**NAT y Firewall**

Frecuentemente, el cliente y servidor de una conexión de red no tienen una ruta de acceso directa y abierta para la comunicación. Los paquetes se filtran, enrutan, analizan y transforman tanto en los equipos de extremo como en equipos intermedios de la red. Las traducciones de direcciones de red (NATs) y los firewalls son ejemplos comunes de aplicaciones intermedias que pueden participar en la comunicación de redes.

Los transportes de Windows Communication Foundation (WCF) y los patrones de intercambio de mensajes (MEP) reaccionan de manera diferente ante la presencia de NAT y firewalls.

**Cómo afectan las NAT a la comunicación**

NAT se creó para permitir a varios equipos compartir una dirección IP externa única. Una NAT de reasignación de puertos asigna una dirección IP interna y un puerto para una conexión a una dirección IP externa con un nuevo número de puerto. El nuevo número de puerto le permite a la NAT correlacionar el tráfico del retorno con la comunicación original. Muchos usuarios domésticos tienen una dirección IP que solo es enrutable de manera privada y confían en una NAT para que proporcione el enrutamiento global de paquetes.

Una NAT no proporciona un límite de seguridad. Sin embargo, las configuraciones NAT comunes evitan que se direccionen los equipos internos directamente. Esto protege los equipos internos de algunas conexiones no deseadas y dificulta la escritura de aplicaciones de servidor que deben devolver de forma asincrónica datos al cliente. La NAT reescribe las direcciones en paquetes para hacer parecer que se están originando conexiones en el equipo NAT. Esto hace que el servidor obtenga un error al intentar abrir una conexión de vuelta al cliente. Si el servidor utiliza la dirección percibida del cliente, se produce un error porque no se puede enrutar la dirección del cliente públicamente. Si el servidor utiliza la dirección NAT, no puede conectarse porque ninguna aplicación está realizando escuchas en ese equipo.

**Cómo afectan los firewalls a la comunicación**

Un *firewall* es un software o dispositivo de hardware que aplica las reglas al tráfico que pasa para decidir si permitir o negar el paso. Puede configurar los firewalls para examinar secuencias de tráfico entrantes o salientes. El firewall proporciona un límite de seguridad para la red en el borde de la red o en el host del extremo. Los usuarios de empresas han mantenido tradicionalmente sus servidores tras un firewall para evitar ataques malintencionados. Desde la introducción del firewall, el número de usuarios también ha aumentado en gran medida. Esto hace probable que uno o ambos extremos de una conexión tengan un firewall que examine los paquetes.

Los firewalls varían en gran medida en cuanto a su complejidad y capacidad para examinar los paquetes. Los firewalls simples aplican reglas basadas en las direcciones de origen y destino y los puertos en los paquetes. Los firewalls inteligentes también pueden examinar el contenido de paquetes para tomar decisiones. Estos firewalls vienen en muchas configuraciones diferentes y se utilizan a menudo para aplicaciones especializadas.

Una configuración común para un firewall del usuario doméstico consiste en prohibir las conexiones entrantes a menos que se haya realizado una conexión de salida previamente a ese equipo. Una configuración común para un firewall de usuario empresarial consiste en prohibir las conexiones entrantes en todos los puertos exceptuando un grupo identificado específicamente.

**Uso de Teredo**

Teredo es una tecnología de transición IPv6 que habilita la direccionabilidad directa de equipos detrás de una NAT. Teredo se basa en el uso de un servidor que puede ser enrutado públicamente y globalmente para revelar conexiones potenciales. El servidor de Teredo da al servidor y cliente de la aplicación un punto de reunión común en el que pueden intercambiar información de conexión. Los equipos solicitan a continuación una dirección Teredo temporal y los paquetes se pasan mediante túneles a través de la red existente. La compatibilidad de Teredo en WCF requiere la habilitación de la compatibilidad con Teredo e IPv6 en el sistema operativo. Windows XP y los sistemas operativos posteriores admiten Teredo. Windows Vista y los sistemas operativos posteriores admiten IPv6 de forma predeterminada y solo requieren que el usuario habilite Teredo.