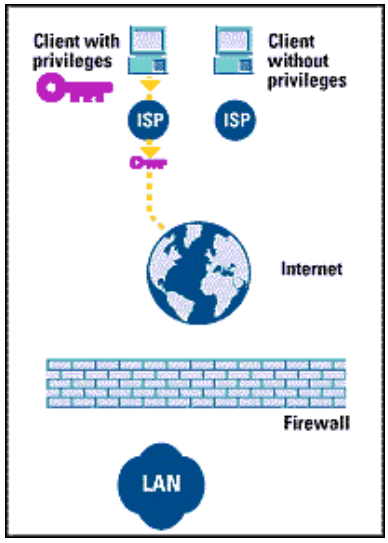
FIREWALL

¿Qué es una red firewall?

Se puede definir de una forma simple una red firewall, como aquel sistema o conjunto combinado de sistemas que crean una barrera segura entre 2 redes. Para ilustrar esta definición podemos observar la figura.



¿Por qué utilizar una red firewall?

El propósito de las redes firewall es mantener a los intrusos fuera del alcance de los trabajos que son propiedad de uno.
Frecuentemente, una red firewall puede actuar como una empresa embajadora de Internet. Muchas empresas usan susistema firewall como un lugar donde poder almacenar información pública acerca de los productos de la empresa, ficheros que pueden ser recuperados por personal de la empresa y otra información de interés para los miembros de la misma. Muchos de estos sistemas han llegado a ser partes importantes de la estructura de servicios de Internet (entre los ejemplos encontrados tenemos: UUnet.uu.net, whitehouse.gov, gatekeeper.dec.com).

¿Contra qué puede proteger una red firewall?

Alguna firewall sólamente permiten tráfico de correo a través de ellas, de modo que protegen de cualquier ataque sobre la red distinto de un servicio de correo electrónico. Otras firewall proporcionan menos restricciones y bloquean servicios que son conocidos por sus constantes problemas de intrusión.
Generalmente, las firewalls están configuradas para proteger contra "logins" interactivos sin autorización expresa, desde cualquier parte del mundo. Esto, ayuda principalmente, a prevenir actos de vandalismos en máquinas y software de nuestra red. Redes firewalls más elaboradas bloquean el tráfico de fuera a dentro, permitiendo a los usuarios del interior, comunicarse libremente con los usuarios del exterior. Las redes firewall, puede protegernos de cualquier tipo de ataque a la red, siempre y cuando se configuren para ello. Las redes

firewall son también un buen sistema de seguridad a la hora de controlar estadísticas de usuarios que intentaron conectarse y no lo consiguieron, tráfico que atraveso la misma, etc... Esto proporciona un sitema muy comodo de auditar la red.

¿Contra qué no puede proteger una red firewall?

Las redes firewall no pueden protegernos de ataques que se producen por cauces distintos de la red firewall instalada. Muchas organizaciones que están aterradas con las conexiones que se puedan producir a través de Internet no tienen coherencia política a la hora de protegerse de invasiones a través de modems con acceso via teléfono. Es estupido poner una puerta de acero de 6 pulgadas de espesor si se vive en una casa de madera, pero por desgracia, algunas empresas se gastan mucho dinero en comprar redes firewall caras, descuidando después las numerosas aberturas por las que se puede colar un intruso (lo que se llaman "back-doors" o "puertas traseras"). Para que una firewall tenga una efectividad completa, debe ser una parte consistente en la arquitectura de seguridad de la empresa. Por ejemplo, una organización que posea datos clasificados o de alto secreto, no necesita una red firewall: En primer lugar, ellos no deberían engacharse a Internet, o los sistemas con los datos realmente secretos deberían ser aislados del resto de la red corportiva.
Otra cosa contra la que las firewalls no pueden luchar, son contra los traidores y estupidos que haya en la propia organización. Es evidente, que de nada sirve que se instale una firewall para proteger nuestra red, si existen personas dentro de la misma que se dedican a traspasar información a través de disquettes (por poner un ejemplo) a empresas espias.

¿Qué ocurre con los virus?

Las redes firewalls no pueden protegernos muy bien contra los virus. Hay demasiados modos de condifcación binaria de ficheros para transmitirlos a través de la red y también son demasiadas las diferentes arquitecturas y virus que intentan introducirse en ellas. En el tema de los virus, la mayor responsaiblidad recae como casi siempre en los usuarios de la red, los cuales deberían tener una gran control sobre los programas que ejecutan y donde se ejecutan.

¿Cuales son algunas de las decisiones básicas al adquirir una red firewall?

Hay una serie de asuntos básicos que hay que tratar en el momento de que una persona toma la responsabilidad (o se la asignan), de diseñar, especificar e implementar o supervisar la instalación de una firewall.
El primero y más importante, es reflejar la política con la que la compañía u organización quiere trabajar con el sistema: ¿Se destina la firewall para denegar todos los servicios excepto aquellos críticos para la misión de conectarse a la red? o ¿Se destina la firewall para porporcionar un método de medición y auditoria de los accesos no autorizados a la red?
El segundo es: ¿Qué nivel de vigilancia, redundancia y control queremos? Hay que establecer una nivel de riesgo aceptable para resolver el primer asunto tratado, para ellos se pueden establecer una lista de comprobración de los que debería ser vigilado, permitido y denegado. En otras palabras, se empieza buscando una serie de objetivos y entonces se combina un análisis de necesidades con una estimación de riesgos para llegar a una lista en la que se especifique los que realmente se puede implementar.
El tercer asunto es financiero. Es importante intentar cuantificar y proponer soluciones en términos de cuanto cuesta comprar o implementar tal cosa o tal otra. Por ejemplo, un producto completo de red firewall puede costar 100.000 dolares. Pero este precio se trata de una firewall de alta resolución final. Si no se busca tanta resolución final, existen otras alternativas mucho más baratas. A veces lo realmente necesario no es gastarse mucho dinero en una firewall muy potente, sino perder tiempo en evaluar las necesidades y encontrar una firewall que se adpate a ellas.

En cuanto al asunto técnico, se debe tomar la decisión de colocar una máquina desprotegida en el exterior de la red para correr servicios proxy tales como telnet, ftp, news, etc.., o bien colocar un router cribador a modo de filtro, que permita comunicaciones con una o más máquinas internas. Hay sus ventajas e incovenientes en ambas opciones, con una máquina proxy se proporciona un gran nivel de auditoria y seguridad en cambio se incrementan los coste de configuración y se decrementa el nivel de servicio que pueden proporcionar.

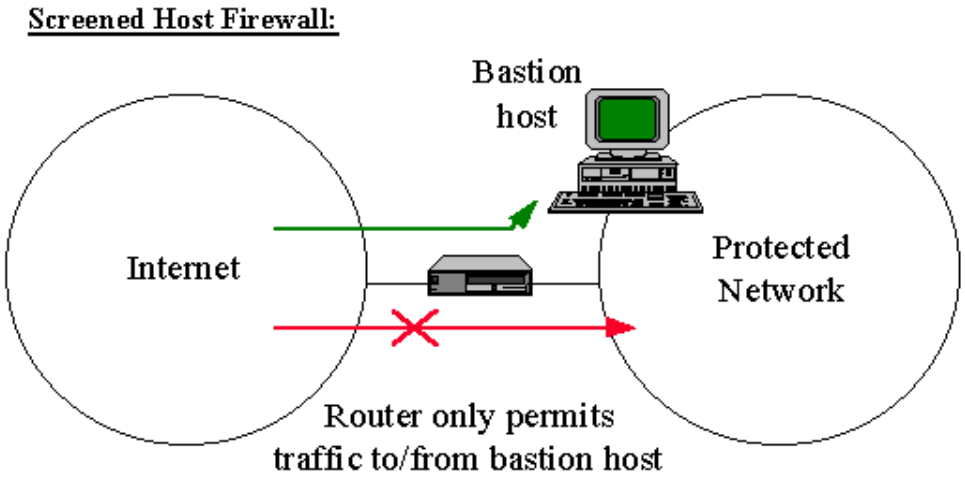
¿Cuales son los tipos básicos de redes firewall?

Conceptualmente, hay dos tipos de firewalls:

- Nivel de red.
- Nivel de aplicación.

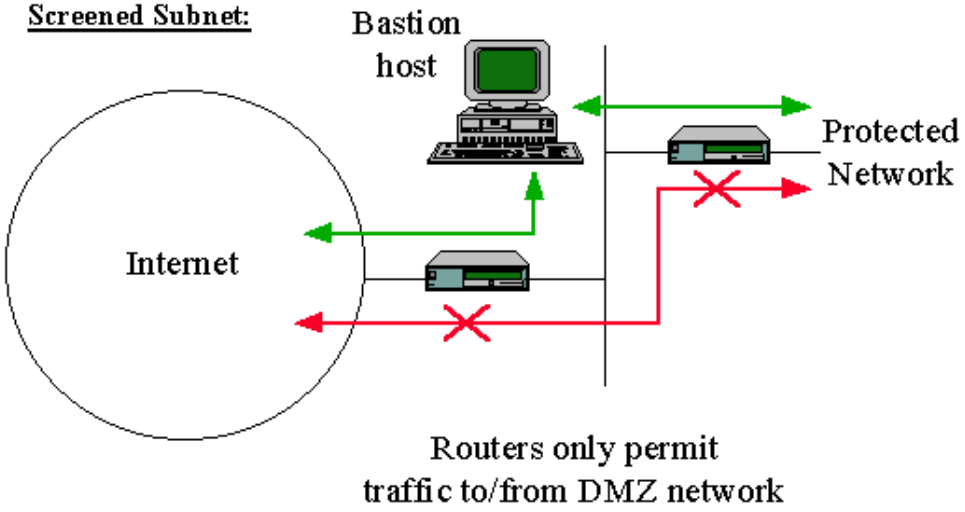
No hay tantas diferencias entre los dos tipos como se podría pensar. Además las últimas tecnologías no aportan claridad para distinguirlas hasta el punto que no está claro cual es mejor y cual es peor. Pero en cualquier caso, se deberá prestar atención y poner mucho cuidado a la hora de instalar la que realmente se necesita en nuestra organización.

Las firewalls a nivel de red generalmente, toman las decisiones basándose en la fuente, dirección de destino y puertos, todo ello en paquetes individuales IP. Un simple router es un "tradicional" firewall a nivel de red, particularmente, desde el momento que no puede tomar decisiones sofisticadas en relación con quién está hablando un paquete ahora o desde donde está llegando en este momento. Las modernas firewall a nivel de red se han sofisticado ampliamente, y ahora mantienen información interna sobre el estado de las conexiones que están pasando a través de ellas, los contenidos de algunos datagramas y más cosas. Un aspecto importante que distingue a las firewall a nivel de red es que ellas enrutan el tráfico directamente a través de ellas, de forma que



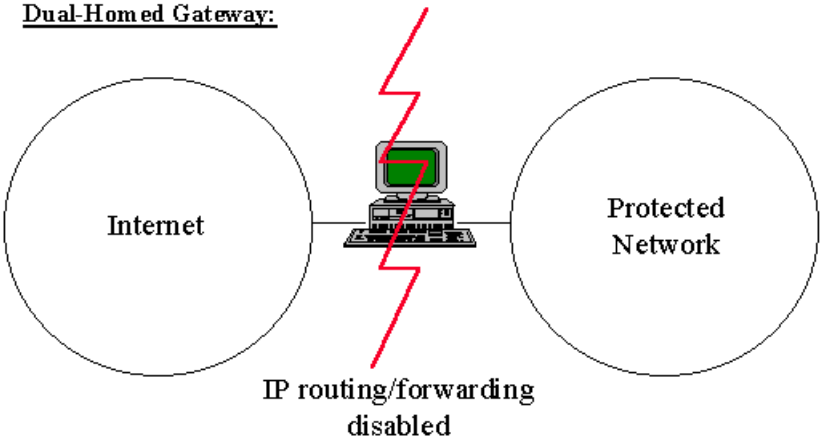
un usuario cualquiera necesita tener un bloque válido de dirección IP asignado. Las firewalls a nivel de red tienden a ser más veloces y más transparentes a los usuarios.

Un ejemplo de una firewall a nivel de red se muestra en la figura anterior. En este ejemplo se representa una firewall a nivel de red llamada "Screend Host Firewall". En dicha firewall, se accede a y desde un único host el cual es controlado por un router operando a nivel de red. El host es como un bastión, dado que está muy defendido y es un punto seguro para refugiarse contra los ataques.



Otros ejemplo sobre una firewall a nivel de red es el mostrado en la figura anterior. En este ejemplo se representa una firewall a nivel de red llamada "screened subnet firewall". En dicha firewall se accede a y desde el conjunto de la red, la cual es controlada por un router operando a nivel de red. Es similar al firewall indicada en el ejemplo anterior salvo que esta si que es una red efectiva de hosts protegidos.

Las Firewalls a nivel de aplicación son generalmente, hosts que corren bajo servidores proxy, que no permiten tráfico directo entre redes y que realizan logines elaborados y auditan el tráfico que pasa a través de ellas. Las



firewall a nivel de aplicación se puede usar como traductoras de direcciones de red, desde que el tráfico entra por un extremo hasta que sale por el otro. Las primeras firewalls a nivel de aplicación eran poco transparentes a los usuarios finales, pero las modernas firewalls a nivel de aplicación son bastante transparentes. Las firewalls a nivel de aplicación, tienden a proporcionar mayor detalle en los informes auditados e implementan modelos de conservación de la seguridad. Esto las hace diferenciarse de las firewalls a nivel de red.

Un ejemplo de una firewall a nivel de aplicación es el mostrado en la figura anterior. En este ejemplo, se representa una firewall a nivel de aplicación llamada "dual homed gateway". Una firewall de este tipo es un host de alta seguridad que corre bajo software proxy. Consta de 2 interfaces de red (uno a cada red) los cuales bloquean todo el tráfico que pasa a traves del host.
El futuro de las firewalls se encuentra a medio camino entre las firewalls a nivel de red y las firewalls a nivel de aplicación. El resultado final de los estudios que se hagan será un sistema rápido de protección de paquetes que conecte y audite datos que pasan a través de el. Cada vez más, las firewalls (tanto a nivel de red como de aplicación), incorporan encriptación de modo que, pueden proteger el tráfico que se produce entre ellas e Internet. Las firewalls con encriptación extremo-a-extremo (end-to-end), se puede usar por organizaciones con múltiples puntos de conexión a Internet , para conseguir utilizar Internet como una "central privada" donde no sea necesario preocuparse de que los datos o contraseñas puedan ser capturadas.

¿Qué son los servidores proxy y como trabajan?

Un servidor proxy (algunas veces se hace referencia a el con el nombre de "gateway" - puerta de comunicación - o "forwarder" - agente de transporte -), es una aplicacion que media en el tráfico que se produce entre una red protegida e Internet. Los proxies se utilizan a menudo, como sustitutorios de routers controladores de tráfico, para prevenir el tráfico que pasa directamente entre las redes. Muchos proxies contienen logines auxiliares y soportan la autentificación de usuarios. Un proxy debe entender el protocolo de la aplicación que está siendo usada, aunque también pueden implementar protocolos específicos de seguridad (por ejemplo: un proxy FTP puede ser configurado para permitir FTP entrante y bloquear FTP saliente).
Los servidores proxy, son aplicaciones específicas. Un conjunto muy conocido de servidores proxy son los TIS Internet Firewall Toolkit "FWTK", que incluyen proxies para Telnet, rlogin, FTP, X-Windows, http/Web, y NNTP/Usenet news. SOCKS es un sistema proxy genéricos que puede ser compilado en una aplicación cliente para hacerla trabajar a través de una firewall.

¿Cómo podemos hacer para que trabajen la Web/http con una firewall?

Hay 3 formas de conseguirlo:

- Permitir establecer conexiones via un router, si se están usando routers protegidos.
- Usar un cliente Web que soporte SOCKS, y correr SOCKS en tu firewall.
- Ejecutar alguna clase de servidor Web proxy en la firewall. El TIS firewall tollkit incluye y proxy llamado http-gw, el cual permite proxy Web, gopher/gopher+ y FTP. Además, muchos clientes Web, tienen servidores proxy construidos directamente en ellos, que soportan: Netspace, Mosaic, Spry, Chamaleon, etc...

¿Cómo podemos hacer para que trabaje FTP a través de una firewall?

Generalemente, se consigue usando un servidor proxy tal como el "firewall toolkit's ftp-gw" o bien realizando alguna de las dos operaciones siguientes:

- Permitiento conexiones entrantes a la red en un rango de puerto restringido.
- Restringiendo las conexiones entrantes usando alguna clase de reglas de protección, preestablecidas.

¿Cómo podemos hacer para que trabaje Telnet a través de una firewall?

Telnet se soporta habitualmente, usando una aplicación proxy tal como "firewall toolkit's tn-gw, o simplemente configurando un router que permita las conexiones salientes usando alguna clase de reglas de protección preestablecidas.

¿Qué ocurre con la denegación del servicio?

La denegación del servicio se produce cuanto alguien decice hacer inútil tu red o firewall por desestabilización, colisión, atasco o colapso en la misma. El problema con la denegación de servicio en Internet es que es imposible prevenirlo. La razón biene, por la distribución natural de la red: cada nodo está conectado via otra red la cual está conectada a otra red, etc... Un administrador de firewall o ISP sólo tiene control sobre unos pocos elementos locales dentro del radio de acción.

Perspectiva de gestión de una firewall.

Nivel de esfuerzo para mantener una firewall típica.
Las típicas firewalls, requieren requieren alrededor de 1 hora a la semana de mantenimiento. Esto es, sin contar el tiempo realitvo a Internet que el administrador de una firewall gastará. La conectividad con Internet trae consigo la necesidad de que alguiente actue como administrador de correo electrónico para Email, Webmaster, gestor de FTP y gestor de noticias USENET. Estas tareas requieren tiempo y pueden llegar a ser un trabajo a tiempo completo para una única persona.
Construirte tu propia firewall.
Hay numerosas herramientas disponibles para construirte tu propia firewall. "Trusted Information Systems", "Inc's Internet Firewall Toolkit", son un ejemplo de implementación de un conjunto de aplicaciones proxies. Si tu estás construyendo tu propio firewall usando un router o una router y su herramienta de desarrollo, tu puedes tener ventajas para la protección del router al construirla. Los libros de Brent Chapman y Elizabeth Zwicky's describen algunos metodos sobre configuración de un router protegido en una firewall. A menos que una persona se ofrezca sin cobrar para construir una firewall, tener contratada a una persona durante una semana en la construcción de una firewall es un conste inutil. Además habría que proporcionar un soporte técnico para el futuro lo cual incrementaría el coste. En años anteriores, había una gran variedad de firewalls comerciales disponibles, y muchas compañías contrataban a consultores para que les construyeran las firewalls. Hoy en dia, no es una buena opción seguir realizando esto, si tenemos en cuenta que el coste de contratar un consultor eventual que nos construya la firewall es superior al de comprar una firewall comercial terminada.
Conocimientos de seguridad
¿Cómo sabemos si una firewall es segura? Es muy dificil saberlo, dado que no hay tests formales que puedan ser facilmente aplicados a algo tán flexible como una firewall. Una moraleja dice que cuanto mayor tráfico de entrada y salida permite una firewall, menor será su resistencia contra los ataques externos. La única firewall que es absolutamente segura es aquella que está apagada.

Si usted está preocupado sobre la calidad de una firewall de un vendedor particular, use el sentido comun y hágale preguntas del tipo siguiente:

- ¿Cuanto tiempo ha estado en los negocios dicho producto?
- El tamaño de la instalación base.
- ¿Han tenido expertos indepedientes revisando el diseño y la implementación de la aplicación en cuestión?

Un vendedor debería claramente explicarle como se diseñó la firewall en concepto de seguridad. No acepte isinuaciones acerca de que los productos de la competencia son inseguros sin habernos explicado la seguridad de producto en cuestión.

Una pregunta tópica: ¿Más caro equivale a más seguro?

Un error común en las firewalls es pensar que pagando más en una firewall cara se consigue más seguridad en la misma. Hay que pensar que si el coste de una firewall es 2 veces superior al de otra, el vendedor tendría que ser capaz de explicarnos por qué dichos producto es 2 veces mejor que el otro.

¿Cómo es una típica instalación de firewall?

La mayoría de la firewalls solía ser verndida como paquetes de consulta. Cuando una firewall erá vendida, parte de su coste se destinaba a instalación y soporte, generalmente, involucrando a un consultor que proporcionaba el vendedor, para ayudar en la instalación. En los "malos días" muchas de las empresas que estabán conectadas a Internet, no tenían expertos en TCP/IP local, de modo que los instaladores de las firewalls, a menudo tenían que dedicar tiempo a configurar los routers y correo electrónico (tareas que deberían haber sido realizadas por el administrador interno de DNS). Algunos vendedores continuan porporcionando tal nivel de servicios mientras que otros, simplemente proporcionan servicio sobre la instalación de su producto.

Tipicamente, cuando se instala una firewall, la conexión a Internet debe estar realizada, pero no tiene que estar conectada a la red protegida. El instalador de la firewall, llega, testea las funciones básicas de la máquina y entonces puede dirigir una reunón en la que se detallen los pasos a seguir en la configuración de la firewall:

- Cual será la política de acceso que se va a poner en práctica.
- A donde se va a dirigir el correo electrónico.
- Dónde se debería buscar la información de login.
- Y otras temas...

Una vez que el instalador tiene una buena base para la configuración de la firewall, entonces se conecta a Internet y testea que las operaciones con la red sean correctas. En ese momento se instalan y chequean las reglas para el control de acceso a la firewall y se conectan a la red protegida. Además de realizan, generalmente, algunas operaciones típicas como acceso a Web, recepción y envío de correo electrónico, etc.. Cuando todos los controles son correcto entonces ya se puede decir que uno está en Internet.

¿Qué vendedores proporcionan servicio de firewall?

Muchos vendedores, proporcionan alguna clase de soporte periódico para preguntas básicas relacionadas con las firewalls. Algunos vendedores incluso proporcionan servicio a distintancia mediante la utilización del correo electrónico.

Algunas proveedores de servicios Internet ofrecen un soporte de firewall como parte del servicio de conexión a Internet. Para organizaciones que son novatas en el uso de TCP/IP o que tienen prisa, es una opción atractiva, dado que un mismo vendedor proporcionar soporte de red, de alquiler de linea y de firewall.

Una cosa importante que proporciona un vendedor con respecto a las firewalls, es un entendimiento de como hacer una política sensata de seguridad. A menos que se sea un vendadero entendido en la materia es mejor dejarse aconsejar antes de lanzarse a la aventura. Cuando un vendedor proporcione soporte de firewall, esté podrá guiarnos a través de la configuración de la firewall para que evitemos ataques externos.

¿Qué vendedores no proporcionan servicio de firewall?

Los vendedores, tipicamente, no configuran sistemas de herencia interna para trabajar con la firewall. Por ejemplo, muchas firewalls asumen que hay que hablar a Internet por un lado y a la red TCP/IP por el otro. Generalmente, es reponsabilidad del cliente, tener sistemas TCP/IP aptos para interactuar con firewall. Para Email, la mayoría de las firewalls soportan sólamente SMTP(Simple Mail Transfer Protocol) y es reponsabilidad del cliente tener un simple compatible con SMTP en algún lugar de la red. A menos que se esté comprando una firewall desde un proveedor de servicios Internet, es responsabilidad del cliente tener una clase de direcciónes de red C IP y un nombre de dominio localizado.

¿Qué preguntas han de realizarse a un vendedor de firewall?

Algunas de las preguntas que se le pueden hacer a un comprador son las siguientes:

Seguridad:

- ¿Cuales son los principales diseños de seguridad de tu firewall?
- ¿Por qué piensas que es segura?
- ¿A qué clase de revisiones y pruebas a sido sometida?

Credenciales corporativas:

- ¿Durante cuanto tiempo ha vendido esta firewall.?
- ¿Qué tamaño ocupa la instalación básica?
- ¿Tiene libro de reclamaciones que podamos consultar?

Soporte e ingeniería:

- ¿Cuantos ingenieros de soporte tienes, con contrato indefinido?
- ¿Durante cuantas horas permanece operativo el servicio de soporte?
- ¿Cuanto cuesta el soporte y mantenimiento técnico?
- ¿Cuál es tu política de actualizaciones?
- ¿Incluye el producto, algun tipo de garantía de hardware o software?

Documentación:

- Solicite una copia de la documentación para revisarla.
- ¿Que clases de informe de auditoria general una firewall? Solicita una copia de todos los informes que genere, para revisarlos.

Funcionamiento:

- ¿La firewall incluye hardware o sólo software?
- ¿Qué clase de interfaces de red soforta la firewall? (¿Necesitaré token ring, routers ethernet, etc...?)
- ¿Es manejable la firewall desde un puesto remoto? ¿Cómo es la seguridad que gestiona la firewall al respecto?

Glosario de términos relacionados con firewall.

Abuso de privilegio:

Cuando un usuario realiza una acción que no tiene asignada de acuerdo a la política organizativa o a la ley.

Ataque interior:

Un atáque originado desde dentro de la red protegida.

Autentificación:

El proceso para determinar la identidad de un usuario que está intentando acceder a un sistema.

Autorización:

Proceso destinado a determinar que tipos de actividades se permiten. Normalmente, la autorización, está en el contexto de la autentificación: una vez autentificado el usuario en cuestión, se les puede autorizar realizar diferentes tipos de acceso o actividades.

Bastion Host:

Un sistema que ha sido configurado para resistir los ataques y que se encuentra instalado en una red en la que se prevee que habrá ataques. Frecuentemente, los Bastion hosts son componentes de las firewalls, o pueden ser servidores Web "exteriores" o sistemas de acceso público. Normalmente, un bastion hosts está ejecutanto alguna aplicación o sistema operativo de propósito general (por ejemplo: UNIX, VMS, WNT, etc...) más que un sistema operativo de firewall.

Detección de intrusión:

Detección de rupturás o intentos de rupturas bien sea manual o vía sistemas expertos de software que atentan contra las actividades que se producen en la red o contra la información disponible en la misma.

Dual Homed Gateway:

Un "Dual Homed Gateway" es un sistema que tiene 2 o más interfaces de red, cada uno de los cuales está conectado a una red diferente. En las configuraciones firewall, un "dual homed gateway" actua generalmente, como bloqueo o filtrador de parte o del total del tráfico que intenta pasar entre las redes.

Firewall:

Un sistema o combinación de sistemas que implementan una frontera entre 2 o más redes.

Firewall a nivel de aplicación:

Un sistema firewall en el que el servicio se proporciona por procesos que mantienen estados de conexión completos con TCP y secuenciamiento. Las firewalls a nivel de aplicación, a menudo redirigen el tráfico, de modo que el tráfico saliente, es como si se hubiera originado desde la firewall y no desde el host interno.

Firewall a nivel de red:

Una firewall en la que el tráfico es exáminado a nivel de paquete, en el protocolo de red.

Host-based Security:

La técnica para asegurar de los ataques, a un sistema individual.

Logging:

El proceso de almacenamiento de información sobre eventos que ocurren en la firewall o en la red.

Perimeter-based Security:

La técnica de securización de una red, para controlar los accesos a todos los puntos de entrada y salida de la red.

Política:

Reglas de gobierno a nivel empresarial/organizativo que afectan a los recursos informáticos, prácticas de seguridad y procedimientos operativos.

Proxy:

Un agente software que actua en beneficio de un usuario. Los proxies típicos, aceptan una conexión de un usuario, toman una decisión al respecto de si el usuario o cliente IP es o no un usuario del proxy, quizas realicen procesos de autentificación adicionales y entonces completan una conexión entre el usuario y el destino remoto.

Router - Encaminador -:

Dispositivo destinado a conectar 2 o más redes de area local y que se utiliza para encaminar la información que atraviesa dicho dispositivo.

Screened Host:

Un host - ordenador servidor - en una red, detrás de un router protegido. El grado en que el host puede ser accesible depende de las reglas de protección del router.

Screened Subnet:

Una subred, detrás de un router protegido. El grado en que la subred puede ser accesible depende de las reglas de protección del router.

Tunneling Router:

Un router o sistema capaz de dirigir el tráfico, encriptándolo y encapsulándolo para transmitirlo a traves de una red y que también es capaz de desencaptular y descifrar lo encriptado.

Bibliografía de interés, acerca de firewall.

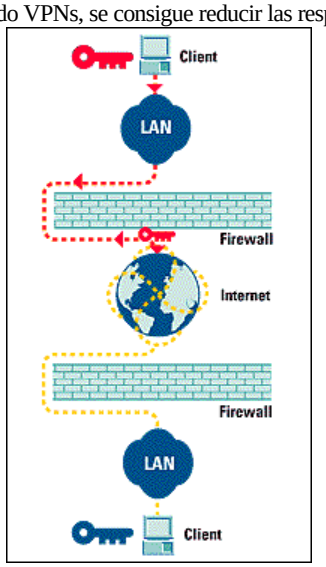
En cuanto a la bibliografía que recomendamos acerca de firewall, existen 2 ligros interesantes, pero que se encuentran en ingles, son los siguientes:

- *"Firewalls and Internet Security: pursuing the wily hacker"* por Bill Cheswick y Steve Bellovin, editado por Addison-Wesley.
- *"Building Internet Firewalls"* por Brent Chapman y Elizabeth Zwicky, editado por O'Rielly and Associates.

REDES PRIVADAS VIRTUALES

¿Qué es una Red Privada Virtual (VPN)?

Las redes privadas virtuales crean un tunel o conducto dedicado de un sitio a otro. Las firewalls o ambos sitios permiten una conexión segura a través de Internet. Las VPNs son una alternativa de coste util, para usar lineas alquiladas que conecten sucursales o para hacer negocios con clientes habituales. Los datos se encriptan y se envian a través de la conexión, protegiendo la información y el password.
La tecnología de VPN proporciona un medio para usar el canal público de Internet como una canal apropiado para comunicar los datos privados. Con la tecnología de encriptación y encapsulamiento, una VPN básica, crea un pasillo privada a trabés de Internet. Instalando VPNs, se consigue reducir las responsabilidades de gestión de



un red local.

¿Cómo trabaja la tecnología de túneles de una Red Privada Virtual?

Las redes privadas virtuales pueden ser relativamente nuevas, pero la tecnología de tuneles está basada en standares preestablecidos. La tecnología de tuneles -Tunneling- es un modo de transferir datos entre 2 redes similares sobre una red intermedia. También se llama "encapsulación", a la tecnología de tuneles que encierra un tipo de paquete de datos dentro del paquete de otro protocolo, que en este caso sería TCP/IP. La tecnología de tuneles VPN, añade otra dimensión al proceso de tuneles antes nombrado -encapsulación-, ya que los paquetes están encriptados de forma de los datos son ilegibles para los extraños. Los paquetes encapsulados viajan a través de Internet hasta que alcanzan su destino, entonces, los paquetes se separan y vuelven a su formato original. La tecnología de autentificación se emplea para asegurar que el cliente tiene autorización para contactar con el servidor.
Los proveedores de varias firewall incluyen redes privadas virtuales como una característica segura en sus productos.

Redes privadas virtuales dinámicas - Dynamic Virtual Private Networks (DVPN) - Enfoque realizado usando aplicaciones de TradeWade Company.

Basadas en la tecnología de Internet, las intranets, han llegado a ser una parte esencial de los sistema de información corporativos de hoy en dia. Sin embargo, Internet no fue diseñada, originalmente, para el ámbito de los negocios. Carece de la tecnología necesaria para la seguridad en las transacciones y comunicaciones que se producen en los negocios. Se presenta pues, un tema peliagudo en los negocios: ¿Cómo establecer y mantener la confianza en un entorno el cual fue diseñado desde el comienzo, para permitir un acceso libre a la información? Para decirlo de otro modo: ¿Cómo conseguir seguridad en una intranet sin chocar con los principios básicos de Internet sobre la flexibilidad, interoperatibilidad y facilidad de uso?
La compañia TradeWade cree que la respuesta apropiada y satisfactoria a esta disyuntiva, se encuentra en la utilización de VPNs dinámicas basadas en los servicios y aplicaciones TradeVPI de dicha compañía. A diferencia de una VPN tradicional que ofrece seguridad limitida e inflexible, una VPN dinámica proporciona ambos extremos, con altos niveles de seguridad, e igualmente importante es que proporciona la flexibilidad necesaria para acoplarse dinámicamente a la información que necesitan los distintos grupos de usuarios. Las VPNs dinámicas, pueden ofrecer esta flexibilidad ya que están básadas en una única arquitectura así como pueden proporcionar otras ventajas. Una VPN dinámica es una habilitadora de intranet. Habilita que una intranet ofrezca más recursos y servicios que de otra forma imposibilitaria al mundo de los negocios a hacer mayor uso de los recursos de información.

Potencial de una Red Privada Virutal Dinámica.

TradeVPI es un conjunto de aplicaciones y servicios relacionados. El potencial de esta solución es el siguiente:

- Proporciona una seguridad importante para la empresa.
- Se ajusta dinámicamente al colectivo dispar de usuarios.
- Permite la posibilidad de intercambio de información en diversos formatos (páginas Web, ficheros, etc.).
- El ajuste que hace para cada usuario lo consigue gracias a los diferentes browsers, aplicaciones, sistemas operativos, etc...
- Permite a los usuarios unirse a distintos grupos, así como a los administradores pueden asigar identidades en un entorno simple pero controlado.
- Mantiene la integridad total, independientemente del volumen administrativo, cambios en la tecnología o complejidad del sistema de información corporativo.

TradeVPI posibilita el uso de Intranet en los negocios.

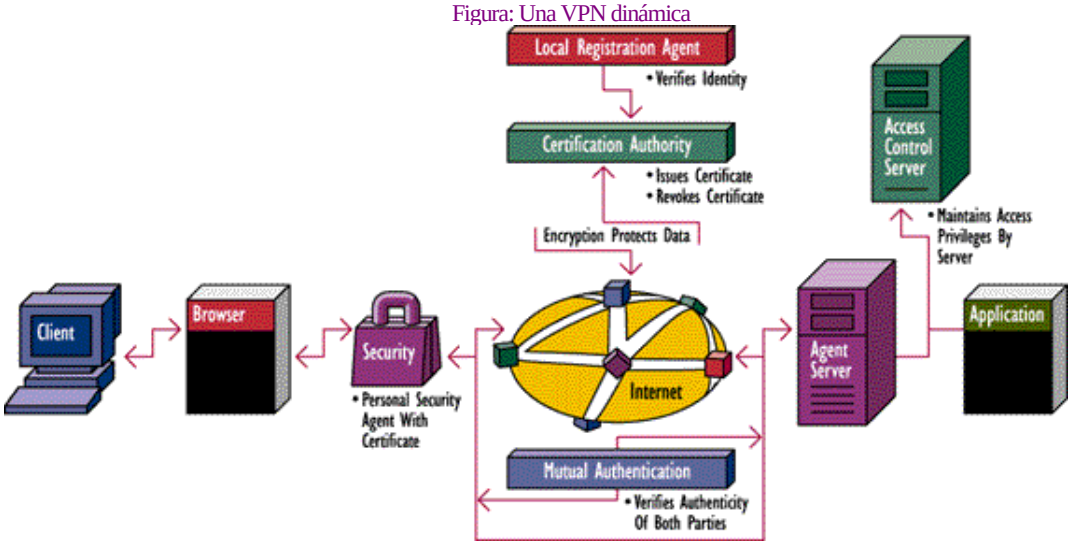
Una VPN dinámica basada en TradeVPI, ofrece a los negocios, la posiblidad de usar intranets y tecnología Internet, con la certeza de que las comunicaciones y transacciones estarán protegidas con la más alta tecnología en seguridad.
Al mismo tiempo, una VPN dinámica, permite que los negocios extiendan sus comunicaciones, y que el acceso a la información se produzca en un entorno agradable, versatil y controlado. En vez de estar diseñando engorrosas pantallas de usuario con las consabidas limitaciones y con esquemas de seguridad inflexibles, una VPN dinámica ha sido diseñada para proporciona el más alto nivel de libertad dentro de un entorno seguro, consiguiendo que el mayor número de usuarios pueda realizar gran su trábajo con la mayor cantidad de información posible .

¿Cómo trabajan las Redes privadas virtuales dinámicas?. Enfoque realizado usando aplicaciones de TradeWade Company.

La VPN dinámica de TradeWave consta de una plataforma de seguridad de red y un conjunto de aplicaciones para usar en la plataforma de seguridad. El diagrama de abajo, muestra como se engranan las piezas de esta plataforma para conseguir una solución del tipo VPN dinámica.

El siguiente ejemplo va pasando a través de las parte de una VPN dinámica suponiendo una comunicación segura HTTP (Web). Sin embargo, TradeVPI no es una aplicación específica, sino que puede trabajar con otras aplicaciones Internet, así como con aplicaciones corporativas específicas.

Figura: Una VPN dinámica



Fusionar la VPN.

Anteriormente, al usar una VPN, un usuario o servicio en primer lugar, debe fusionar (join) la VPN, registrandola con el certificado de autenticidad (CA). Un empleado corporativo confiada, llamaba a un agente del Registro Local, el cual confirmaba todos los requisitos del registro. Los fuertes procesos de seguridad, aseguraba que sólamente los usuarios nominados, estaban registrados y recibían la certificación. La CA, aseguraba que los certificados revocados eran enviados por correo y se denegaba el servicio cuando se intentaban usar.

Usando VPN de TradeWave.

Los usuarios y servicios, reciben continuamente, información dentro de la VPN. Sin embargo, los pasos básicos de cada intercambio son los mismos. Siguiendo los pasos ilustrados en la figura, un usuario realiza una petición de información a un servidor, pulsando con su ratón en un hipervínculo. Los pasos seguidos se pueden describir en los siguientes puntos:

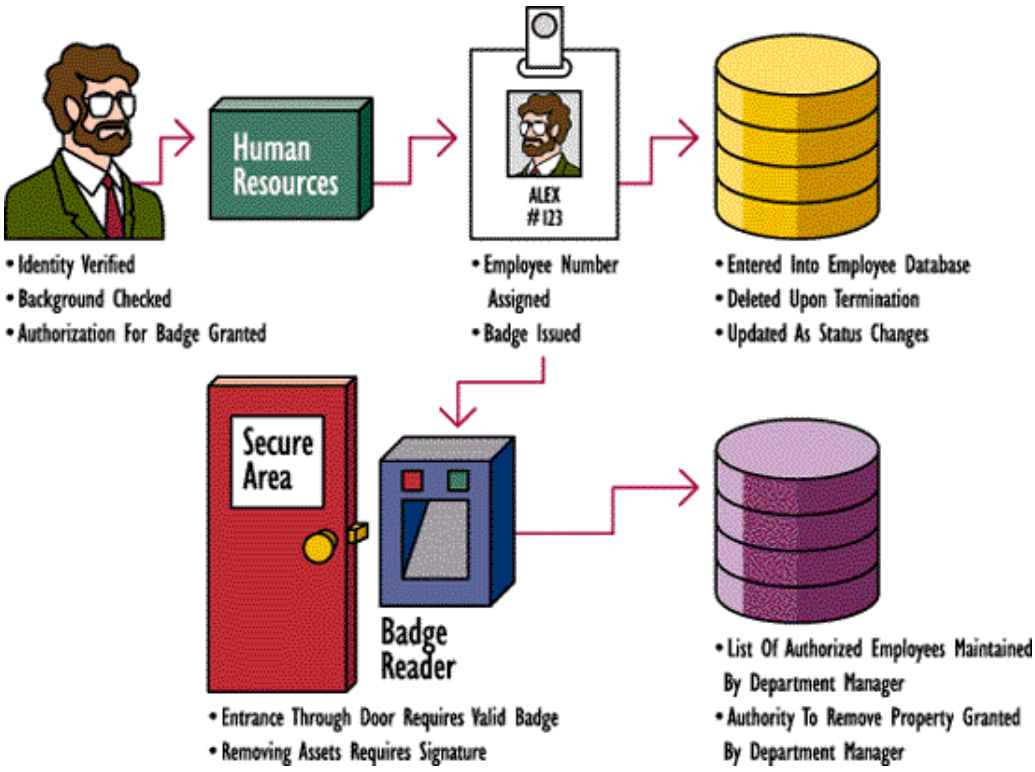
1. ***Un usuario solicita información usando una aplicación tal como un browser Internet, desde un ordenador de sobremesa.*** El intercambio de información comienza cuando un usuario envia información a otro usuario o solicita información al servidor. La VPN, puede incorporar aplicaciones propietarias. Sin embargo, también debe ofrecer aplicaciones que se beneficien de Internet, y particularmente, de la WWW. En el supuesto de que un usuario ha accedido a un hipervínculo desde dentro de algun documento Web, dicho hipervínculo es seguro y sólamente puede ser accedido por usuarios autorizados.
2. ***La aplicación envía y asegura el mensaje.*** Cuando un cliente y un servidor detectan que se necesita seguridad para transmitir la petición y para ver el nuevo documento, ellos se interconectan en un mutuo protocolo de autentificación. Este paso verifica la identidad de ambas parten, antes de llevar a cabo cualquier acción. Una vez se produce la autentificación, pero ántes de que la aplicación envie la petición, se asegura el mensaje encriptándolo. Adicionalmente, se puede atribuir un certificado o firma electrónica al usuario. Encriptando la información, se protege la confidencialidad y la integridad. Si se envía la firma, se podrá usar para auditorias. Para habilitar la interoperatividad entre múltiples mecanismos de seguridad, las funciones de seguridad se deben basar en standares bien definidos, tal como el standard de Internet GSSAPI (Generic Security Services Application Programming Interface).
3. ***El mensaje se transmite a través de Internet.*** Para que la p etición alcance el servidor, debe dejar la LAN y viajar a través de Internet, lo cual le permitirá alcanzar el servidor en algún punto de la misma.

Durante este viaje, puede darse el caso de que atraviese 1 o más firewalls ántes de alcanzar su objetivo. Una vez atravesada la firewall, la petición circula a lo largo del pasillo Internet hasta alcanzar el destino.

4. ***El mensaje recibido debe pasar controles de seguridad.*** Cuando el mensaje alcanza su destino, puede ser que tenga que atravesar otra firewall. Estafirewall protegerá cuidadosamente el tráfico entrante asegurando que se ciñe a la política corporativa, antes de dejarlo atravesar la red interna. El mensaje se transfiere al servidor. Como consecuencia de la autentifiación mutua que se produjo entre el cliente y el servidor, el servidor conoce la identidad del usuario cliente cuando recibe la petición.
5. ***Durante la petición, se verifican los derechos de acceso de los usuarios.*** Al igual que en todas las redes corporativas, todos los usuarios no pueden acceder a la totalidad de la información corporativa. En una VPN dinámica, el sistema debe poder restringir que usuarios pueden y no pueden acceder a la misma. El servidor debe determinar si el usuario tiene derechos para realizar la petición de información. Esto lo hace, usando un mecanismos de control , preferiblemente un servidor separado. El servidor de control de acceso, restringe el acceso a la información en niveles de documento. De modo que, si incluso un usuario presenta un certificado válido, puede ser que se le deniege el acceso basándose en otros criterios (por ejemplo: políticas de información corporativa).
6. ***La petición de información es devuelta por Internet, previamente asegurada.*** Si el usuario tiene derechos de acceso a la petición de información, el servidor de información encripta la misma y opcionalmente la certifica. Las claves establecidas durante los pasos de autentificación mútua se usan para encriptar y desencriptar el mensaje. Ahora, un usuario tiene su documento asegurado.

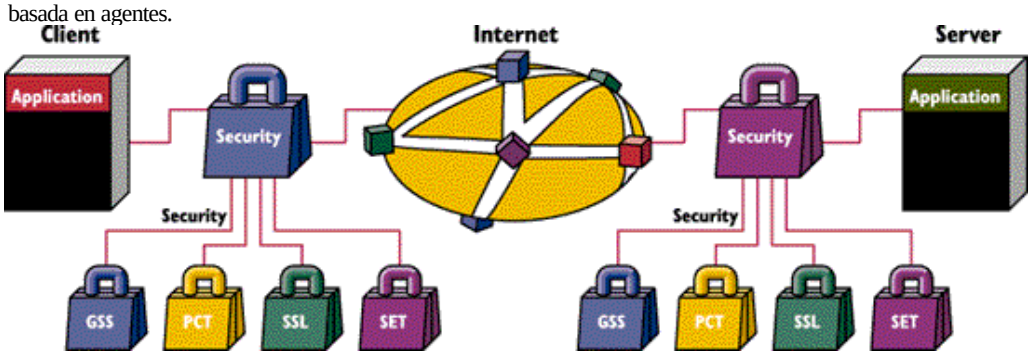
Una equivalencia a las VPN dinámicas: Una identificación de empleado y un sistema de identificación.

Para entender la solución propuesta por TradeWave para las VPN podemos considerar un equivalente consistente en una identificación de empleado corporativo y un sistema de identificación. Del mismo modo que los departamentos de Recursos Humanos o Seguridad pueden verificar la identidad de un empleado y asignar un número de empleado único, una VPN verifica la identidad del usuario y emite un único "nombre distintivo" el cual se usa para todos los accesos y movimientos dentro del sistema. Del mismo modo que una compañía también lleva el control de quienes tienen una clave de seguridad y donde pueden ir con ella, las VPN tienen controlada la gestión y ponen a disposición claves y certificados. Al igual que muchas tarjetas de seguridad pueden ser reutilizadas por una compañía, muchas claves se pueden reconvertir, mediante el Certificado de Autorización.
Además, del mismo modo que los accesos a construcciones y areas de seguridad, se controlan por varios niveles de seguridad, las VPN validan las Listas de Control de Acceso contra los nombre de usuario y passwords, para autorizar el acceso a redes y a ciertos documentos y ficheros. Por último, las VPN mantienen una lista de usuarios revocados y deniegan los futuros accesos al sistema a dichos usuarios, al igual que se produce en una empresa cuando un usuario se marcha debe devolver todos los sistemas de identificación de seguridad para no poder volver a entrar en la compañía. La siguiente figura muestra la equivalente constatada en este párrafo.



Extensibilidad y Arquitectura basada en agentes de TradeVPI.

Un aspecto crítico en las VPN de TradeWave es su arquitectura basada en agentes. Los agentes TradeWave son módulos o entidades software que se comunican via protocolos standard. Como consecuencia de ello, TradeWave ha "desacoplado" arquitectónicamente sus agentes de otras aplicaciones, de forma que un negocio puede cambiar o expandir su intranet - incluyendo expansión de plataformas - sin tener que rediseñar su sistema intranet. Más especificamente, esta arquitectura permite que un negocio seleccione y use cualquier browser, cualquier servidor y cualquier aplicación con su VPN dinámica. La siguiente figura muestra la arquitectura basada en agentes.



Los agentes TradeWave puden:

- Ser insertados facilmente, en streams de comunicaciones existentes con un mínimo de alteración en el sistema.

- Contener habilidades que no poseen el sistema existente.
- Ser actualizados rápidamente.
- Incorporar múltiples protocolos de seguridad.

Además, la arquitectura basada en agentes, proporciona una solución la problema tradicional en los sistemas de información corporativos: el conflicto entre los stándares de empresa por un lado y la adopción local de tecnologías para necesidades específicas en el otro. Una arquitectura basada en agentes permite, por ejemplo, departamentos que usen los browsers que ellos quieran sin perturbar los stándares de seguridad empresaria.

TradeAttachés.

Un beneficio adicional a la arquitectura basada en agentes es la posibilidad de usar una variedad de módulos software llamados TradeAttachés. Estos módulos se pueden añadir al sistema TradeVPI para incrementar su funcionalidad e interoperatibilidad. Por ejemplo, TradeAttachés permite que la VPN se puede extender para incluir diferentes protocolos de seguridad sin perturbar a los browsers o servidores.
Con este sistema, están inmediatamente disponibles, las nuevas funciones de seguridad. TradeVPI también puede gestionar simultáneamente, varios TradeAttachés de seguridad, de modo que la VPN puede soportar múltiples plataformas de seguridad al mismo tiempo.

ACCESO REMOTO SEGURO

¿Cuál es el propósito de los accesos remotos seguros?

Con los accesos remotos seguros, las conexiones via modem telefónico pueden transferir datos seguros via un proveedor de servicios Internet o via una red corporativa. Los datos se encriptan en el cliente antes de que sean transmitidos y se desencriptan en la puerta de la firewall. El software proporcionado, habilita a los usuarios remotos a que se pueden conectar a la red corporativa como si ellos estuvieran detrás de la firewall.
La tecnología de VPN proporciona un medio para usar el canal público de Internet como una canal apropiado para comunicar los datos privados. Con la tecnología de encriptación y encapsulamiento, una VPN básica, crea un pasillo privada a trabés de Internet. Instalando VPNs, se consigue reducir las responsabilidades de gestión de un red local.

¿Qué es una red segura, privada y virtual?

Una red privada virtual es una red donde todos los usuarios parecen estar en el mismo segmento de LAN, pero en realidad están a varias redes (generalmente públicas) de distancia. Esto se muestra en la Figura 1. Para lograr esta funcionalidad, la tecnología de redes seguras, privadas y virtuales debe completar tres tareas. Primero, deben poder pasar paquetes IP a través de un túnel en la red pública, de manera que dos segmentos de LAN remotos no parezcan estar separados por una red pública. Segundo, la solución debe agregar encripción, tal que el tráfico que cruce por la red pública no pueda ser espiado, interceptado, leído o modificado. Finalmente, la solución tiene que ser capaz de autenticar positivamente cualquier extremo del enlace de comunicación de manera que un adversario no pueda acceder a los recursos del sistema.

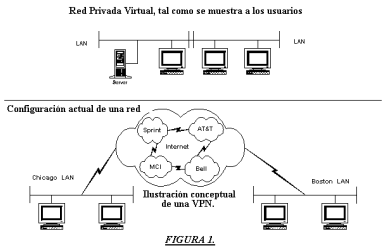


FIGURA 1.

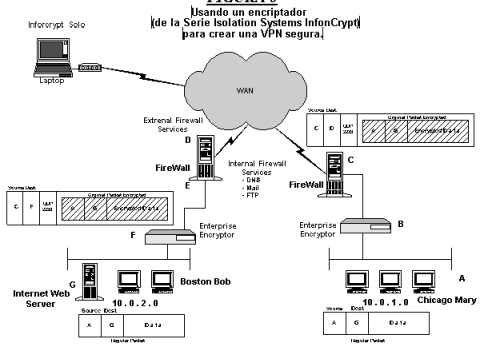
¿Cómo se consigue una red privada segura a través de un paquete de software como la "Serie InfoCrypt de Isolation Systems"?

La Serie InfoCrypt de Isolation Systems crea una red privada segura de la siguiente manera. Primero, los paquetes IP que tienen como destino una zona protegida son encapsulados en un nuevo paquete que contiene sólo las direcciones IP de los encriptores origen y destino. Esto le permite a los clientes conectar redes IP sin routear a redes IP routeadas, creando un túnel efectivo a través de la red pública por donde pasar los paquetes. La encripción es lograda usando Triple Pass DES con llaves de doble o triple longitud para encriptar paquetes destinados a redes remotas. Como la encripción es una función matemática que requiere significativos recursos del sistema, los InfoCrypt Enterprise Encrytors de Isolation Systems incorporan un procesador ASIC (Application Specific Integrated Circuit) dedicado exclusivamente a los procesos de encripción y desencripción. Esto provee a los clientes con una performance de red en tiempo de real. Los productos InfoCrypt de Isolation Systems, encriptan el paquete entero, incluyendo el encabezado original, antes de encapsular la información en un nuevo paquete. Además de proteger los datos que se están transmitiendo, esto esconde completamente la topología interna de las dos redes remot as y también protege otra información de encabezado valiosa, tal como el tipo de tráfico (por ejemplo, Mail, tráfico de Web, FTP, etc.), de los ojos curiosos de hackers y adversarios.

Cómo la serie InfoCrypt de Isolation Systems puede ser utilizada en conjunto con Firewalls para crear verdaderas redes seguras, privadas y virtuales.

Una mejor solución a la hora de buscar un red segura, privada y virtual, consiste en la unión de paquetes de seguridad junto con firewalls, un ejemplo de esta configuración se muestra en la figura 5. La figura, también demuestra como un paquete IP es manipulado mientras se mueve de la computadora cliente de María hasta el site de Web en Boston.

FIGURA 5
Usando un encriptador de la Serie Isolation Systems InfonCrypt para crear una VPN segura.



Cuando María necesita el site de Web privado, crea un paquete destinado a la dirección IP del site de Web en Boston. Este paquete es interceptado por el encriptor que se fija en su tabla interna de asociaciones seguras y verifica si María puede, de hecho, acceder al site y determina que algoritmo de encripción debe utilizar cuando encripte el paquete. Asumiendo que María tiene los permisos correctos, el encriptor va a desencriptar el paquete entero incluyendo el encabezado IP original. Como la encripción se realiza con DES o Triple Pass DES, María no tiene que preocuparse de adversarios que quieran interceptar sus paquetes mientras estos viajan a través de la Internet, y luego leer o modificar sus transmisiones. Esta es una ventaja significativa sobre el caso explicado más arriba donde todas las transmisiones a través de la Internet ocurren abiertamente, y por ende, pueden ser fácilmente interceptadas por un hacker.
El encriptor en Chicago va a crear un nuevo paquete siendo la dirección origen la dirección IP negra y la dirección destino aquella correspondiente a la firewall en Boston. El paquete tendrá un encabezado UDP con protocolo 2233. El paquete va a pasar a través de la firewall en Chicago que va a usar un proxy de manera tal que el paquete que se va de la firewall tendrá la dirección externa de la firewall de Chicago como su dirección de origen. El paquete tiene ahora un origen routeable y una dirección de destino y por ende, puede ser routeado a través de la Internet a la firewall en Boston. Cuando el paquete es recibido en Boston, la firewall de Boston va

a examinar el paquete y al encontrar que es UDP protocolo 2233, lo puenteará a la dirección IP negra del encriptor en Boston.
Con esta configuración no se abren agujeros en la firewall. Las razones son las siguientes. Primero, el tráfico es sólo puenteado a la interface negra del encriptor que está en Boston. El encriptor en Boston usará certificados digitales X.509 para identificar positivamente que el que envía los paquetes es el encriptor de Chicago y que María tiene permiso para acceder a los recursos especificados antes de pasar el paquete. Si no puede autenticar el otro extremo de la comunicación o si María no tiene permiso para acceder a esos determinados recursos, el paquete será rebotado. Note que los certificados digitales son significativamente mas confiables que usar la dirección IP de María o un password. Es más, un único proxy es creado en la firewall para cualquier tipo de tráfico que María pueda estar enviando, sea este una búsqueda de DNS, acceso al Web, transferencia de archivos, etc. Esto incrementa significativamente la flexibilidad de la solución y reduce el número de agujeros en la firewall.
Asumiendo que el encriptor en Boston puede autenticar a María y que ella tiene permiso para acceder a los recursos especificados, el encriptor en Boston va a sacar el encabezado de IP, desencriptar el paquete original de María y routearlo al servidor de Web como fue requerido.
Otra ventaja importante es que esta solución va a trabajar tanto si María está detrás del InfoCrypt Enterprise Encryptor en Chicago, o usando el InfoCrypt Solo para llamar al ISP desde otro lugar.

Conseguir seguridad en las redes privadas virtuales a través del paquete F-Secure de la compañía Data Fellows.

F-Secure VPN es una solución flexible y de coste aprovechable para obtener los beneficios de Internet comprometiendose a mantener la seguridad en la misma. Dota a la gestión de la red de tuneles entre los puntos de empresa manteniendo el acceso a puntos externos si se quiere. Es mejor usar este paquete en union a una firewall para conseguir un control total sobre el tráfico de datos de toda la organización.
F-Secure VPN es un nuevo producto de la compañía Data Fellows que se encuentra dentro de la linea de productos enfocados a la seguridad de Internet. La compañía Data Fellows Ltd, es la primera vendedora de productos de seguridad. Usa los mecanismos de encriptación disponibles, más sofisticados y además es compatible con las arquitecturas modernas Cliente-Servidor y por supuesto Internet.

Introducción al producto F-Secure VPN.

El modo tradicional de conectar puntos empresariales próximos es usar servicios tradicionales "Telco" tales como X.25, lineas alquiladas o Frame Relay. Sin embargo, esos servicios tendieron a ser difíciles de obtener o era muy caros, principalmente en el entorno internacional. Como resultado de esto, muchos usuarios están pensando seriamente en usar Internet como su nexo de unión empresarial. Un gran número de analistas creen que pronto Internet reemplazará a la mayoría de las comunicaciones entre puntos empresariales internacionales, y también penetrará en las redes empresariales nacionales.
F-Secure VPN es una encaminador -router- de encriptación que te posibilita construir una VPN sobre la red con una seguridad criptográfica similar a la utilizada en el ejercito. Si tu eres un gestor de red corporativa, te ayudará a recortar el coste de las lineas sin perder seguridad. Si eres un proveedor de servicios, te dará la oportunidad de competir y revasar a la competencia, dado que F-Secure VPN te proporciona nuevos servicios con respecto a la seguridad.

Características de F-Secure VPN

Las características principales son las siguientes:

- **Fácil de instalar.** Requiere muy pocos parámetros de instalación para el administrador, durante la instalación inicial.
- **Fácil de configurar.** F-Secure VPN 1.1 destaca por un editor de red gráfico que permite configurar la totalidad de la red VPN desde una simple estación de trabajo.

- **Configurable para asegurar las conexiones Extranet.** Con el editor de red de F-Secure VPN, se puede definir la seguridad en las conexiones Extranet con tus clientes habituales.

- **Rápido.** En la actualidad, las redes privadas virtuales pueden aumentar la velocidad en tus conexiones entre puntos empresariales gracias a que comprimen todo el tráfico añadiendoles encriptación.

- **Seguro.** Usa una extensa variedad de algoritmos de selección de usuarios, incluyendo 3DES, Blowfish, RSA, etc.

- **Basado en una tecnología ampliamente testeada y usada.** F-Secure VPN está basado en la tecnología F-Secure SSH, el standard de hecho para conexiones entre terminales encriptados usando Internet. De hecho, esta tecnología es usada por la NASA

- **Asequible.** Una pequeña red privada virtual de 2 puntos puede instalarse por 5000 dolares más el precio de los PC's dedicados.

- **Disponible a nivel global, con una fuerte encriptación.** Data Fellows puede enviar el software encriptado a todo el mundo, sin ningún compromiso, desde las oficinas situadas en Europa o en US. Como compañía Europea que es, no se encuetra bajo las restricciones de exportación americanas referentes a la encriptación.

Arquitectura de F-Secure VPN

F-Secure encripta paquetes TCP/IP en el transcurso de la comunicación sobre Internet o una Intranet. Trabaja con cualquier clase de base de routers y firewalls instalados. También suministra la mayoria de potentes encriptadores disponibles, incluyendo triple DES (Encriptador de Datos Standard) y Blowfish. Además, F-Secure comprime datos, autentifica otros servidores encriptados, realiza gestión de claves distribuidas.
Normalmente, F-Secure VPN se situa detrás tanto de la firewall corporativa como del router (aunque también se admite otro tipo de configuraciones). El paquete incluye Unix y la herramienta de encriptación que es facilmente instalable en un Petium PC. Después de un intercambio y autentificación de claves iniciales entre los servidores F-Secure y otros puntos, el gestor de red únicamente desmonta el teclado y la pantalla con lo que la máquina llega a ser un servidor seguro. Entonces, los routers se deben configurar para enviar todos los paquetes TCP/IP procedentes de la encriptación, al servidor F-Secure y el resto de paquetes sin censura, se encaminarán normalmente. Los gestores de red, también tienen que configurar un puerta en su firewall para permitir que el tráfico encriptado alcance el servidor F-Secure sin filtrarlo.
Cuando se recibe un paquete, F-Secure VPN comprime y encripta tanto las cabeceras TCP como el resto de datos útiles. Entonces lo encapsula formando un segundo paquete que se envia a través de un "tunel virtual" desde la unidad F-Secure hasta otro punto. El software en el punto destino, desencripta el paquete y lo vuelve a dejar en su estado original antes de enviarlo a través de su LAN.
F-Secure VPN usa un protocolo llamada Secure Shell (SSH) que ha surgido como una standard de hecho para las comunicaciones seguras a través de Internet. El protocolo ha sido usado y testeado por organizaciones tales como la NASA (Washington, D.C.), así como por muchos bancos americanos. El standard ha sido desarrollado por el Grupo de Seguridad IP (IPSec) or la IETF(Internet Engineering Task Force) y estará implementado y listo para su aprovación a finales de 1997. SSH permite la gestión de claves distribuidas: en vez de almacenar las claves en una base de datos central lo cual ya es un claro objetivo para los ataques, los servidores F-Secure poseen sus propias claves. Y se pueden configurar para que cambien las claves de sesión cada hora de modo que estén protegidos contra los "hackers". El intercambio de claves se realiza de una forma segura, usando SSH y el

algoritmo de clave-pública de RSA Data Security Inc. (Redwood City, California). El límite recomendado para una red privada virtual es de 100 puntos seguros, debito al complejo sistema de gestión de claves de sesión.

Los beneficios de F-Secure contra los mecanismos de encriptación tradicionales.

F-Secure VPN es la única solución si se compara con las alternativas principales de encriptadores hardware standars. A menudo, esos proporcionan sólamente encriptación punto a punto lo cual las hace incómodas y caras para usar en un entorno Internet. Algunas firewall también porporcionan tuneles de encriptación pero esas soluciones son propietarias (atan al usuario a una cierta firewall) y a menudos son más complicadas de configurar y actualizar.

Los beneficios de F-Secure VPN son los siguientes:

- Cualquier PC con los requerimientos mínimos puede correr el software de F-Secure VPN.
- La red VPN es dinámicamente ampliable de modo que nuevas LANs se puede añadir a VPN existente sin demasiada configuración.
- Se pueden usar conexiones a internet de bajo coste para formar la VPN. Tradicionalmente, las redes privadas virtuales seguras han estado construyendose usando lineas alquiladas muy caras.
- Automáticamente se encriptan y protegen contra alteraciones, todas las conexiones F-Secure VPN.
- F-Secure VPN se integra con cualquiera de las firewalls existentes.
- F-Secure VPN soporta conexiones Extranet seguras.