NAT y Firewall en redes p2p

Día a día la crece la cantidad de usuarios que acceden a redes P2P (Peer to Peer) por medio de conexiones con un gran ancho de banda. Estas redes P2P ya no solo se utilizan para intercambio de archivos, sino que además se utilizan para la transmisión de VoIP (Voz sobre IP), MI (Mensajería Instantánea), videoconferencia, entre muchas otras. Uno de los problemas más graves a los que se enfrenta un sistema P2P es la existencia de Firewalls y sobre todo, de entornos NAT (Network Address Translation), que son dispositivos que proveen de conexión a Internet a un gran número de equipos a través de una sola dirección. En este trabajo se describen los protocolos estándares que actúan y el funcionamiento e implementación de conexiones P2P a través de NAT/Firewalls utilizando transversabilidad. Describiendo de una manera gráfica y detallada distintas técnicas para lograr la solución, mostrando además ventajas y desventajas de la solución.

Capitulo 1

Introducción

El uso de mecanismos NAT, (traducción de direcciones) permite usar una sola IP pública para toda una red privada. Pero esta práctica imposibilita el uso de muchas aplicaciones, que quedan relegadas a su uso en Intranets, dado que muchos protocolos son incapaces de atravesar los dispositivos NAT. Protocolos como RTP y RTCP (Protocolo de Transporte en Tiempo Real y Protocolo de Control en Tiempo Real) usan UDP con asignación dinámica de puertos (NAT no soporta esta traslación). Estos protocolos se utilizan para la transmisión de sonido y vídeo, muy utilizados hoy en día por un sinnúmero de empresas para realizar videoconferencias con otras sucursales. Al buscar una solución para crear conexiones P2P a través de Firewalls con NAT, son muchas las alternativas que existen. Pero la idea principal es crear este tipo de conexiones sin modificar configuraciones en los firewalls, y además no entrar en gastos de nuevas tecnologías que utilicen elementos intermedios. Este proyecto busca dar solución a la transversabilidad en firewalls, de forma en que solamente se necesite un servidor con IP pública, y una aplicación P2P que realice la transversabilidad. Bajo este esquema otras soluciones quedan fuera del tema por razones de costo e implementación y serán solamente mencionadas. Para realizar esta transversabilidad es necesario analizar el funcionamiento de las redes P2P, los software orientados a esta tecnología, protocolos estándares de conectividad, tipos de NAT usados y métodos de transversabilidad existentes.

Objetivo General

Implementar la Transversabilidad en Firewalls, de manera que se pueda enviar un archivo mediante una conexión P2P, a través de firewalls o dispositivos que realicen NAT. Todo esto sin cambiar configuraciones en los Firewalls.

Objetivos Específicos

- Realizar un estudio de las redes P2P.
- Realizar un estudio de Traducción de Direcciones.
- Investigar los distintos métodos existentes actualmente para realizar transversabilidad.
- Analizar la estructura y funcionamiento de Protocolos Involucrados.
- Estudios de otros proyectos de transversabilidad relacionados.
- Implementar la Transversabilidad.

¿Por qué?

Actualmente estamos bajo el funcionamiento de IPv4, con lo que tenemos 4,294,967,296 direcciones IP distintas para ser utilizadas públicamente. Aunque pareciera ser una cantidad suficiente para el total de computadoras y otros aparatos que necesitarían una dirección IP, el hecho es que estas han sido repartidas en diversas clases, dominios y usos, lo cual reduce las posibilidades de que cualquier persona pueda asignar una dirección IP pública, es decir identificada por el resto de Internet. La solución es el protocolo de nueva generación IPv6, que otorga mucha mayor cantidad de direcciones, pero aún deberá pasar mucho tiempo para que se realicen las modificaciones necesarias en las redes de manera que sean compatibles con esta norma. Mientras tanto NAT es una alternativa previa al uso de IPv6, pero la utilización de NAT genera que muchas aplicaciones que trabajan bajo redes P2P no funcionen adecuadamente. Esto debido a que un NAT implica, en cierta medida, colocar un Firewall que protege a la red local, ya que al no saber los equipos externos la dirección privada de los sistemas internos, no solicita la conexión. Todo enlace hacia Internet deberá generarse bajo petición de los equipos locales. En videoconferencia por ejemplo detrás de un NAT es el equipo local el que debe iniciar la llamada, cuando el sistema remoto contesta, es el equipo NAT quien le responde, y al no tener capacidades de negociación (H.323 para este caso), la llamada termina.

Posibles soluciones a esta problemática expuesta

- Ubicar un sistema que responda a las conexiones entrantes en la Zona Desmilitarizada (DMZ).
- Configurar el equipo NAT para enviar las peticiones entrantes en ciertos puertos hacia la IP privada del equipo local.
- Utilizar servidores duales (requiere inversión).

Todas estas soluciones involucran la adquisición de equipamiento, por lo tanto inversión, y configuración de equipos. La solución que se propone pretende posibilitar el uso de aplicaciones P2P de un modo seguro y transparente, facilitar la conectividad P2P a través de NAT sin configuraciones especiales , y permitir la construcción de futuros software P2P que funcionen en entornos con NAT.

Capitulo 2

Traducción de direcciones (NAT)

El crecimiento actual de las redes y los masivos cambios en seguridad han creado nuevas vías que hacen difícil el funcionamiento de algunas aplicaciones. La arquitectura original de Internet donde cada equipo se podía comunicar directamente con otro utilizando una IP única y global, ha sido remplazada por una nueva arquitectura de direcciones, consistente en una dirección global y muchas direcciones privadas interconectadas por NAT [1]. En esta nueva arquitectura como se ve en la figura 1, sólo los equipos que tengan dirección pública pueden ser fácilmente conectados por otros en la red, ya que tienen una única, global y ruteable dirección IP. Los equipos de las redes privadas pueden conectarse entre sí, o pueden establecer conexiones TCP o UDP con equipos que pertenezcan a la red pública.

Figura 1: Esquema de conectividad en Internet

6

Los dispositivos que realizan el NAT traducen la dirección y puertos de los paquetes que provienen de las redes privadas hacia las redes públicas [1], por lo tanto los dispositivos NAT generalmente permite sólo conexiones salientes y bloquea cualquier trafico entrante, a no ser que este configurado específicamente de otra manera. Esta nueva arquitectura de direcciones permite la comunicación cliente / servidor en el caso típico donde el cliente se encuentra en una red privada y el servidor se encuentra en la red pública. Esta arquitectura hace difícil la comunicación directa entre dos equipos (que es importante para las redes P2P) que pertenezcan a distintas redes privadas. Con esto tenemos que muchas aplicaciones P2P que comparten archivos, realizan videoconferencia, y juegos en línea que no funcionan a través de entornos con NAT.

Cómo funciona el NAT

Cuando un cliente en la red interna contacta a un equipo público, envía paquetes IP destinados a ese

equipo. Estos paquetes contienen toda la información de direccionamiento necesaria para que puedan ser llevados a su destino. NAT se encarga de estas piezas de información:

1. Dirección IP de origen (Ej:192.168.0.1)
2. Puerto TCP o UDP de origen (Ej: 12345)

Cuando los paquetes pasan a través de la pasarela de NAT, son modificados para que parezca que se han originado y provienen de la misma pasarela de NAT. La pasarela de NAT registra los cambios que realiza en su tabla de estado, para así poder:

1. a) Invertir los cambios en los paquetes devueltos.

1. b) Asegurarse de que los paquetes devueltos pasen a través del cortafuego.

Por ejemplo, podrían ocurrir los siguientes cambios:

- IP de origen: sustituida con la dirección externa de la pasarela (Ej:216.155.76.8)
- Puerto de origen: sustituido con un puerto no en uso de la pasarela. (Ej: 50050)

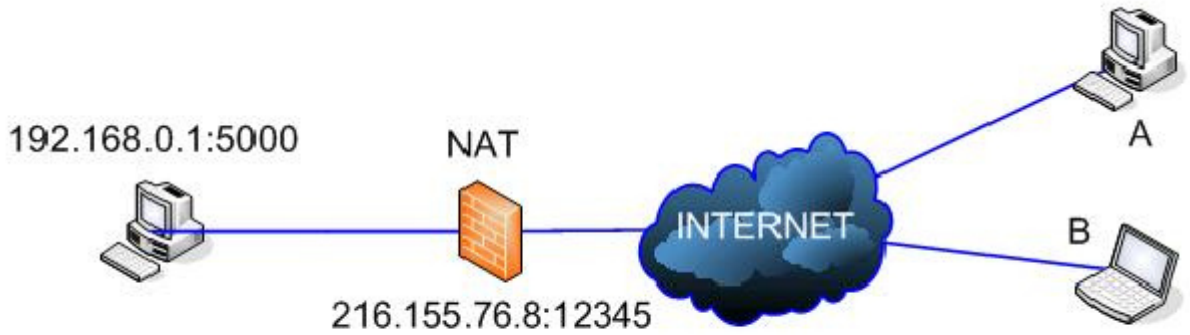
Ni la máquina interna ni el otro equipo de Internet se dan cuenta de estos pasos de traducción. Para el equipo interno, el sistema NAT es simplemente una pasarela a Internet. Para el equipo público, los paquetes parecen venir directamente del sistema NAT; ni siquiera se da cuenta de que existe la estación interna. Cuando el anfitrión de Internet responde a los paquetes internos de la máquina, los direcciona a la IP externa de la pasarela NAT (216.155.76.8) y a su puerto de traducción (50050). La pasarela de NAT busca entonces en la tabla de estado para determinar si los paquetes de respuesta concuerdan con alguna conexión establecida.

Tipos de NAT

Existen cuatro tipos de NAT [1]. Para las direcciones internas los tres primeros tipos de NAT mantienen una traducción de dirección independiente de la dirección de destino. El cuarto tipo de NAT creará una traducción independiente por cada conexión con el destinatario. A menos que el NAT posea una tabla de traducción estática, la traducción se inicia cuando el primer paquete es enviado desde el cliente a través del NAT y éste será válido por una cierta cantidad de tiempo (generalmente un par de minutos), a menos que se sigan enviando paquetes a esa IP y puerto.

Full Conexión

En el caso de la conexión completa o llena, (Full Cone) ver figura 2, cuando la traducción se encuentra establecida, cualquier equipo que quiera alcanzar al cliente detrás del NAT, necesita sólo conocer la dirección y el puerto de donde el tráfico está siendo enviado. Por ejemplo un equipo detrás de un NAT con dirección 192.168.0.1 enviando y recibiendo en el puerto 5000, se ha traducido a la dirección externa 216.155.76.8 en el puerto 12345. Cualquier equipo de Internet puede enviar tráfico a esta IP externa y este tráfico será traspasado a la dirección cliente 192.168.0.1:5000.



Conexión Restringida

En este caso de la conexión restringida, (Restricted Cone) ver figura 3, la IP y puerto externo son abiertos cuando el equipo de la red privada envía tráfico saliente a una dirección IP específica . Por ejemplo si el cliente envía paquetes hacia el equipo A, el NAT traduce la dirección privada 192.168.0.1:5000 a la dirección pública 216.155.76.8:12345, dejando que solamente el equipo A pueda enviar tráfico a esa dirección pública. El NAT bloqueará cualquier otro tráfico que venga de una dirección distinta. Por lo tanto el equipo B podrá enviar tráfico hacia la red privada, solamente si antes el equipo que se encuentra detrás del NAT a enviado tráfico a este equipo B.

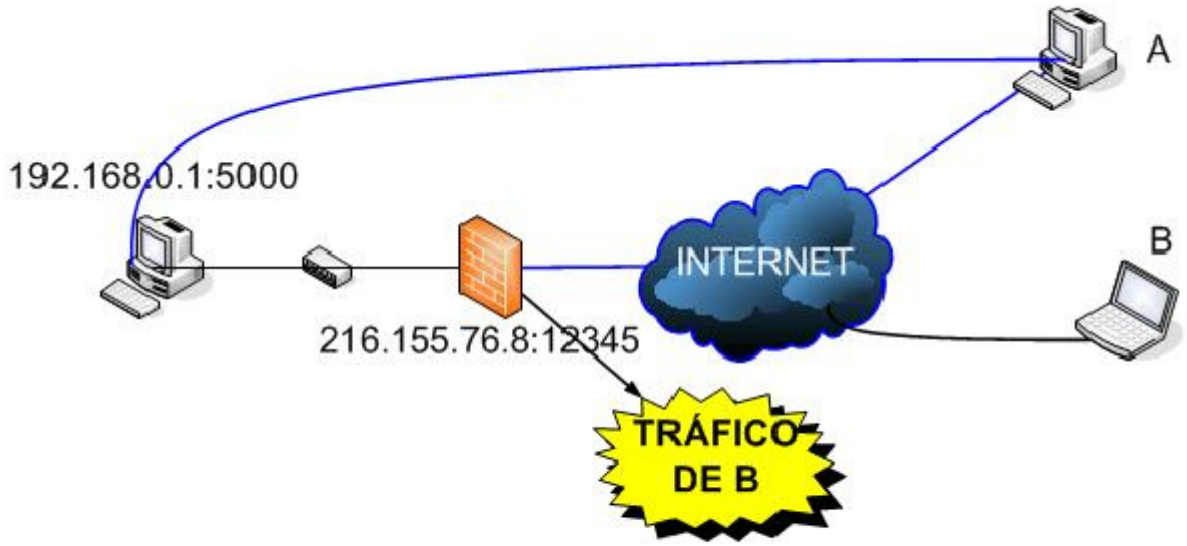


Figura 3 : NAT Conexión restringida

Conexión Restringida por Puerto

Una conexión restringida por puerto, (Port Restricted Cone) ver figura 4, es casi idéntica a la conexión restringida, pero en este caso el NAT bloqueará todo el tráfico, a menos que el cliente haya enviado

antes tráfico a una IP y puerto especifico, solo entonces esa IP:PUERTO tendrán acceso a la red privada. Entonces en nuestro ejemplo si el cliente envía tráfico al equipo B puerto 10101, el NAT sólo permitirá tráfico proveniente desde 200.72.40.55:10101, ahora si el cliente envía a múltiples direcciones y puertos entonces estas direcciones podrán responder al cliente a la dirección 216.155.76.8:12345.

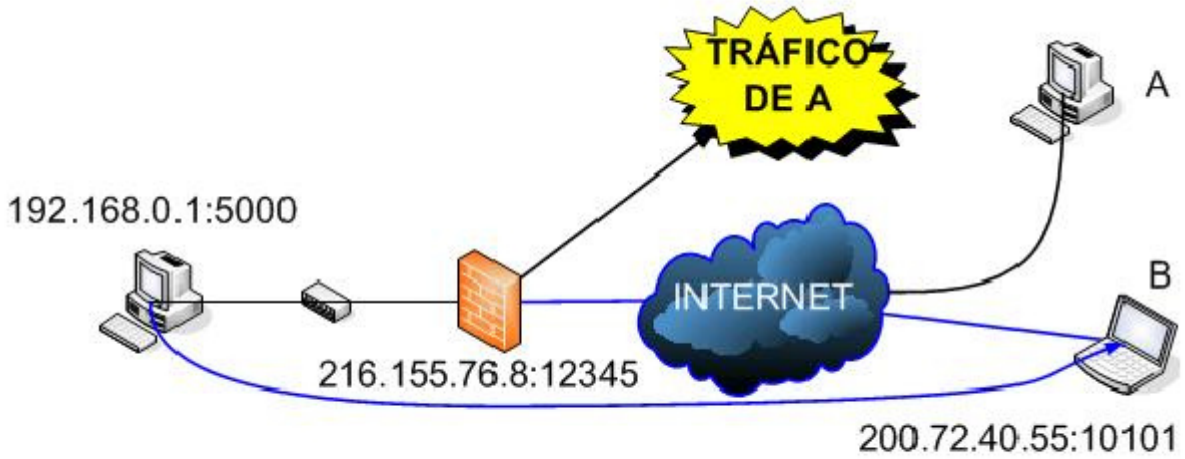


Figura 4 : Conexión restringida por puerto

Simétrico

El último tipo de NAT simétrico, (Symmetric NAT) ver figura 5, es diferente de los otros tres. Específicamente debido a que la traducción de la IP pública a la privada depende de la IP de destino donde ha sido enviado el tráfico. Para nuestro ejemplo si el cliente envía tráfico desde la dirección privada 192.168.0.1:5000 al equipo B, la dirección traducida sería la 216.155.76.8 con el puerto 12345, y si el equipo privado envía tráfico a otra IP pública distinta la dirección traducida para ese equipo sería la 216.155.76.8 con el puerto 45678.

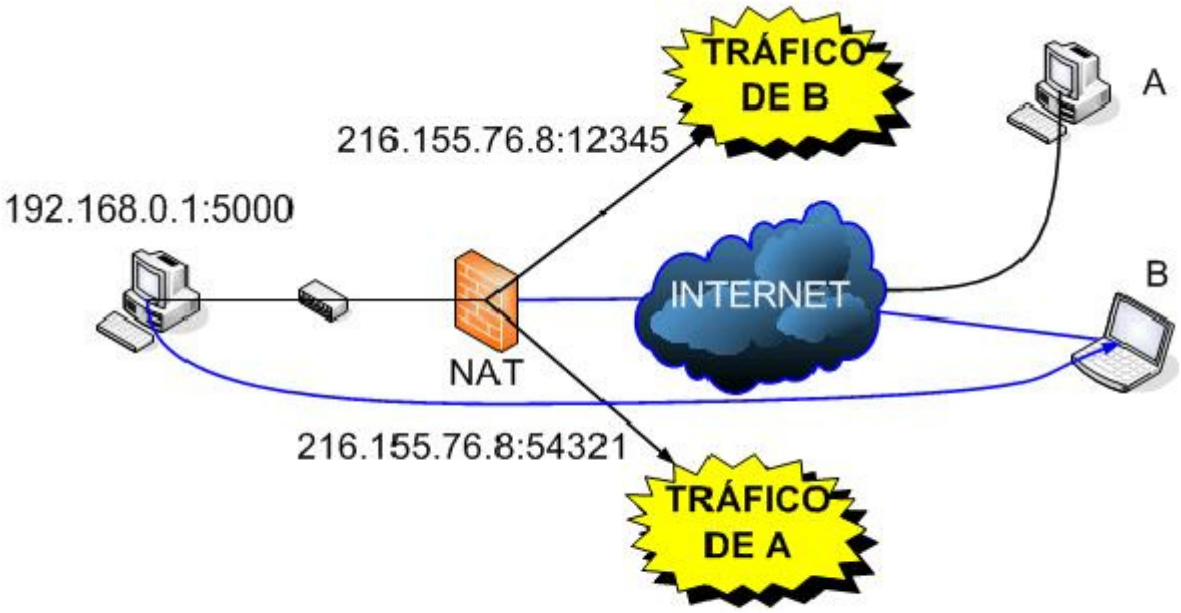


Figura 5: NAT Simétrico

El equipo B puede solamente responder a su dirección traducida (216.155.76.8:12345) y el equipo A a su dirección (216.155.76.8:45678). Si cualquier otro equipo envía tráfico a cualquiera de estas dos direcciones éste será rechazado.

STUN

STUN (Simple Traversal of UDP Through NAT) es un protocolo liviano que permite a las aplicaciones descubrir la presencia y tipos de NAT y/o Firewalls entre ellos y la Internet [2]. También provee a las aplicaciones la determinación de la dirección IP pública asignada por el dispositivo NAT. STUN trabaja con muchos NAT existentes, y no requiere ningún comportamiento especial. Como resultado se obtiene una red variada de aplicaciones que pueden funcionar a través de la infraestructura NAT. Esta compuesto por un programa STUN servidor que tiene que estar disponible en la Internet, y por el cliente STUN que tiene que ser alojado dentro de la red que se encuentra tras el dispositivo NAT o Firewall. El cliente STUN es una entidad que genera peticiones STUN, y este cliente puede ser utilizado por un PC, o puede ser ejecutado como elemento de red, como por ejemplo un servidor de conferencias. El servidor STUN es una entidad que recibe peticiones STUN y envía respuestas STUN. Dentro de las principales características a destacar de STUN tenemos:

- STUN activa un dispositivo para encontrar su dirección pública y tipo de NAT que da accesoa Internet.
- STUN opera en los puertos TCP y UDP 3478.
- STUN aún no es soportado por todos los tipos de dispositivos VoIP.
- STUN puede usar registros DNS SRV para encontrar servidores STUN unidos al dominio.
- El nombre del servicio es _stun._udp o _stun._tcp

Funcionamiento de STUN

Las peticiones STUN especifican los siguientes parámetros:

- •Dirección de Respuesta
- •IP Cambiada
- •Puerto Cambiado

El servidor STUN enviará su respuesta a la dirección IP y puerto especificado en la dirección derespuesta. Si el campo no se encuentra definido, entonces el servidor enviará la respuesta a ladirección IP y puerto de donde recibió la petición. Si la dirección IP de cambio y el puerto decambio no están definidos, el servidor STUN responderá desde la dirección IP y puerto donde elpaquete inicial fue enviado. Si la dirección IP de cambio está definida, el servidor responderá desdeuna dirección IP diferente, y si el puerto de cambio está definido, el servidor responderá desde unpuerto diferente. La respuesta STUN contiene la siguiente información:

- •Dirección mapeada: La dirección IP y puerto del cliente que es vista por el primerservidor STUN afuera del NAT, una vez recibida la petición STUN.
- •Dirección cambiada: La dirección IP que debería ser fuente de la respuesta recibida,si la petición tiene activado el flag de cambio de dirección IP.
- •Dirección Fuente: La dirección IP y puerto donde la respuesta STUN fue enviada.Usando una combinación de diferentes peticiones hacia el servidor STUN, un cliente puededeterminar si el equipo se encuentra disponible a la Internet, si el equipo se encuentra detrás de unFirewall que bloquea UDP, si el equipo se encuentra detrás de un NAT y que tipo de NAT estádetrás.