Firewall

NAT-PAT

**Grupo8**

Sergio Guzman

Cristian Espindola

Gabriel Ituarte

***Firewalls***

Un firewall o cortafuegos es la parte de una red que está diseñada para bloquear el acceso no autorizado, permitiendo así sólo comunicaciones autorizadas. Permite, limita, cifra y descifra el tráfico entre los diferentes ámbitos basándose en un conjunto de normas y criterios. Se utilizan para evitar que los usuarios de Internet no autorizados tengan acceso a redes privadas conectadas a Internet. Todos los mensajes que entren o salgan de esas intranets pasan a través del firewall, que examina cada mensaje y bloquea aquellos que no cumplen los criterios de seguridad especificados. Un firewall puede ayudar a impedir que hackers o software malintencionado (comogusanos) obtengan acceso al equipo, así como impedir que el equipo envíe software malintencionado a otros. Pueden ser implementados en hardware o software, o una combinación de ambos.

**Las reglas que se pueden implementar en un firewall son:**

❖ Administrar los accesos de los usuarios a los servicios de la red

❖ Registrar todos los intentos de entrada y salida y almacenarlos en logs

❖ Filtrar paquetes en función de su origen, destino, y número de puerto (filtro de direcciones).

❖ Filtrar determinados tipos de tráfico en nuestra red o pc (filtrado de protocolo).

❖ Controlar el número de conexiones que se están produciendo desde un mismo punto

❖ Controlar las aplicaciones que pueden acceder a Internet

❖ Detección de puertos que están en escucha y no deberían estarlo

*¿Cómo funciona?*

El filtrado de paquetes llevado a cabo por un cortafuegos actúa

en las tres primeras capas del modelo OSI, lo que significa que

todo el trabajo lo realiza entre la red y las capas físicas. Cuando

el emisor origina un paquete y es interceptado por el

cortafuegos, éste último comprueba las reglas de filtrado de

paquetes que lleva configuradas, aceptando o rechazando el

paquete en consecuencia. Cuando el paquete pasa a través de

cortafuegos, se filtra mediante un protocolo y un número de

puerto base. Por ejemplo, si existe una norma en el cortafuegos

para bloquear el acceso telnet, bloqueará el protocolo IP para el

número de puerto 23.

**Historia**

La tecnología de los cortafuegos surgió a finales de 1980, cuando Internet era una tecnología bastante nueva en cuanto a su uso global y la conectividad. Hasta entonces Los predecesores de los cortafuegos para la seguridad de la red fueron los routers, que mantenían a las redes separadas unas de otras.

La visión de Internet como una comunidad relativamente pequeña de usuarios con máquinas compatibles, que valoraba la predisposición para el intercambio y la colaboración, llevó a una serie de importantes violaciones de seguridad de Internet. Por lo que el Cortafuegos se convertiría en un dispositivo indispensable dentro de la arquitectura de una red con acceso a Internet.

**Primera generación**

La Primera generación de corta fuegos data de 1988, cuando el equipo de ingenieros de Digital Equipment Corporation (DEC) desarrolló los sistemas de filtro conocidos como cortafuegos de filtrado de paquetes. Esta primera generación actúa mediante la inspección de los paquetes. Si uno no coincide con el conjunto de reglas del filtro, el paquete se descarta enviando una respuesta de error al emisor.

cada paquete se filtra basándose únicamente en la información contenida en él.

**Los elementos que se tienen en cuenta para tomar decisiones son:**

* La dirección de origen desde donde, supuestamente, viene el paquete (capa 3).
* La dirección del host de destino del paquete (capa 3).
* El protocolo específico que está susado para la comunicación, frecuentemente Ethernet o IP aunque existen iendo cortafuegos capas de desenvolverse con otros protocolos como IPX, NetBios, etc (capas 2 y 3).
* El tipo de tráfico: TCP, UDP o ICMP (capas 3 y 4).
* Los puertos de origen y destino de la sesión (capa 4).

Con todas o algunas de esta características se forman dos listas de reglas: una de permitidas y otra de denegadas. La forma en que un paquete recibido se procesa en función de estas dos listas difiere según el modelo, el fabricante y la configuración del cortafuegos lo que define en gran medida la permisividad del mismo.

Los más restrictivos exigen que el paquete pase con éxito por ambas listas, es decir, que no sea denegado en una y sea expresamente autorizado en la otra. En algunos cortafuegos solo existe una única lista de reglas y el paquete es procesado según la primera regla que encontramos en la tabla y define como tratarlo. Otros usan la última regla que encuentran como acción a efectuar. Por último, también encontramos diferencias en cuanto a que hacer cuando no se encuentra ninguna regla válida: algunos productos aceptan el paquete y otros lo rechazan.

En la siguiente tabla tenemos un pequeño ejemplo de una de estas últimas listas de

reglas en la que el cortafuegos posee la dirección IP 192.168.1.1:

Aparte de Aceptar (*Accept*) o Rechazar (*Deny o Drop*), la mayoría de los cortafuegos de este tipo poseen un tercer tipo de acción: Descartar (*Discard* o *Stealth*). Cuando un paquete es procesado por una regla que define esta acción, este se elimina ‘silenciosamente’ sin devolverse error alguno al originario del mismo creando un efecto de ‘agujero negro’ y evitando así el cortafuegos revelar su presencia.

**Ventajas**

Las principales ventajas de este tipo de cortafuegos están en su rapidez, transparencia y flexibilidad. Proporcionan un alto rendimiento y escalabilidad a muy bajo costo. son muy útiles para bloquear la mayoría de los ataques de Denegación de Servicio, por lo que se siguen implementando como servicios integrados en algunos routers .

* Rapidez, transparencia y flexibilidad.
* Alto rendimiento y escalabilidad a muy bajo costo.
* son muy útiles para bloquear la mayoría de los ataques de Denegación de Servicio, por ello se siguen implementando como servicios integrados en algunos routers.

**Desventajas**

Sus principales inconvenientes son su limitada funcionalidad y su dificultad a la

hora de configurarlos y mantenerlos.

* No pueden prevenir contra ataques que exploten vulnerabilidades específicas de determinadas aplicaciones, puesto que no examinan las capas altas del modelo OSI.

* La complejidad en la construcción de reglas hace que deban de ser configurados por expertos conocedores del protocolo y que sean muy susceptibles a los errores.
* Vulnerables a técnicas de *spoofing.*

No son efectivos como medida única de seguridad, pero si muy prácticos como primera barrera, en la que se bloquean ciertos ataques, se filtran protocolos no deseados y se pasan los paquetes restantes a otro cortafuegos que examine las capas más altas del protocolo.

**Segunda generación: "stateful" filters - cortafuegos de estado**

Los cortafuegos de segunda generación, llamados cortafuegos con inspección de

estado, o *Stateful Inspection Firewalls* o *Circuit Level Firewalls*, son básicamente

cortafuegos de filtrado de paquetes en los que, además, se valida a la hora de aceptar

o rechazar un paquete el hecho de que este sea una petición de nueva conexión o

pertenezca a un circuito virtual (o sesión) ya establecido entre un host externo y otro

interno.

Cuando una aplicación crea una sesión TCP con un host remoto, se establece un

puerto en el sistema ‘originario’ de la conexión con objeto de recibir allí los datos

provenientes del sistema remoto. De acuerdo a las especificaciones de TCP, este

puerto del host cliente estará comprendido entre el 1023 y el 16.384. En el sistema

remoto se establecerá, asimismo, un puerto que será siempre menor al 1024.

Los cortafuegos por filtrado de paquetes deben de permitir tráfico entrante en todos

los puertos superiores (1023 hasta 16.384) para permitir los datos de retorno de las

conexiones salientes. Esto crea un gran riesgo de intrusiones.

Los cortafuegos con inspección de estado resuelven eficazmente este problema construyendo una tabla con información correspondiente a todas las sesiones TCP abiertas y los puertos que utilizan para recibir los datos y no permitiendo el tráfico entrante a ningún paquete que no corresponda con ninguna de estas sesiones y puertos.

Para hacer esto, los cortafuegos de este tipo examinan rigurosamente el establecimiento de cada conexión (en la capa 4 del modelo OSI) para asegurarse de que esta es legítima y está permitida. Los paquetes no son remitidos a su destino hasta que el establecimiento de la conexión ha sido correctamente completado y verificado.

El cortafuegos mantiene una tabla de conexiones válidas y deja pasar los paquetes que contienen información correspondiente a una entrada válida en dicha tabla de circuitos virtuales. Una vez que la conexión finaliza la entrada en la tabla es eliminada y el circuito virtual entre los dos hosts es cerrado.

Las tablas de estado de circuitos virtuales suelen contener, por cada conexión, la

siguiente información:

* Un identificador de sesión único asignado por el cortafuegos a cada conexión establecida.
* El estado de la conexión: negociándose (*handshake*), establecida o cerrándose (capa 4).
* El número de secuencia del último paquete (capa 4).
* La dirección IP origen de los datos (capa 3).
* La dirección IP destino de los datos (capa 3).

Usando esta información y con un ligera inspección de las cabeceras de los

paquetes, el cortafuegos es capaz de determinar cuando un paquete es válido y cuando

no lo es. Una vez que la conexión es establecida, el resto de los paquetes asociados

con ella son rutados sin mas comprobaciones.

Esto los haría, de base, tremendamente vulnerables a ciertos tipos de ataques, pero muy pocos cortafuegos de este tipo son tan rudimentarios.

Sobre esta base, y aprovechando la gran velocidad y consistencia que supone la misma, se realizan otro tipo de verificaciones para asegurarse de que no ha habido suplantamiento (*spoofing*), que no existen paquetes malformados, etc. También son comunes en ellos la implantación de sistemas de translación de direcciones, NAT, que ocultan eficazmente el interior de nuestra red a intrusos externos.

**Ventajas**

Las principales ventajas de esta generación de cortafuegos son la velocidad de filtrado, la solidez de sus principios de cara a establecer una política de seguridad y, en conjunto con un esquema de traslación de direcciones, la sólida protección adicional a las direcciones IP internas.

**Desventajas**

Sus principales debilidades residen en su limitación estrictamente al escrutinio del protocolo TCP, la imposibilidad de chequear protocolos de niveles altos, las limitaciones inherentes a su mecánica de actuación a la hora de llevar un registro de sucesos y la imposibilidad de implementar algunos servicios de valor añadido, como realizar cacheado de objetos http o filtrado de URL’s (puesto que no ‘entienden’ estos protocolos).

* Limitación estrictamente al escrutinio del protocolo TCP.
* Imposibilidad de chequear protocolos de niveles altos
* Limitaciones a la hora de llevar un registro de sucesos
* Imposibilidad de implementar algunos servicios de valor añadido

**Tercera generación: application layer - cortafuegos de aplicación**

Como su nombre indica, esta generación de cortafuegos evalúa los paquetes realizando una validación en la capa de aplicación antes de permitir una conexión , al igual que los cortafuegos de segunda generacion, mantienen un riguroso control del estado de todas las conexiones y el número de secuencia de los paquetes. Lo que los hace mucho más seguro y fiables, ya que repercute en las siete capas del modelo OSI. En esencia es similar a los cortafuegos predecesores, con la diferencia de que también podemos filtrar el contenido del paquete.

Prácticamente la mayoría de los cortafuegos de este tipo funcionan implementando servicios de Proxy. Lo que proporcionando un control de acceso adicional y un detallado registro de sucesos.

Los agentes o servicios Proxy están formados por dos componentes: un servidor y un cliente. Ambos suelen implementarse como dos procesos diferentes lanzados por un único ejecutable. El servidor actúa como destino de las conexiones solicitadas por un cliente de la red interna. El cliente del servicio proxy es el que realmente encamina la petición hacía el servidor externo y recibe la respuesta de este. Posteriormente, el servidor proxy remite dicha respuesta al cliente de la red interna.

De esta forma estamos creando un aislamiento absoluto impidiendo una comunicación directa entre la red interna y la externa. En el diálogo entre cliente y servidor proxy se evalúan las peticiones de los clientes de la red interna y se decide aceptarlas o rechazarlas en base a un conjunto de reglas, examinando meticulosamente que los paquetes de datos sean en todo momento correctos. Puesto que son servicios hechos a medida para el protocolo que inspeccionan, se tiene un control total y un registro de sucesos al más alto detalle.

**Ventajas:**

Las principales ventajas de este tipo de cortafuegos son sus detallados registros de tráfico (ya que pueden examinar la totalidad del paquete de datos), el valor añadido que supone tener un servicio de autenticación de cara a seguridad de la red, y la casi nula vulnerabilidad que presentan ante ataques de suplantación (*spoofing*), el aislamiento que realizan de nuestra red, la seguridad que proporciona la

‘comprensión’ a alto nivel de los protocolos que inspeccionan y los servicios añadidos, como caché y filtro de URL’s, que prácticamente todos implementan.

* Detallados registros de tráfico (ya que pueden examinar la totalidad del paquete de datos).

* Servicio de autenticación de cara a seguridad de red.

* Casi nula vulnerabilidad que presentan ante ataques de suplantación (*spoofing*),

* Aislamiento de red.

* Comprensión a alto nivel de los protocolos que inspeccionan
* Servicios añadidos, como caché y filtro de URL’s.

**Desventajas:**

Entre los inconvenientes están sus menores prestaciones (en cuanto a velocidad de inspección se refiere) frente a los otros modelos ya vistos, la necesidad de contar con servicios específicos para cada tipo distinto de tráfico, la imposibilidad de ejecutar muchos otros servicios en el (puesto que escucha en los mismos puertos), la imposibilidad de inspeccionar protocolos como UDP, RPC y otros servicios comunes, la necesidad de reemplazar la pila TCP nativa en el servidor donde se ejecutan y lo vulnerables que resultan ante ataques directos al sistema operativo sobre el que se suelen ejecutar.

* Menor velocidad de inspección frente a los otros modelos.
* Servicios específicos para cada tipo distinto de tráfico.

* Imposibilidad de ejecutar muchos otros servicios a la vez (puesto que escucha en los mismos puertos).
* Imposibilidad de inspeccionar protocolos como UDP, RPC y otros servicios comunes.
* Vulnerable ante ataques directos al sistema operativo sobre el que se suelen se ejecutar.

**Cortafuegos posteriores:**

**Cortafuegos Híbridos.**

En los últimos años las fronteras entre las distintas generaciones de cortafuegos se han ido disolviendo, aparecen en el mercado productos comerciales que combinan las mejores características de cada generación. Así, por ejemplo, podemos encontrar con facilidad cortafuegos a nivel de aplicación con servicios de proxy que incluyen filtrado de paquetes para inspeccionar las tramas UDP.

En definitiva, la combinación de tecnologías y la amalgama de características de los

actuales productos ha potenciado las ventajas de estos equipos pero también ha

complicado en gran medida la tarea de elegir cual es el cortafuegos más adecuado a

nuestras necesidades.

1994, una compañía israelí llamada Check Point Software Technologies patentó un software denominándolo FireWall-1.

Aunque está catalogado como un cortafuegos de inspección de estados, el Firewall-

1 en realidad es un cortafuegos híbrido que intercepta los paquetes entre las capas 2 y

3 del modelo OSI, extrae la información relativa al estado de la conexión y mantiene dinámicamente tablas con información sobre el estado de las conexiones abiertas o en trámites de ser establecidas.

El módulo de inspección del Firewall-1 se carga dinámicamente en el núcleo (*kernel*) del sistema operativo de la máquina que lo aloja inspeccionando todos los paquetes entrantes y salientes que

pasan por las interfaces de red. Ningún paquete es procesado por las capas superiores

hasta que el motor de inspección verifica que cumple con las políticas de seguridad

establecidas.

* no se limita a la inspección de algunos datos de las cabeceras, sino que analiza información específica referente a todas las capas situadas por encima suyo, así como la información contenida en los datos del paquete.
* Para protocolos sin estado (como UDP y RPC) crea y almacena datos de contexto sobre una conexión virtual.
* permitir ciertos comandos mientras que deshabilita otros para una determinada aplicación.

( es posible permitir un ping ICMP mientras que se deniega un Redirect o permitir un get sobre SNMP mientras que deshabilitamos los comandos set sobre el mismo protocolo).

* Posee, adicionalmente, módulos especificos para realizar inspecciones ‘a medida’ sobre cientos de aplicaciones, servicios y protocolos, tales como Oracle, My SQL, RealAudio, etc.

*Tipos*

*Cortafuegos de capa de red o de filtrado de paquetes*

Funciona a nivel de red como filtro de paquetes IP. Se pueden realizar filtros según los distintos campos de los paquetes IP: dirección IP origen, dirección IP destino. A menudo se permiten filtrados según campos de nivel de transporte, como el puerto origen y destino, o a nivel de enlace de datos como la dirección MAC.

*Cortafuegos de capa de aplicación*

Trabaja en el nivel de aplicación, de manera que los filtrados se pueden adaptar a características propias de los protocolos de este nivel. Por ejemplo, si trata de tráfico HTTP, se pueden realizar filtrados según la URL a la que se está intentando acceder, e incluso puede aplicar reglas en función de los propios valores de los parámetros que aparezcan en un formulario web.Un cortafuegos a nivel 7 de tráfico HTTP suele denominarse proxy, y permite que los ordenadores de una organización entren a Internet de una forma controlada. Un proxy oculta de manera eficaz las verdaderas direcciones de red.

*Cortafuegos personal*

Del mismo modo que un delincuente informático puede intentar acceder a una computadora de una gran empresa, puede también intentar acceder a una computadora personal mal protegida con el objetivo de sustraer ficheros personales o instalar virus desde la red. La herramienta adecuada para la seguridad del sistema es un firewall personal. Es un caso particular de cortafuegos que se instala como software en un ordenador, filtrando las comunicaciones entre dicho ordenador y el resto de la red. Se usa por tanto, a nivel personal.

Funciona de forma permanente, monitoreando las conexiones que entran y salen de la computadora y es capaz de distinguir las que son legítimas de las realizadas por atacantes. En este segundo caso, las bloquea y lo notifica al usuario del ordenador.

El firewall personal, junto con un antivirus, proporciona el mayor grado de seguridad posible con herramientas comerciales.

*Demilitarized Zone (DMZ)*

Es frecuente conectar al cortafuegos a una tercera red, llamada zona desmilitarizada o DMZ, en la que se ubican los servidores de la organización que deben permanecer accesibles desde la red exterior. En seguridad informática, una zona desmilitarizada o red perimetral es una red local que se ubica entre la red interna de una organización y una red externa, generalmente en Internet. El objetivo de una DMZ es que las conexiones desde la red interna y la externa estén permitidas, mientras que en general las conexiones desde la DMZ sólo se permitan a la red externa -- los equipos en la DMZ no pueden conectar con la red interna. Esto permite que los equipos de la DMZ puedan dar servicios a la red externa a la vez que protegen la red interna en el caso de que intrusos comprometan la seguridad de los equipos situados en la zona desmilitarizada. Para cualquiera de la red externa que quiera conectarse ilegalmente a la red

interna, la zona desmilitarizada se convierte en un callejón sin salida.

La DMZ se usa habitualmente para ubicar servidores que es necesario que sean accedidos desde fuera,como servidores de correo electrónico, Web y DNS. Estos servicios alojados en estos servidores son los únicos que pueden establecer tráfico de datos entre el DMZ y la red interna, por ejemplo, una conexión de datos entre el servidor web y una base de datos protegida situada en la red interna.Las conexiones que se realizan desde la red externa hacia la DMZ se controlan generalmente utilizando port address translation (PAT).

Una DMZ se crea a menudo a través de las opciones de configuración del cortafuegos, donde cada red se conecta a un puerto distinto de éste. Esta configuración se llama cortafuegos en trípode (three-legged firewall).

*Ventajas de un cortafuegos*

❖ Bloquea el acceso a personas y/o aplicaciones no autorizadas a redes privadas

❖ Protege de intrusiones

❖ Optimización de acceso; identifica los elementos de la red internos y optimiza que la comunicación entre ellos sea más directa si así se desea

❖ Protección de información privada

❖ Protección contra virus

*Limitaciones*

❖ No puede proteger contra aquellos ataques cuyo tráfico no pase a través de él.

❖ No puede proteger de las amenazas a las que está sometido por ataques internos o usuarios

negligentes.

❖ No puede proteger contra los ataques de ingeniería social.

❖ No protege de los fallos de seguridad de los servicios y protocolos cuyo tráfico esté permitido.

*Políticas*

Hay dos políticas básicas en la configuración de un cortafuegos que cambian radicalmente la filosofía fundamental de la seguridad en la organización:

❖ Política restrictiva: Se deniega todo el tráfico excepto el que está explícitamente permitido. El cortafuegos obstruye todo el tráfico y hay que habilitar expresamente el tráfico de los servicios que se necesiten. Esta aproximación es la que suelen utilizar la empresas y organismos gubernamentales.

❖ Política permisiva: Se permite todo el tráfico excepto el que esté explícitamente denegado. Cada servicio potencialmente peligroso necesitará ser aislado básicamente caso por caso, mientras que el resto del tráfico no será filtrado. Esta aproximación la suelen utilizar universidades, centros de investigación y servicios públicos de acceso a Internet.

La política restrictiva es la más segura, ya que es más difícil permitir por error tráfico potencialmente peligroso, mientras que en la política permisiva es posible que no se haya contemplado algún caso de tráfico peligroso y sea permitido por omisión.

*Ejemplos de configuración de firewalls personales*

Windows incluye un firewall desde Windows XP en 2001, así que pagar por un firewall de terceros no tiene mucho sentido. Sin embargo, este cortafuegos protege al sistema de ataques del exterior, y no de programas locales que abusen de tu conexión a la red. Para una protección bilateral, existen muchos firewall gratuitos disponibles para cumplir esa tarea. Algunos de los requisitos ideales para un firewall personal son:

*Protección de puertos*

La conexión a Internet garantiza acceso a ilimitadas colecciones de información, pero también permite acceso de otros a nuestra computadora. Una de las tareas principales del firewall incluye permitir el tráfico de red válido y sólo el tráfico válido. Los puertos de una PC pueden estar abiertos, cerrados o en modo ‘sigiloso’. Cuando están en este último estado, no son visibles a atacantes externos, lo cual es ideal.

*Auto-protección*

Algunos firewalls indican su estado de forma desprotegida en el registro. Algo tan simple como cambiar el valor de ‘habilitado’ a ‘deshabilitado’ puede desactivar la protección. El firewall más elaborado del mundo no sirve de mucho si un programa malicioso puede finalizar sus procesos. Los cortafuegos personales actuales incluyen mecanismos contra los ataques de malware.

*Control de programas*

En los primeros firewalls, los usuarios eran bombardeados con pop-ups alertando sobre programas que querían acceder a una IP particular por un puerto particular. No todos los usuarios son capaces de responder con seguridad si permitir o denegar la conexión, y la mayoría lo resuelve eligiendo indiscriminadamente ‘permitir’.Los firewalls actuales incluidos en los programas de seguridad se encargan de esta cuestión internalizando por completo el control de programas. Configuran los permisos para programas conocidos y buenos, bloquean programas malos, y monitorean el comportamiento de programas desconocidos. Los firewalls personales no son tan sofisticados, por lo cual cada uno usa su propia técnica para reducir al máximo los pop-ups.

Existe un gran número de ofertas en el mercado. En algunos casos, los productos son gratuitos para usuarios particulares, y pagos sólo para empresas. La mayoría de las empresas que desarrollan y mantienen antivirus también disponen de estos productos. Algunos firewalls personales gratuitos:

**ZoneAlarm Free Firewall 2013**

Hace todo lo que un firewall gratis debería, incluye un número de características que son

relevantes para la seguridad. Es duro, bloquea hackers y gestiona el control de programas

sin un montón de popups.

**Comodo Firewall (2013)**

Tiene bloqueador de comportamiento, que protege áreas sensibles del sistema. Su

función Sandbox permite la navegación y la informática sin riesgo. DNS seguro previene

los ataques basados en DNS. Incluye navegador endurecido. Puede resultar abrumador

para gente con pocos conocimientos tecnológicos.

**TinyWall 2.1**

Este firewall gratis trabaja en conjunto con el Windows Firewall para ofrecer una simple,

efectiva y bilateral(two-way) protección firewall para Windows Vista y posteriores. Si

solo querés un firewall sin mucha parafernalia puede ser una buena opción.

*IETF standard documents (RFCs)*

La recomendación RFC 2979 de la IETF define las características de comportamiento y requerimientos de interoperabilidad para los cortafuegos de Internet. Plantea dichos requerimientos como un paso inicial necesario para hacer consistente el comportamiento de los cortafuegos en distintas plataformas, de acuerdo con las prácticas aceptadas del protocolo IP.

Otros RFC relacionados con firewall:

RFC 3093: Firewall Enhancement Protocol (FEP)

RFC 2647: Benchmarking Terminology for Firewall Performance (agosto ‘99)

RFC 3511: Benchmarking Methodology for Firewall Performance (abril ‘03)

***NAT-PAT***

NAT (Network Address Translation - Traducción de Dirección de Red) es un mecanismo utilizado por

routers IP para intercambiar paquetes entre dos redes que asignan mutuamente direcciones incompatibles.

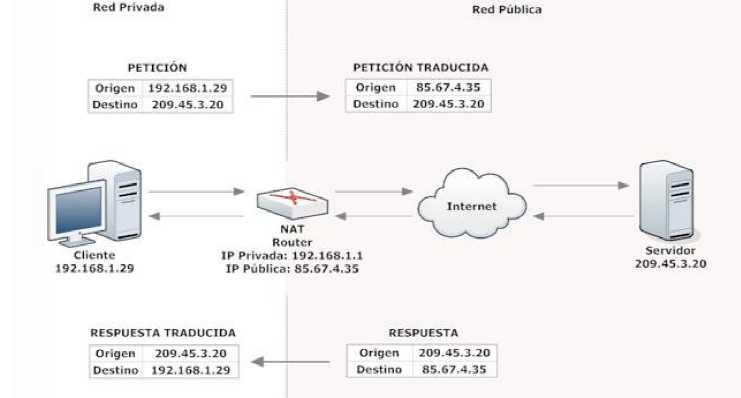
Este fue desarrollado por Cisco y consiste en convertir, en tiempo real, las direcciones utilizadas en los

paquetes transportados. También es necesario editar los paquetes para permitir la operación de

protocolos que incluyen información de direcciones dentro de la conversación del protocolo.

*Funcionamiento*

La mayoría de los NAT asignan varias máquinas -hosts- privadas a una dirección IP expuesta públicamente. En una configuración típica, una red local utiliza unas direcciones IP designadas “privadas” para subredes(RFC 1918). Un ruteador en esta red tiene una dirección privada en este espacio de direcciones. El ruteador también está conectado a Internet por medio de una dirección pública asignada por un proveedor de servicios de Internet. Como el tráfico pasa desde la red local a Internet, la dirección de origen en cada paquete se traduce sobre la marcha, de una dirección privada a una dirección pública. El ruteador sigue la pista de los datos básicos de cada conexión activa (en particular, la dirección de destino y el puerto).Cuando una respuesta llega al ruteador utiliza los datos de seguimiento de la conexión almacenados en la fase de salida para determinar la dirección privada de la red interna a la que remitir la respuesta. Todos los paquetes de Internet tienen una dirección IP de origen y una dirección IP de destino. En general, los paquetes que pasan de la red privada a la red pública tendrán su dirección de origen modificada, mientras que los paquetes que pasan a la red pública de regreso a la red privada tendrán su dirección de destino modificada. Estas traducciones de dirección se almacenan en una tabla, para recordar qué dirección y puerto le corresponde a cada dispositivo cliente y así saber donde deben regresar los paquetes de respuesta.



*NAT y TCP/UDP*

Los "Pure NAT" que operan sólo en IP, pueden o no analizar correctamente los protocolos que les concierne con la información IP. Tan pronto como la pila de protocolos es atravesada (incluso con protocolos básicos como TCP y UDP), los protocolos se romperán a menos NAT toma acción más allá de la capa de red.Los principales protocolos de la capa de transporte, TCP y UDP, tienen una suma de comprobación que cubre todos los datos que llevan, así como la cabecera TCP / UDP, además de una "pseudo-cabecera" que contiene las direcciones IP de origen y destino del paquete que lleva la cabecera TCP / UDP. Para que un NAT nuevo pase TCP o UDP con éxito, se debe volver a calcular la suma de comprobación del encabezado TCP / UDP basado en las direcciones IP traducidas, no los originales, y poner la suma de comprobación en la cabecera UDP/TCP del primer paquete del conjunto fragmentado de paquetes. El NAT receptor debe recalcular la suma de comprobación de IP en cada paquete que pasa al host de destino y también reconocer y recalcular la cabecera TCP / UDP utilizando las direcciones traducidas y la pseudo-cabecera. El problema no está completamente resuelto. Una solución es que el NAT receptor reensamble el segmento entero y recalcule la suma de comprobación calculada a lo largo de todos los paquetes.

*Tipos de NAT*

*Static NAT (Uno a uno)*

El tipo más simple de NAT proporciona una traducción una-a-una de las direcciones IP. La RFC 2663 se refiere a este tipo de NAT como NAT Básico. En este tipo de NAT únicamente, las direcciones IP, las sumas de comprobación (checksums) de la cabecera IP, y las sumas de comprobación de nivel superior, que se incluyen en la dirección IP necesitan ser cambiadas. El resto del paquete se puede quedar sin tocar. Es corriente ocultar un espacio completo de direcciones IP, normalmente son direcciones privadas IP, detrás de una única dirección IP (o pequeño grupo de direcciones IP) en otro espacio de direcciones (normalmente público).

Cuando el cliente envía paquetes fuera de la red, NAT traduce la dirección IP interna del cliente a una dirección externa. Para los usuarios externos, todo el tráfico que entra a la red y sale de ella tiene la misma dirección IP o proviene del mismo conjunto de direcciones.

Su uso más común es permitir utilizar direcciones privadas (definidas en el RFC 1918) para acceder a Internet. Existen rangos de direcciones privadas que pueden usarse libremente y en la cantidad que se quiera dentro de una red privada. Si el número de direcciones privadas es muy grande puede usarse solo una parte de direcciones públicas para salir a Internet desde la red privada. De esta manera simultáneamente sólo pueden salir a Internet con una dirección IP tantos equipos como direcciones públicas se hayan contratado.

*Dynamic NAT*

Es un tipo de NAT en la que una dirección IP privada se mapea a una IP pública basándose en una tabla de direcciones de IP registradas (públicas). Normalmente, el router NAT en una red mantendrá una tabla de direcciones IP registradas, y cuando una IP privada requiera acceso a Internet, el router elegirá una dirección IP de la tabla que no esté siendo usada por otra IP privada. Esto permite aumentar la seguridad de una red dado que enmascara la configuración interna de una red privada, lo que dificulta a los hosts externos de la red el poder ingresar a ésta. Para este método se requiere que todos los hosts de la red privada que deseen conectarse a la red pública posean al menos una IP pública asociadas.

*Overlapping NAT*

Cuando las direcciones IP utilizadas en la red privada son direcciones IP públicas en uso en otra red, el encaminador posee una tabla de traducciones en donde se especifica el reemplazo de éstas con una única dirección IP pública. Así se evitan los conflictos de direcciones entre las distintas redes.

*Overloading NAT (PAT - Uno a muchos)*

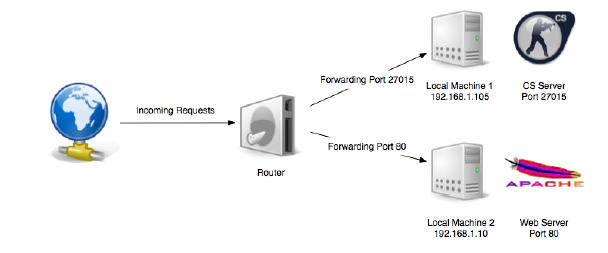
El caso de NAT con sobrecarga o PAT (Port Address Translation) es el más común de todos y el más usado en los hogares. Consiste en utilizar una única dirección IP pública para mapear múltiples direcciones IPs privadas. Las ventajas que brinda tienen dos enfoques: por un lado, el cliente necesita contratar una sola dirección IP pública para que las máquinas de su red tengan acceso a Internet, lo que supone un importante ahorro económico; por otro lado se ahorra un número importante de IPs públicas, lo que demora el agotamiento de las mismas.

Para poder hacer esto el router hace uso de los puertos. En los protocolos TCP y UDP se disponen de 65.536 puertos para establecer conexiones. De modo que cuando una máquina quiere establecer una conexión, el router guarda su IP privada y el puerto de origen y los asocia a la IP pública y un puerto al azar.Cuando llega información a este puerto elegido al azar, el router comprueba la tabla y lo reenvía a la IP privada y puerto que correspondan.

*Port forwarding*

Es el método por el cual una computadora en la red privada es accesible por las computadoras que existen en Internet, incluso cuando la computadora a la que se quiere acceder está detrás de un router. Este método es común cuando se hostea servidores de juegos, descargas de forma peer to peer y aplicaciones que utilizan voz sobre IP.

Toda pedido de conexión incluye un puerto. Este puerto es tan solo un numero y es en parte lo que ayuda a la computadora a saber que es el paquete. Un ejemplo es el puerto 80 que se utiliza para HTTP. Cuando se aplica Port Forwarding al router, se le indica a qué IP debe redirigir el paquete cuando este viene con un determinado puerto. Por ejemplo, en caso de venir un paquete con el puerto de destino igual a 80, el router enviará este paquete a una máquina de la red privada que se encuentre con ese puerto abierto, la cual sea probablemente un web server.



*Aplicaciones afectadas por NAT*

Varias aplicaciones que se usan diariamente son afectadas por el uso de NAT. Esto se debe a que utilizan distintas conexiones simultáneas con distintas IP o puertos. Entre ellas, se destacan las siguientes:

❖ FTP (Utiliza conexiones separadas)

❖ Voice over IP

❖ RTSP

❖ RealAudio

❖ X-windows

Para solucionar este problema, se deben aplicar técnicas especiales para evitar el comportamiento “aleatorio” de NAT y lograr que las comunicaciones no fallen. Algunas técnicas a nombrar pueden ser ALG(Application Layer Gateway) o NAT-T (Traversal NAT), . que permiten la traducción de IP/Puerto para ciertos protocolos de la capa de aplicación.

*Ventajas*

❖ Gran ahorro de direcciones IPv4: Podemos conectar múltiples máquinas de una red a Internetusando una única dirección IP pública.

❖ Seguridad. Las máquinas conectadas a la red mediante NAT no son visibles desde el exterior, por lo que un atacante externo no podría averiguar si una máquina está conectada o no a la red.

❖ Mantenimiento de la red. Sólo sería necesario modificar la tabla de reenvío de un router para

desviar todo el tráfico hacia otra máquina mientras se llevan a cabo tareas de mantenimiento.

*Desventajas*

❖ Checksums TCP y UDP: El router tiene que volver a calcular el checksum de cada paquete que modifica. Por lo que se necesita mayor potencia de computación.

❖ No todas las aplicaciones y protocolos son compatibles con NAT: Hay protocolos que introducen el puerto de origen dentro de la zona de datos de un paquete, por lo que el router no lo modifica y la aplicación no funciona correctamente.

*Ejemplos de software NAT*

❖ Internet Connection Sharing (ICS): NAT+DHCP para Windows desde W98SE

❖ WinGate: como ICS pero con más control

❖ IPFilter: Solaris, NetBSD, FreeBSD, xMach.

❖ PF (software): El filtro de paquetes OpenBSD.

❖ Netfilter/iptables el filtro de paquetes de Linux y su interface

***IETF standard documents (RFCs)***

❖ RFC 2663: Terminología y consideraciones sobre Traducción de Direcciones IP - IP Network

Address Translator (NAT) Terminology and Considerations

❖ RFC 3022: Traductor de Dirección de Red IP Tradicional (NAT Tradicional) - Traditional IP Network Address Translator (Traditional NAT)

❖ RFC 4787: Traducción de direcciones de red (NAT) Requisitos de comportamiento para Unicast UDP - Network Address Translation (NAT) Behavioral Requirement for Unicast UDP

❖ RFC 1918: Asignación de direcciones para Internet privadas - Address Allocation for Private

Internets

❖ RFC 2993: Architectural Implications of NAT

❖ RFC 1631: The IP Network Address Translator (NAT)