Práctica 11 Redes de Computadores: Network Address Translation (NAT)

Kevin Mateo Alvarado Suarez (kevin.alvarado@ucuenca.edu.ec),
Santiago Ariel Armijos Goercke (santiago.armijos@ucuenca.edu.ec),
Raúl Marcelo Ortiz Gaona (raul.ortiz@ucuenca.edu.ec)
Universidad de Cuenca
Redes de Computadores

Resumen

Este informe detalla la implementación exitosa del Protocolo de Traducción de Direcciones de Red (NAT) en una red simulada utilizando el software Cisco Packet Tracer. La práctica se llevó a cabo para abordar la necesidad de conservar direcciones IP públicas y mejorar la seguridad de la red. Se seleccionó e implementó un tipo específico de NAT (Estático, Dinámico o PAT) para cumplir con los objetivos predefinidos. La configuración incluyó la adecuada definición de interfaces y listas de acceso (ACL). Se realizaron pruebas exhaustivas de conectividad y escenarios específicos, destacando la influencia de NAT en las comunicaciones entre redes internas y externas.

I. Introducción

En el siempre dinámico panorama de las redes de computadoras, la gestión eficiente de direcciones IP y la seguridad de la información son imperativos fundamentales. El Protocolo de Traducción de Direcciones de Red (NAT) emerge como una solución clave para abordar la creciente escasez de direcciones IP públicas y para salvaguardar la integridad de las redes. Este informe detalla una práctica llevada a cabo en un entorno simulado mediante el software Cisco Packet Tracer, centrándose en la implementación y configuración de NAT.

La necesidad de optimizar la asignación de direcciones IP y mejorar la seguridad de la red motiva esta exploración de NAT. A medida que las redes evolucionan para adaptarse a un número cada vez mayor de dispositivos conectados, la implementación efectiva de NAT se vuelve crucial para facilitar la conectividad de múltiples dispositivos desde una única dirección IP pública. Este informe proporciona una visión detallada de la topología de red utilizada, la selección del tipo de NAT más adecuado para los objetivos específicos y la configuración detallada en el router principal.

II. Objetivos

1. Conocer el funcionamiento del servicio NAT.
2. Conocer la importancia del servicio NAT.
3. Conocer las ventajas y desventajs del servicio NAT.
4. Simular el uso del servicio NAT.

III. Marco Teórico

III.1. Protocolo NAT

Las direcciones IPv4 están compuestas por 32 bits y tienen la capacidad de generar un total de 4.294.967.296 direcciones. En su concepción, se tenía la certeza de que esta cantidad sería suficiente para asignar una dirección a cada dispositivo en el mundo. Sin embargo, con la explosión de Internet, la demanda aumentó significativamente. A pesar de que el número de direcciones IP disponibles era considerable, no era suficiente para abarcar la cantidad de dispositivos conectados a la red. [1] Ante la evidencia de que la demanda futura no podría ser satisfecha con la cantidad existente de direcciones IP, se implementaron diversas estrategias provisionales [1]:

- Reservar bloques de direcciones (direcciones privadas).
- Emplear direccionamiento sin clase (CIDR).
- Utilizar NAT (Traducción de Dirección de Red).

El protocolo IPv4 permitía que los nodos o hosts se conectaran a Internet utilizando direcciones IP públicas. Cada empresa u organización solicitaba un bloque de direcciones al Registro de Internet Regional (RIR) correspondiente, que asignaba direcciones según sus necesidades. El término ”dirección IP pública”se refiere a aquellas que son enrutables en Internet, no a que puedan ser utilizadas públicamente

sin un contrato previo. Adicionalmente, se empleaban direcciones IP privadas, las cuales no son enrutables en Internet. Por lo tanto, no es necesario solicitar permiso a ninguna entidad para utilizarlas. A diferencia de las direcciones públicas, las privadas se adquieren mediante pago y una solicitud formal a un proveedor de servicios de Internet (ISP) o a un RIR, dependiendo del tamaño de la organización, empresa o hogar que las va a utilizar. [1]

III.1.1. Tipo de NAT: Hay tres categorías de NAT [2]:

- NAT Estático: Convierte una dirección IP privada en una pública, manteniendo siempre la misma dirección IP pública asociada.
- NAT Dinámico: Asigna las direcciones IP privadas al conjunto de direcciones públicas, permitiendo variaciones en la dirección IP pública asignada.
- Traducción de Dirección de Puerto (PAT): Utiliza una única dirección IP pública para todos los dispositivos internos, asignando puertos distintos a cada dirección privada. También conocido como Sobrecarga de NAT (NAT Overload).

III.1.2. Funcionamiento: Se utiliza como una solución provisional ante el agotamiento de direcciones IPv4. Además, contribuye a reducir los costos asociados con la adquisición de direcciones IP públicas, permitiendo la conexión de numerosos dispositivos a Internet mediante una única dirección IP pública. En términos prácticos, cuando un dispositivo desea enviar un paquete a Internet, se sigue un proceso en el que la dirección IP local se traduce a la dirección IP pública antes de salir a la red. A su regreso desde Internet, la dirección IP pública se traduce nuevamente a la dirección IP local mediante NAT. Este proceso puede compararse con una situación cotidiana en la que deseamos comunicarnos con un abogado de un despacho de abogados. Aunque solo tengamos el número público del despacho (IP pública), al marcarlo, interactuamos inicialmente con un secretario (NAT), quien luego nos conecta con el abogado (dispositivo) utilizando el teléfono (router). Es importante señalar que la mayoría de los routers en hogares y empresas en la actualidad emplean NAT, realizando la traducción de direcciones IP privadas a las direcciones IP públicas asignadas por su proveedor de servicios de Internet (ISP) o Registro de Internet Regional (RIR). [1]

III.2. Ventajas y desventajas de NAT

Las beneficios más notables de NAT incluyen [1]:

- Conservación de direcciones IPv4: Facilita la conexión de múltiples dispositivos a Internet mediante una única dirección pública, contribuyendo al ahorro de direcciones IPv4.
- Configuración sencilla: Por lo general, su configuración es simple y directa.
- Mantenimiento mínimo: Requiere un mantenimiento mínimo, limitándose principalmente a la modificación de la tabla de reenvío del router.
- Capa de seguridad adicional: Ofrece una capa de seguridad al hacer que los dispositivos de la red local no sean visibles desde el exterior, especialmente en el caso de NAT estático.
- Mejora de la flexibilidad y confiabilidad: Aumenta la flexibilidad y confiabilidad de las conexiones mediante el uso de grupos.
- Compatibilidad con diversos protocolos: Es compatible con la mayoría de los protocolos de comunicación, destacándose en particular con los ampliamente utilizados, como TCP y UDP.

A continuación se describen las desventajas [1]:

- Requerimientos de procesamiento del router: Puede exigir más potencia de procesamiento por parte del router.
- Posible deterioro del rendimiento: El rendimiento puede degradarse, dando lugar a un aumento en la latencia (”lag”).
- Incompatibilidad con ciertos protocolos: Algunos protocolos de capas superiores, como ICM, son incompatibles con NAT.
- Reducción del seguimiento IP de extremo a extremo: Disminuye la capacidad de realizar un seguimiento IP completo desde el origen hasta el destino.
- Complejidad en la resolución remota de problemas: La resolución remota de problemas puede volverse más compleja cuando es necesaria.
- Posibles problemas con juegos online: Puede causar complicaciones en los juegos en línea, ya que estos requieren un ancho de banda y una latencia óptimos.

III.3. Listas de Acceso

Una Lista de Control de Acceso (ACL) de red regula y decide si permitir o denegar el flujo de tráfico específico tanto entrante como saliente a nivel de subred en una VPC. Puede optar por utilizar la ACL de red predeterminada de su VPC o crear una personalizada con reglas similares a las de sus grupos de seguridad, agregando así una capa adicional de seguridad. [3]

Existen dos tipos comunes de listas de acceso asociadas con NAT [3]:

- Lista de Acceso Estándar (Standard Access List): Estas listas de acceso permiten o deniegan el tráfico basándose únicamente en la dirección IP de origen. Son más simples y se aplican a todo el tráfico que coincide con la dirección IP especificada.
- Lista de Acceso Extendida (Extended Access List): Estas listas de acceso ofrecen una mayor granularidad al permitir la definición de condiciones basadas en varios factores, como la dirección IP de origen y destino, el número de puerto, el tipo de protocolo, entre otros. Proporcionan un control más detallado sobre qué tráfico se traduce mediante NAT.

Las listas de acceso del protocolo NAT permiten al administrador de red especificar qué tráfico debe someterse a la traducción de direcciones y cuál debe ser excluido. Estas reglas son cruciales para gestionar el flujo de datos a través del enrutador que realiza la traducción de direcciones, garantizando que se aplique NAT de manera selectiva según las necesidades y políticas de la red. La configuración precisa de las listas de acceso del protocolo NAT es esencial para lograr un control efectivo sobre la asignación de direcciones IP y la seguridad de la red. [3]

IV. Desarrollo

IV.1. Explicación de la Práctica

Se necesita establecer comunicación entre las 2 diferentes redes LAN con un servidor con dirección IP publica, para esto se hará uso de Network Address Translation (NAT).

IV.2. Disposición de los dispositivos

Se conectó un router a cada uno de los switches mediante un cable de par trenzado directo. Luego, se procedió a conectar dos computadoras en 2 de los switches y un servidor en el switch restante, totalizando 3 switches, 4 computadoras, 1 servidor y 2 laptops. Este paso se realizó con el propósito de configurar cada dispositivo a través de la consola, facilitando así la posterior prueba de comunicación en la red. A continuación se muestra la disposición de estos dispositivos.

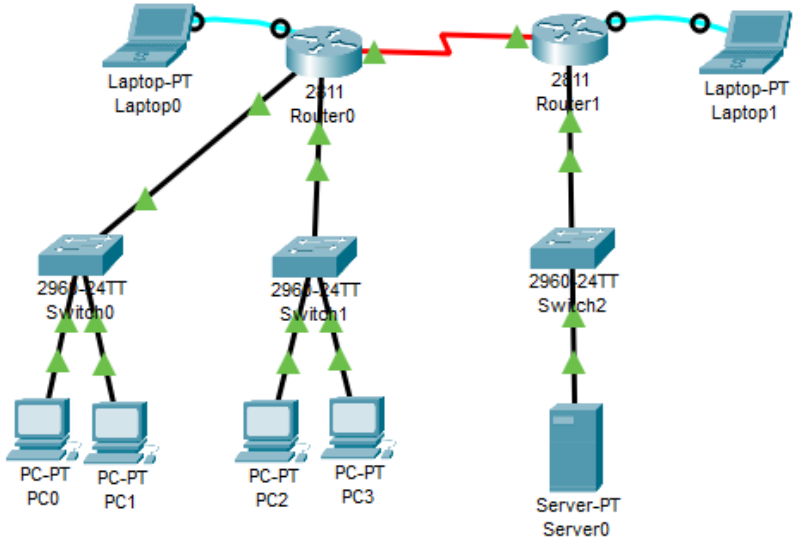

Figura 1: Disposición Dispositivos.

IV.3. Programación Router (NAT)

A continuación se muestras los comandos usados en esta sección:

Router 0 (Redes LAN)

```
Router(config)#access-list 1 permit 192.168.0.0 0.0.0.255
Router(config)#ip nat inside source list 1 interface serial 0/0/0 overload
Router(config)#interface fastethernet 0/0
Router(config-if)#ip nat inside
Router(config-if)#ip address 192.168.0.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit

Router(config)#access-list 2 permit 172.31.0.0 0.0.0.255
Router(config)#ip nat inside source list 2 interface serial 0/0/0 overload
Router(config)#interface fastethernet 0/1
Router(config-if)#ip nat inside
Router(config-if)#ip address 172.31.0.1 255.255.0.0
Router(config-if)#no shutdown
Router(config-if)#exit

Router(config)#interface serial 0/0/0
Router(config-if)#ip nat outside
Router(config-if)#ip address 150.1.0.1 255.255.0.0
Router(config-if)#exit
```

Router 1 (Servidor)

```
Router(config)#interface fastethernet 0/0
Router(config-if)#ip address 172.100.0.1 255.255.0.0
Router(config-if)#no shutdown
Router(config-if)#exit

Router(config)#interface serial 0/0/0
Router(config-if)#ip address 150.1.0.2 255.255.0.0
Router(config-if)#no shutdown
Router(config-if)#exit
```

IV.4. Programación Router (Tablas de Enrutamiento (RIP))

Para la configuración del protocolo RIP en cada uno de los routers se utilizo la siguiente serie de comandos:

Router 0 (Redes LAN)

```
Router(config)#router rip
Router(config-router)#version 2
Router(config-router)#no auto summary
Router(config-router)#network 150.1.0.0
Router(config-router)#network 192.168.0.0
Router(config-router)#network 172.31.0.0
Router(config-router)#exit
```

Router 1 (Servidor)

```
Router(config)#router rip
Router(config-router)#version 2
Router(config-router)#no auto summary
Router(config-router)#network 150.1.0.0
Router(config-router)#network 172.100.0.0
Router(config-router)#exit
```

IV.5. Configuración de las direcciones IP, máscaras de red y Gateway a cada dispositivo

Por ultimo, toca configurar cada uno de los dispositivos LAN (computadoras de escritorio) con una IP, mascara de red y Gateway correspondiente.

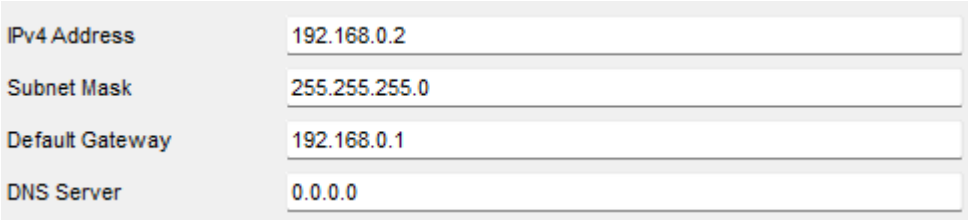

Figura 2: Configuración Dispositivo LAN 1.

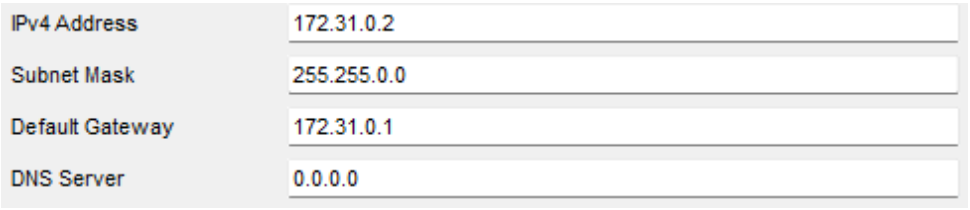

Figura 3: Configuración Dispositivo LAN 2.

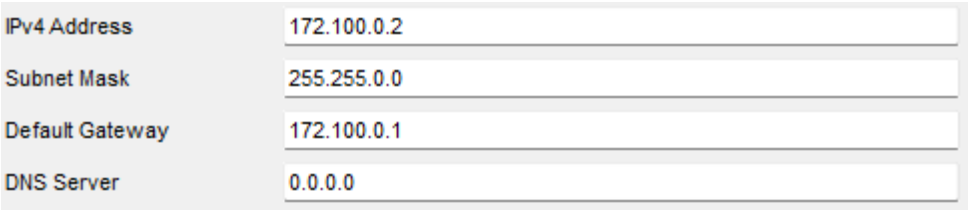

Figura 4: Configuración Dispositivo Servidor.

IV.6. Diseño final de la red

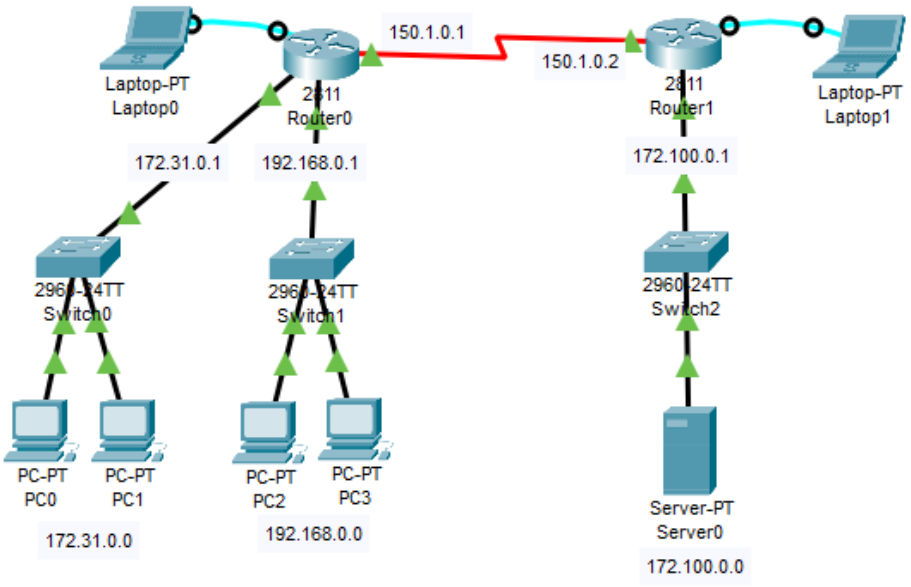

Figura 5: Diseño Final de la Red

IV.7. Pruebas de comunicación

```
C:\>ping 172.100.0.2

Pinging 172.100.0.2 with 32 bytes of data:

Reply from 172.100.0.2: bytes=32 time=1ms TTL=126
Reply from 172.100.0.2: bytes=32 time=2ms TTL=126
Reply from 172.100.0.2: bytes=32 time=2ms TTL=126
Reply from 172.100.0.2: bytes=32 time=1ms TTL=126

Ping statistics for 172.100.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

Figura 6: Comunicación LAN 1 - Servidor

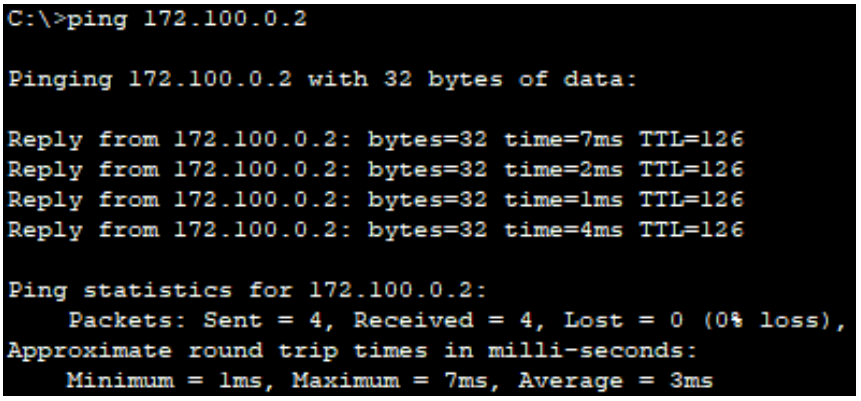

Figura 7: Comunicación LAN 2 - Servidor

V. Conclusiones

La exploración de las Listas de Control de Acceso (ACL) de red en el contexto de las Virtual Private Clouds (VPC) revela su papel fundamental en fortalecer la seguridad y gestionar el flujo de tráfico. La incorporación de ACL de red proporciona una capa adicional de seguridad, permitiendo una personalización detallada de las reglas para adaptarse a las necesidades específicas de la red. La coordinación eficaz entre ACL de red y grupos de seguridad ofrece un enfoque integral para la gestión de la seguridad en la VPC, asegurando un control preciso sobre las comunicaciones. La ausencia de costos adicionales refuerza la atractiva naturaleza de esta herramienta como un medio rentable para mejorar la infraestructura de red. El diagrama presentado ilustra la función esencial de las ACL de red al regular el tráfico entre subredes, subrayando su importancia en la arquitectura de red. En resumen, la implementación estratégica de ACL de red emerge como un componente esencial para optimizar la seguridad y la eficiencia en entornos de VPC.

Referencias

[1] “NAT: Qué es y para qué sirve,” Jun. 2022. [Online]. Available: https://openwebinars.net/blog/nat-que-es-y-para-que-sirve/
[2] weimar.gutierrez@zohocorp.com, “¿Qué es NAT y cómo funciona?” Mar. 2023. [Online]. Available: https://blogs.manageengine.com/espanol/2023/03/11/nat-como-funciona.html
[3] “Controlar el tráfico hacia las subredes utilizando las ACL de red - Amazon Virtual Private Cloud.” [Online]. Available: https://docs.aws.amazon.com/es_es/vpc/latest/userguide/vpc-network-acls.html#nacl-basics