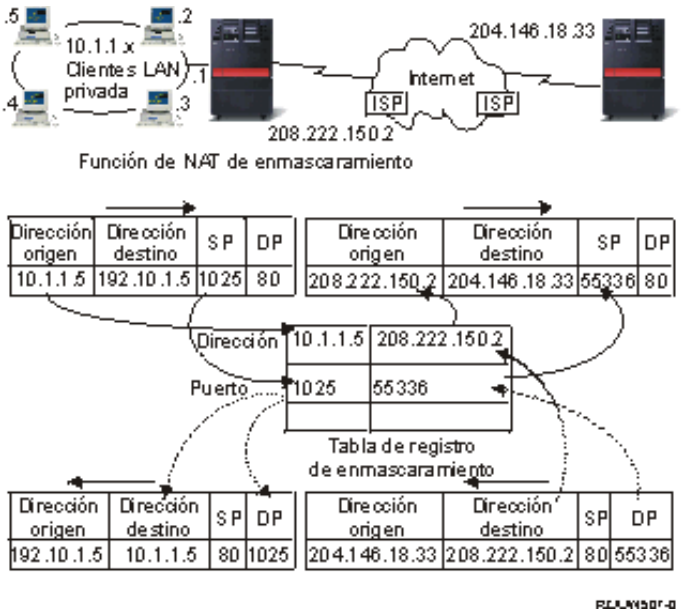
NAT de enmascaramiento

La función de NAT de enmascaramiento sirve para permitir a la red privada ocultarse detrás de, así como estar representada por, la dirección enlazada con la interfaz pública. En muchas ocasiones, se trata de la dirección que ha sido asignada por un proveedor de servicios Internet (ISP) y puede ser una dirección dinámica en el caso de las conexiones PPP. Este tipo de conversión sólo sirve para conexiones cuyo origen esté en el interior de la red privada y cuyo destino se halle en la red pública exterior. Cada conexión de salida se mantiene utilizando un número de puerto IP de origen diferente.

La función de NAT de enmascaramiento permite a las estaciones de trabajo que tengan direcciones IP privadas comunicarse con los sistemas principales de Internet mediante el AS/400. Éste tiene una dirección IP, asignada por el ISP local, como pasarela Internet. Se emplea el término máquina conectada localmente para hacer referencia a todas las máquinas de una red interna, independientemente del cuál sea el método de conexión (LAN o WAN) y de cuál sea la distancia que cubre la conexión. Se utiliza el término máquinas externas para designar las máquinas situadas en Internet. La figura siguiente ilustra el modo en que actúa la función de NAT de enmascaramiento.



Desde el punto de vista de Internet, todas las estaciones de trabajo están en apariencia contenidas en el AS/400; es decir, sólo hay una dirección IP asociada tanto con el AS/400 como con las estaciones de trabajo. Cuando un direccionador recibe un paquete dirigido a la estación de trabajo, intenta determinar cuál es la dirección de la LAN interna que debe recibirlo y se lo envía.

Cada estación de trabajo debe estar configurada de manera que el AS/400 sea su pasarela y, a la vez, su destino por omisión. La correspondencia entre una conexión de comunicación (puerto) determinada y una estación de trabajo se configura cuando una de las estaciones de trabajo envía un paquete al AS/400 para que se envíe a Internet. La función de NAT de enmascaramiento guarda el número de puerto, de manera que, cuando recibe a través de la conexión la respuesta al paquete de la estación de trabajo, puede enviarla a la estación de trabajo correcta.

La función de NAT de enmascaramiento crea y mantiene un registro de las conexiones de puerto activas y de la hora del último acceso por parte de cualquiera de los dos extremos de la conexión. De este registro se eliminan de forma periódica todas las conexiones que han estado desocupadas durante un período de tiempo

predeterminado tomando como base la suposición de que una conexión desocupada ha dejado de utilizarse.

Toda comunicación entre la estación de trabajo e Internet debe ser iniciada por las máquinas conectadas localmente. Se trata de un cortafuegos de seguridad efectivo; Internet desconoce por completo la existencia de las estaciones de trabajo y no puede difundir sus direcciones por Internet.

Un factor clave en la implementación de la función de NAT de enmascaramiento es la utilización de puertos lógicos, emitidos por la función de NAT de enmascaramiento con el fin de distinguir las diversas corrientes de comunicación. TCP contiene un número de puerto de origen y otro de destino. A estas designaciones, la función de NAT añade un número de puerto lógico.

Proceso de NAT de enmascaramiento de salida:

El mensaje de salida de la figura anterior es un paquete procedente de la LAN privada que va hacia Internet. Los mensajes de salida (de una ubicación local a una externa) contienen el puerto de origen utilizado por la estación de trabajo de la que son originarios. La función de NAT guarda este número y lo sustituye en la cabecera de transporte por un número exclusivo de puerto lógico. En el caso de los datagramas de salida, el número de puerto de origen es el número de puerto local.

1. El proceso de NAT de enmascaramiento de salida supone que todos los paquetes IP que recibe van con rumbo a direcciones IP externas y, por tanto, no realiza ninguna comprobación con objeto de determinar si los paquetes deben direccionarse localmente.

2. El conjunto de números de puerto lógico busca una coincidencia en la capa de transporte, así como la dirección IP de origen y el puerto de origen. Si la encuentra, se sustituye el puerto de origen por el número de puerto lógico correspondiente. Si no se encuentra ningún número de puerto coincidente, se crea uno nuevo, se selecciona un nuevo número de puerto lógico y se sustituye el puerto de origen por éste.

3. Se convierte la dirección IP de origen.

4. A continuación, IP procesa el paquete de la forma habitual y se envía el mismo al sistema externo correcto.

Proceso de NAT de enmascaramiento de entrada (respuesta y otros):

El mensaje de entrada de la figura anterior es un paquete procedente de Internet que va hacia la LAN privada. En el caso de los datagramas de entrada, el número de puerto de destino es el número de puerto local. (En el caso de los mensajes de entrada, el número de puerto de origen es el número de puerto externo. En el caso de los mensajes de salida, el número de puerto de destino es el número de puerto externo).

Los mensajes de respuesta devueltos desde de Internet con rumbo a una máquina conectada localmente tienen un número de puerto lógico asignado por enmascaramiento como número de puerto de destino en la cabecera de la capa de transporte. Los pasos del proceso de entrada de NAT de enmascaramiento son:

1. La función de NAT de enmascaramiento busca en su base de datos el número de puerto lógico (puerto de origen). Si no lo encuentra, se supone que el paquete es un paquete no solicitado y se devuelve al llamador sin efectuar cambio alguno. A continuación, se maneja como si se tratase de un destino desconocido normal.

2. Si se encuentra un número de puerto lógico coincidente, se realiza una comprobación más con objeto de determinar que la dirección IP de origen coincide con la dirección IP de destino de la entrada existente de la tabla de números de puerto lógico. Si coincide, se sustituye el puerto de origen que figura en la cabecera IP por el número de puerto de la máquina local original. Si la comprobación falla, se devuelve el paquete sin efectuar cambio alguno.

3. Se colocan las direcciones IP coincidentes locales en el destino IP del paquete.

4. A continuación, IP o TCP procesa el paquete de la forma habitual y el paquete va a parar a la máquina conectada localmente correcta. Dado que la función de NAT de enmascaramiento necesita un número de puerto lógico para determinar cuáles son las direcciones correctas de los puertos de origen y de destino, no puede manejar los datagramas no solicitados procedentes de Internet.

[Página de presentación de Information Center | Comentarios] [Legal | Glosario de AS/400]