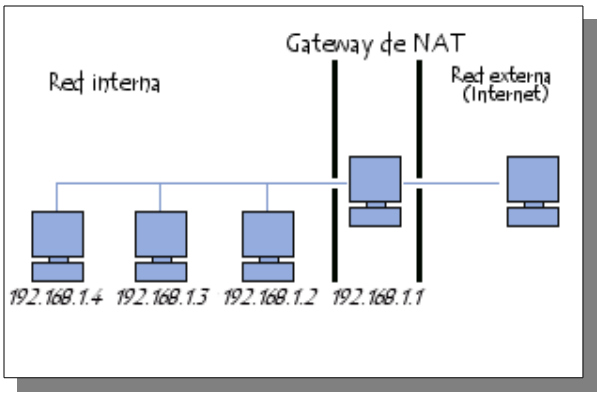
El principio de NAT

La conversión de direcciones de red o NAT se desarrolló para resolver la falta de direcciones IP con el protocolo IPv4 (dentro de poco tiempo el protocolo IPv6 resolverá este problema).

De hecho, en las direcciones IPv4 la cantidad de direcciones IP enrutables (que son únicas en el mundo) no es suficiente para permitir que todos los equipos que lo requieran estén conectados a Internet.

Por lo tanto, el principio de NAT consiste en utilizar una conexión de pasarela a Internet, que tenga al menos una interfaz de red conectada a la red interna y al menos una interfaz de red conectada a Internet (con una dirección IP enrutable) para poder conectar todos los equipos a la red.

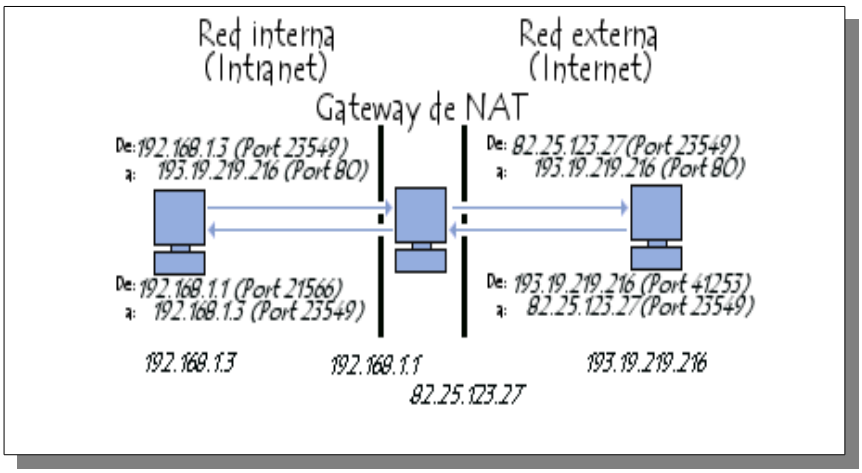


Es cuestión de crear, al nivel de la pasarela, una conversión de paquetes desde la red interna hacia la red externa.

Por lo tanto, se configura cada equipo en la red que necesite acceso a Internet para que utilice una pasarela de NAT (al especificar la dirección IP de la pasarela en el campo "Gateway" [Pasarela] con sus parámetros TCP/IP). Cuando un equipo de red envía una solicitud a Internet, la pasarela hace la solicitud en su lugar, recibe la respuesta y la envía al equipo que hizo la solicitud.

Normas :

- RFC 3022 - Conversor de direcciones de red IP tradicional (NAT tradicional)
- RFC 1918 - Asignación de direcciones para Internets privadas



Debido a que la pasarela oculta completamente las direcciones internas en la red, el mecanismo de conversión de direcciones de red brinda una función segura. De hecho, para un observador externo de la red, todas las solicitudes parecen provenir de la dirección IP de pasarela.

Espacio de la dirección

La organización que administra el espacio de direcciones públicas (direcciones IP enrutables) es la Agencia de Asignación de Números de Internet (IANA, Internet Assigned Number Authority). RFC 1918 define un espacio de dirección privada que permite que cualquier organización asigne direcciones IP a equipos en su red interna sin correr el riesgo de entrar en conflicto con una dirección IP pública asignada por la IANA. Estas direcciones conocidas como no enrutables corresponden a las siguientes series de direcciones:

- Clase A: desde 10.0.0.0 hasta 10.255.255.255;
- Clase B: desde 10.16.0.0 hasta 172.31.255.255;
- Clase C: desde 192.168.0.0 hasta 192.168.255.55

Todos los equipos de una red interna, conectados a Internet a través de un router y que no posean una dirección IP pública, deben utilizar una dirección que se encuentre dentro de estas series. Para redes domésticas pequeñas, generalmente se utiliza la serie de direcciones comprendidas entre 192.168.0.1 y 192.168.0.255.

Conversión estática

El principio de NAT estática consiste en vincular una dirección IP pública con una dirección IP interna privada en la red. Por lo tanto, el router (o más precisamente la pasarela) permite que una dirección IP privada (por ejemplo 192.168.0.1) esté vinculada con una dirección IP enrutable pública en Internet y lleva a cabo la conversión, en cualquier dirección, al cambiar la dirección en el paquete IP.

Por consiguiente, la conversión de direcciones de red estática permite que equipos de una red interna estén conectados a Internet de manera transparente, pero no resuelve el problema de falta de direcciones, en la medida en que n direcciones IP enrutables son necesarias para conectar n equipos a la red interna.

Conversión dinámica

La NAT dinámica permite que diversos equipos con direcciones privadas compartan una dirección IP enrutable (o un número reducido de direcciones IP enrutables). Entonces visto desde afuera, todos los equipos de la red interna prácticamente poseen la misma dirección IP. Ésta es la razón por la cual a veces se utiliza el término "enmascaramiento IP" para indicar la conversión de direcciones de red dinámica.

Para poder "multiplexar" (compartir) las diferentes direcciones IP en una o varias direcciones IP enrutables, la NAT dinámica utiliza la Conversión de direcciones por puerto (PAT, Port Address Translation), es decir, la asignación de un puerto de origen diferente para cada solicitud, de manera que se pueda mantener una correspondencia entre las solicitudes que provienen de la red interna y las respuestas de los equipos en Internet, todas enviadas a la dirección IP del router.

Habilitación de puertos

La conversión de direcciones de red sólo permite solicitudes provenientes de la red interna hacia la red externa, con lo cual es imposible que un equipo externo envíe un paquete a un equipo de la red interna. En otras palabras, los equipos de la red interna no pueden funcionar como un servidor con respecto a la red externa.

Por esta razón, existe una extensión NAT llamada "habilitación de puertos" o mapeo de puertos que consiste en configurar la pasarela para enviar todos los paquetes recibidos en un puerto particular a un

equipo específico de la red interna. Por lo tanto, si la red externa necesita acceder a un servidor Web (puerto 80) que funciona en un equipo 192.168.1.2, será necesario definir una regla de habilitación de puertos en la pasarela, con lo cual se redirigirán todos los paquetes TCP recibidos en el puerto 80 al equipo 192.168.1.2.

Activación de puertos

La mayoría de las aplicaciones cliente-servidor realiza una solicitud a través de un host remoto en un puerto determinado y a su vez abre un puerto para recuperar los datos. Sin embargo, ciertas aplicaciones utilizan más de un puerto para intercambiar datos con el servidor. Éste es el caso, por ejemplo, del FTP, para el que se establece una conexión por el puerto 21, pero los datos se transfieren por el puerto 20. Por lo tanto, con NAT, después de una solicitud de conexión en el puerto 21 de un servidor FTP remoto, la pasarela espera una conexión en un solo puerto y rechazará la solicitud de conexión en el puerto 20 del cliente.

Existe un mecanismo derivado de la NAT llamado "activación de puertos" que permite autorizar la conexión con determinados puertos (habilitación de puertos) si se completa una condición (solicitud). Por lo tanto, se trata de una habilitación de puertos condicional que permite que un puerto se abra sólo cuando una aplicación lo solicita. De esta manera, el puerto no permanece permanentemente abierto.

Redes Privadas Virtuales

Las redes de área local (LAN) son las redes internas de las organizaciones, es decir las conexiones entre los equipos de una organización particular. Estas redes se conectan cada vez con más frecuencia a Internet mediante un equipo de interconexión. Muchas veces, las empresas necesitan comunicarse por Internet con filiales, clientes o incluso con el personal que puede estar alejado geográficamente.

Sin embargo, los datos transmitidos a través de Internet son mucho más vulnerables que cuando viajan por una red interna de la organización, ya que la ruta tomada no está definida por anticipado, lo que significa que los datos deben atravesar una infraestructura de red pública que pertenece a distintas entidades. Por esta razón, es posible que a lo largo de la línea, un usuario entrometido, escuche la red o incluso secuestre la señal. Por lo tanto, la información confidencial de una organización o empresa no debe ser enviada bajo tales condiciones.

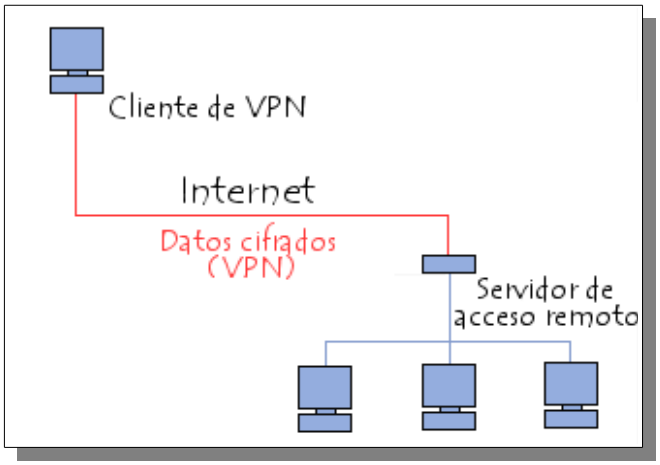
La primera solución para satisfacer esta necesidad de comunicación segura implica conectar redes remotas mediante líneas dedicadas. Sin embargo, como la mayoría de las compañías no pueden conectar dos redes de área local remotas con una línea dedicada, a veces es necesario usar Internet como medio de transmisión.

Una buena solución consiste en utilizar Internet como medio de transmisión con un protocolo de túnel, que significa que los datos se encapsulan antes de ser enviados de manera cifrada. El término Red privada virtual (abreviado VPN) se utiliza para hacer referencia a la red creada artificialmente de esta manera.
Se dice que esta red es virtual porque conecta dos redes "físicas" (redes de área local) a través de una conexión poco fiable (Internet) y privada porque sólo los equipos que pertenecen a una red de área local de uno de los lados de la VPN pueden "ver" los datos.

Por lo tanto, el sistema VPN brinda una conexión segura a un bajo costo, ya que todo lo que se necesita es el hardware de ambos lados. Sin embargo, no garantiza una calidad de servicio comparable con una línea dedicada, ya que la red física es pública y por lo tanto no está garantizada.

Funcionamiento de una VPN

Una red privada virtual se basa en un protocolo denominado protocolo de túnel, es decir, un protocolo que cifra los datos que se transmiten desde un lado de la VPN hacia el otro.



La palabra "túnel" se usa para simbolizar el hecho que los datos estén cifrados desde el momento que entran a la VPN hasta que salen de ella y, por lo tanto, son incomprensibles para cualquiera que no se encuentre en uno de los extremos de la VPN, como si los datos viajaran a través de un túnel. En una VPN de dos equipos, el cliente de VPN es la parte que cifra y descifra los datos del lado del usuario y el servidor VPN (comúnmente llamado servidor de acceso remoto) es el elemento que descifra los datos del lado de la organización.

De esta manera, cuando un usuario necesita acceder a la red privada virtual, su solicitud se transmite sin cifrar al sistema de pasarela, que se conecta con la red remota mediante la infraestructura de red pública como intermediaria; luego transmite la solicitud de manera cifrada. El equipo remoto le proporciona los datos al servidor VPN en su red y éste envía la respuesta cifrada. Cuando el cliente de VPN del usuario recibe los datos, los descifra y finalmente los envía al usuario.

Protocolos de túnel

Los principales protocolos de túnel son:

- **PPTP** (Protocolo de túnel punto a punto) es un protocolo de capa 2 desarrollado por Microsoft, 3Com, Ascend, US Robotics y ECI Telematics.
- **L2F** (Reenvío de capa dos) es un protocolo de capa 2 desarrollado por Cisco, Northern Telecom y Shiva. Actualmente es casi obsoleto.
- **L2TP** (Protocolo de túnel de capa dos), el resultado del trabajo del IETF (RFC 2661), incluye todas las características de PPTP y L2F. Es un protocolo de capa 2 basado en PPP.
- **IPSec** es un protocolo de capa 3 creado por el IETF que puede enviar datos cifrados para redes IP.

Protocolo PPTP

El principio del PPTP (Protocolo de túnel punto a punto) consiste en crear tramas con el protocolo PPP y encapsularlas mediante un datagrama de IP.

Por lo tanto, con este tipo de conexión, los equipos remotos en dos redes de área local se conectan con una conexión de igual a igual (con un sistema de autenticación/cifrado) y el paquete se envía dentro de un datagrama de IP.

De esta manera, los datos de la red de área local (así como las direcciones de los equipos que se encuentran en el encabezado del mensaje) se encapsulan dentro de un mensaje PPP, que a su vez está encapsulado dentro de un mensaje IP.

Protocolo L2TP

L2TP es un protocolo de túnel estándar (estandarizado en una RFC, solicitud de comentarios) muy similar al PPTP. L2TP encapsula tramas PPP, que a su vez encapsulan otros protocolos (como IP, IPX o NetBIOS).

Protocolo IPSec

IPSec es un protocolo definido por el IETF que se usa para transferir datos de manera segura en la capa de red. En realidad es un protocolo que mejora la seguridad del protocolo IP para garantizar la privacidad, integridad y autenticación de los datos enviados.

IPSec se basa en tres módulos:

- Encabezado de autenticación IP (AH), que incluye integridad, autenticación y protección contra ataques de REPLAY a los paquetes.
- Carga útil de seguridad encapsulada (ESP), que define el cifrado del paquete. ESP brinda privacidad, integridad, autenticación y protección contra ataques de REPLAY.
- Asociación de seguridad (SA) que define configuraciones de seguridad e intercambio clave. Las SA incluyen toda la información acerca de cómo procesar paquetes IP (los protocolos AH y/o ESP, el modo de transporte o túnel, los algoritmos de seguridad utilizados por los protocolos, las claves utilizadas, etc.). El intercambio clave se realiza manualmente o con el protocolo de intercambio IKE (en la mayoría de los casos), lo que permite que ambas partes se escuchen entre sí.

El protocolo PPP

El protocolo PPP proporciona un método estándar para transportar datagramas multiprotocolo sobre enlaces simples punto a punto entre dos "hosts"

Estos enlaces proveen operación bidireccional full dúplex y se asume que los paquetes serán entregados en orden.

Tiene tres componentes:

1. Un mecanismo de enmarcado para encapsular datagramas multiprotocolo y manejar la detección de errores.
2. Un protocolo de control de enlace (LCP, Link Control Protocol) para establecer, configurar y probar la conexión de datos.
3. Una familia de protocolos de control de red (NCPs, Network Control Protocols) para establecer y configurar los distintos protocolos de nivel de red.

Funcionamiento general

Para dar un panorama inicial del funcionamiento de este protocolo en el caso comentado, en que un usuario de una PC quiera conectarse temporalmente a Internet, describiremos brevemente los pasos a seguir:

En primera instancia, la PC llama al router del ISP (Internet Service Provider, proveedor del servicio de Internet), a través de un módem conectado a la línea telefónica.

Una vez que el módem del router ha contestado el teléfono y se ha establecido una conexión física, la PC manda al router una serie de paquetes LCP en el campo de datos de uno o más marcos PPP (esto será explicado con mayor detalle más adelante). Estos paquetes y sus respuestas seleccionan los parámetros PPP por usar.

Una vez que se han acordado estos parámetros se envían una serie de paquetes NCP para configurar la capa de red.

Típicamente, la PC quiere ejecutar una pila de protocolos TCP/IP, por lo que necesita una dirección IP. No hay suficientes direcciones IP para todos, por lo que normalmente cada ISP tiene un bloque de ellas y asigna dinámicamente una a cada PC que se acaba de conectar para que la use durante su sesión. Se utiliza el NCP para asignar la dirección de IP.

En este momento la PC ya es un host de Internet y puede enviar y recibir paquetes IP. Cuando el usuario ha terminado se usa NCP para destruir la conexión de la capa de red y liberar la dirección IP.

Luego se usa LCP para cancelar la conexión de la capa de enlace de datos.

Finalmente la computadora indica al módem que cuelgue el teléfono, liberando la conexión de la capa física.

PPP puede utilizarse no solo a través de líneas telefónicas de discado, sino que también pueden emplearse a través de SONET o de líneas HDLC orientadas a bits.

IETF

Internet Engineering Task Force (IETF) (en español Grupo de Trabajo de Ingeniería de Internet1) es una organización internacional abierta de normalización, que tiene como objetivos el contribuir a la ingeniería de Internet, actuando en diversas áreas, como transporte, encaminamiento, seguridad. Fue creada en EE. UU. en 1986. El IETF es mundialmente conocido por ser la entidad que regula las propuestas y los estándares de Internet, conocidos como RFC.

RFC

Request for Comments son una serie de publicaciones del grupo de trabajo de ingeniería de internet que describen diversos aspectos del funcionamiento de Internet y otras redes de computadoras, como protocolos, procedimientos, etc. y comentarios e ideas sobre estos.1 2 Cada RFC constituye un monográfico o memorando que ingenieros o expertos en la materia han hecho llegar al IETF, el consorcio de colaboración técnica más importante en Internet, para que éste sea valorado por el resto de la comunidad. De hecho, la traducción literal de RFC al español es "Petición de comentarios".

SONET

La red óptica sincronizada (en idioma inglés Synchronous Optical Network, cuyo acrónimo es SONET) es un estándar para el transporte de telecomunicaciones en redes de fibra óptica.

Taller :

1. Que software existe en Linux y en Windows para crear VPN?
2. Como se crea nuestra red VPN en Windows?
3. Si tengo dos computadores conectados a una VLAN, con direcciones de redes diferentes, se podrán comunicar?
4. Si tengo una VLAN10 configurada con direcciones de red 192.168.10.0/24 y coloco dos computadores en esa VLAN10 con direcciones de red 192.168.20.0/24, se podrán comunicar? Explicar.
5. Si tengo una Switch normal con dos hosts con direcciones de red 192.168.10.0/24 y adiciono dos computadores en ese Switch con direcciones de red 192.168.20.0/24, se podrán comunicar? Explicar.
6. Si tengo varias VLAN en un Switch se podrán comunicar entre si esas VLAN?
7. Como hago para que se puedan comunicar entre si las VLAN?