1ra ed.). Maylands: Prentice Hall.
- Desarrollo y Aplicaciones.(1999). Disponible en: http://vobo.com.mx/intranet.html.
- Intranet.(1996).Disponible en: http://www.wntmag.com/atrasados/1996/02_oct96/intranet.html.
- Intranets.(1999). Disponible en: http://www.geocities.com/SiliconValley/2208/Insituacion.html.

Rodrigo Fuentes
rfuentes@mf.gov.ve