Firewall
NAT-PAT

David Jonatan Correa

Camila García

Ángeles Tella Arena

Tecnicatura Universitaria en Programación Informática
Universidad Nacional de Quilmes
Junio de 2014

Firewalls

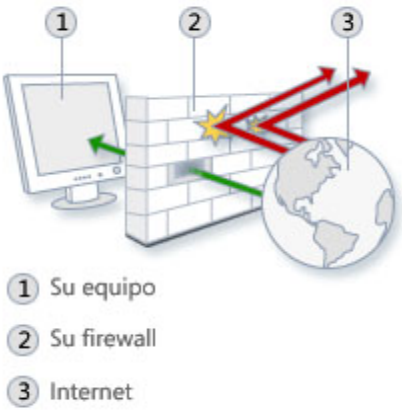
Un firewall o cortafuegos es la parte de una red que está diseñada para bloquear el acceso no autorizado, permitiendo así sólo comunicaciones autorizadas. Permite, limita, cifra y descifra el tráfico entre los diferentes ámbitos basándose en un conjunto de normas y criterios.
Se utilizan para evitar 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 (como gusanos) 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.



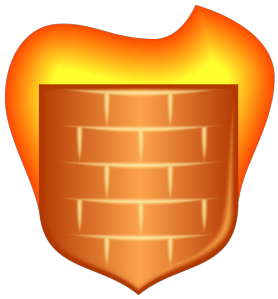
Historia

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. 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.
El gusano Morris fue el primer ejemplar de malware autorreplicable que afectó a internet. El 2 de noviembre de 1988, aproximadamente 6000 de los 60 000 servidores conectados a la red fueron infectados por este gusano informático, lo que motivó que se buscaran medidas de seguridad más extremas.

Primera generación: packet filters - filtrado de paquetes

El primer documento publicado para la tecnología firewall 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.

El filtrado de paquetes actúa mediante la inspección de los paquetes. Si uno coincide con el conjunto de reglas del filtro, el paquete se reducirá (descarte silencioso) o será rechazado, desprendiéndose de él y enviando una respuesta de error al emisor. Este tipo de filtrado de paquetes no presta atención a si el paquete es parte de una secuencia existente de tráfico; se filtra cada paquete basándose únicamente en la información contenida en él (por lo general utiliza una combinación del IP emisor del paquete y la de destino, su protocolo, y, en el tráfico TCP y UDP, el número de puerto).



Segunda generación: "stateful" filters - cortafuegos de estado

Durante 1989 y 1990 se desarrolló la segunda generación de servidores de seguridad. Esta versión tiene en cuenta la colocación de cada paquete individual dentro de una serie de paquetes. Esta tecnología se conoce generalmente como la inspección de estado de paquetes, ya que mantiene registros de todas las conexiones que pasan por el cortafuegos, siendo capaz de determinar si un paquete indica el inicio de una nueva conexión, es parte de una existente, o es un paquete erróneo. Este tipo de cortafuegos pueden ayudar a prevenir ataques contra conexiones en curso o ciertos ataques de denegación de servicio.

Tercera generación: application layer - cortafuegos de aplicación

Actúa sobre la capa de aplicación del modelo OSI, entendiendo ciertas aplicaciones y protocolos (por ejemplo: protocolo de transferencia de ficheros, DNS o navegación web), y permite detectar si un protocolo no deseado se coló a través de un puerto no estándar o si se está abusando de un protocolo de forma perjudicial.

Un cortafuegos de aplicación es mucho más seguro y fiable cuando se compara con un cortafuegos de filtrado de paquetes, ya que repercute en las siete capas del modelo OSI. En esencia es similar a un cortafuegos de filtrado de paquetes, con la diferencia de que también podemos filtrar el contenido del paquete.

Un cortafuegos de aplicación puede filtrar protocolos de capas superiores tales como FTP, TELNET, DNS, DHCP, HTTP, TCP, UDP y TFTP. Por ejemplo, si una organización quiere bloquear toda la información relacionada con una palabra en concreto, puede habilitarse el filtrado de contenido para bloquear esa palabra en particular.

Posteriores

En 1992, Bob Braden y DeSchon Annette, de la Universidad del Sur de California (USC), dan forma al concepto de cortafuegos. Su producto, conocido como "Visas", fue el primer sistema con una interfaz gráfica, fácilmente implementable y compatible con sistemas operativos como Windows o MacOS. En 1994, una compañía israelí llamada Check Point Software Technologies lo patentó como software denominándolo FireWall-1. Actualmente, la Internet Engineering Task Force (IETF) está trabajando en la estandarización de protocolos para la gestión de cortafuegos. Otro de los ejes en desarrollo consiste en integrar la identidad de los usuarios dentro del conjunto de reglas del cortafuegos. Algunos cortafuegos proporcionan características tales como unir a las identidades de usuario con las direcciones IP o MAC; otros proporcionan características de identificación real solicitando la firma del usuario para cada conexión.

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.

Comparación de firewalls

Comparación entre features básicas de filtrado

Can Target:	Changing default policy to accept/reject (by issuing a single rule)	IP destination address(es)	IP source address(es)	TCP/UDP destination port(s)	TCP/UDP source port(s)	Ethernet MAC destination address	Ethernet MAC source address	Inbound firewall (ingress)	Outbound firewall (egress)
IPFire	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Trend Micro Internet Security	Yes	Yes	Yes	Yes	Yes	No	No	Yes	Yes
Untangle	Yes	Yes	Yes	Yes	Yes	No	No	Yes	Yes
Vyatta	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Windows XP Firewall	No	No	Yes	Partial	No	No	No	Yes	No
Windows Vista Firewall	Yes	Yes	Yes	Yes	Yes	No	No	Yes	Yes
Windows 7 / Windows 2008 R2 Firewall	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
WinGate	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Zeroshell	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes
Zorp	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Comparación entre features avanzadas

Can:	work at OSI Layer 4 (stateful firewall)	work at OSI Layer 7 (application inspection)	Change TTL? (Transparent to traceroute)	Configure REJECT-with answer	DMZ - allows for single/several hosts not to be firewalled	Filter according to time of day	Redirect TCP/UDP ports (port forwarding)	Redirect IP addresses (forwarding)	Filter according to User Authorization	Traffic rate - limit / QoS	Tarpit	Log
IPFire	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
Sidewinder	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Untangle	Yes	Yes (Some modules)	No	No	Yes	Yes (With Policy manager)	Yes	Yes	Yes	Yes	Yes	Yes
WinGate	Yes	Yes	Yes	No	Yes	Yes	Yes	No	Yes	Yes	No	Yes
Zeroshell	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes

Comparación entre otros features

Features:	Modularity: supports third-party modules to extend functionality?	IPS : Intrusion prevention system	Open-Source License?	supports IPv6 ?	Class: Home / Professional	Operating Systems on which it runs?
IPFire	Yes	Yes, with Snort	Yes	Yes (since IPFire 3)	Both	Linux-based appliance distribution
Untangle	Yes	Yes	Yes	No	Both	Linux (built on Debian)
Vyatta	Yes	Yes	Yes	Yes	Professional	Vyatta OS (built on Debian)
WinGate	Yes	-	No	No	Professional	Windows 2000, Windows XP, Windows 2003, Windows Vista, Windows 2008. 32bit and 64bit.

Comparación entre features extra (non-firewall)

Can:	NAT (static, dynamic w/o ports, PAT)	IDS (Intrusion Detection System)	VPN (Virtual Private Network)	AV (Anti-Virus)	Sniffer	Profile selection
IPFire	Yes	Yes (with integrated Snort)	Yes (IPsec and OpenVPN)	Yes (with clamav)	Yes (with tcpdump)	-
Untangle	Yes	Yes	Yes (IPsec and OpenVPN)	Yes (clamav,commtouch (optional))	Yes (tcpdump)	-
Vyatta	Yes (supports three NAT types)	Yes (integrated Snort)	Yes (IPsec and OpenVPN)	Yes (with clamav,Sophos Antivirus (optional))	Yes (with wireshark or tcpdump)	-
WinGate	Yes	Yes (with NetPatrol)	Yes (proprietary)	Yes (Kaspersky Labs)	Yes (filtered capturing to pcap format)	No

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)

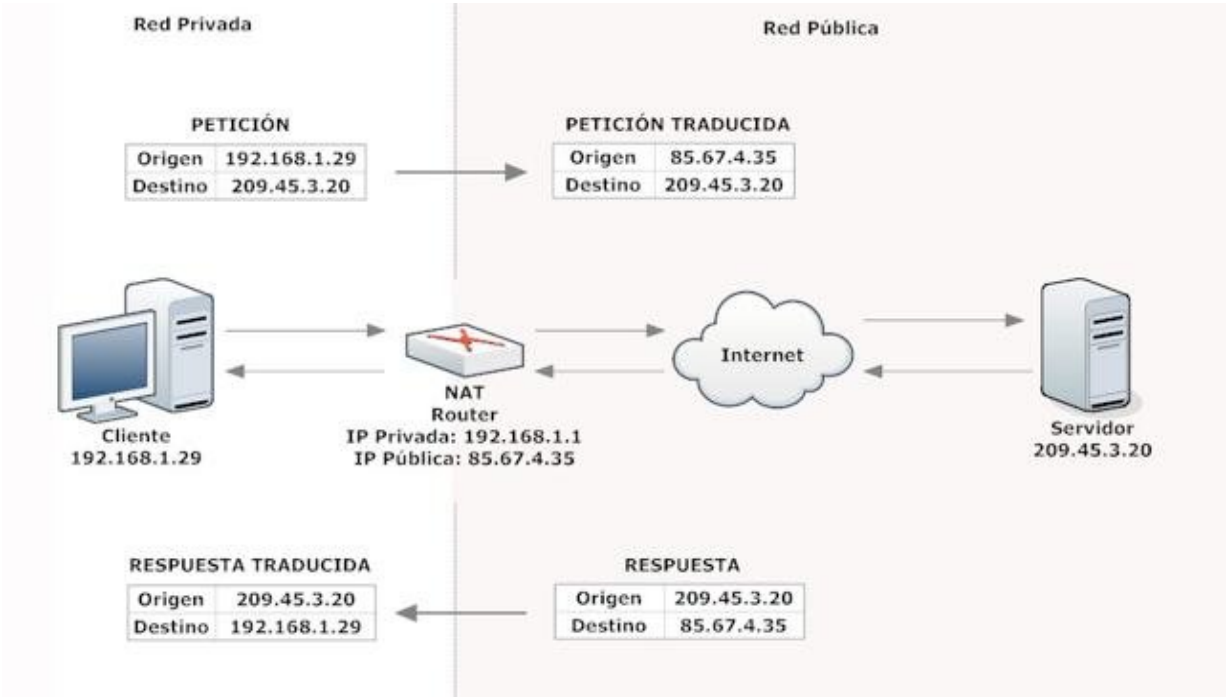
La recomendación RFC 2979 de la IETF define las características de comportamiento y requerimientos de interoperabilidad para los cortafuegos de Internet. Plantea dichos requerimientos como un paso inicial necesario para hacer consistente el comportamiento de los cortafuegos en distintas plataformas,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

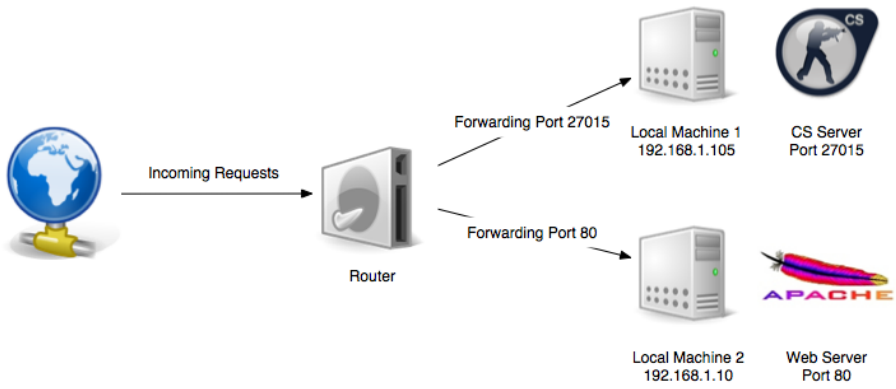
Cuando las direcciones IP utilizadas en la red privada son direcciones IP públicas en uso en otra red, el encaminador posee una tabla de traducciones en donde se especifica el reemplazo de éstas con una única dirección IP pública. Así se evitan los conflictos de direcciones entre las distintas redes.

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 Internet usando 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

Ejemplos de configuración

Este ejemplo para configurar un NAT en un router, es realizado con un simulador de router real, el Cisco Packet Tracer. En esta muestra, contamos con 3 routers, un Switch y tres computadoras.

<u>NAT con sobrecarga (conexiones del equipo desde Internet a la red con IPs privadas)</u>

- Se conectan los dispositivos entre sí por los puertos adecuados en cada caso (ethernet, ATM, Serial, etc.)
- Se configura el enrutamiento IP con RIP -Routing Information Protocol, Protocolo de Información de Enrutamiento-, ya que se recomienda para configuraciones más sencillas y rápidas.
- Parametrizaciones del ejemplo:
  - El puerto conectado a internet es el Ethernet0
  - El puerto conectado a la red LAN es el Ethernet1
  - El rango IP de la LAN es 192.168.1.0 con máscara 255.255.255.0 y wildmask 0.0.0.255
  - La lista de accesos se llamará INTERNET
  - PAT: Orientando puerto de HTTP 80 sobre máquina 192.168.0.1 puerto 8080

```
Router(config)#ip nat inside source list INTERNET interface Dialer0 overload
Router(config)#ip access-list standard INTERNET
Router(config)#permit 192.168.1.0 0.0.0.255
Router(config)#deny   any
```

➢ Asociación de interfaces (puertos) al NAT

```
Router(config)#interface ethernet0
Router(config)#ip nat outside
Router(config)#interface ethernet1
Router(config)#ip nat intside
```

➢ Implementación del PAT

```
Router(config)#ip nat inside source static tcp 192.168.0.1 8080 interface ethernet0 80
```

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)

Referencias

Firewall

Microsoft - ¿Qué es un firewall?
DesarrolloWeb.com - ¿Qué es un firewall?
UNAM - Firewalls personales
Vinagre Asesino - Tipos de firewalls: ventajas y desventajas
IETF - RFC 2979: Behavior of and Requirements for Internet Firewalls
PCMag - The best free firewalls
es.comp.os.linux - Configuración de un cortafuegos
hTecnicoBAT - IPTables, ejemplo de firewall personal
Wikipedia - Comparison of firewalls

NAT - PAT

Xataka On - NAT
HowStuffWorks - NAT
ADSL FAQs - ¿Qué es NAT?
University of St. Andrews - NAT, complete learning resource
Super User - What is port forwarding?
PortForward.com - How To Port Forward a Router
Uninet - Problems due to widespread use of NAT and IPSEC considerations