SNAT/MASQUERADE

- NAT involves re-writing the source and/or destination addresses of IP packets as they pass through a router or firewall.
- **SNAT replaces** the private IP address from the packet with the public IP address of the router external interface.
- Netfilter framework enables a Linux machine with an appropriate number of network cards (interfaces) to become a router capable of NAT.
- SNAT uses the nat table and the POSTROUTING chain.
- MASQUERADE is a special case of SNAT used when the public IP address of the NAT Router is dynamic. It will automatically use the IP address of the outgoing network interface for network translation.
- When uses SNAT or MASQUERADE the netfilter also performs port address translation (PAT) on the packet.

SNAT/MASQUERADE

Configuration:

1. Enable the routing process

A. echo "1" > /proc/sys/net/ipv4/ip_forward

or

B. Edit /etc/sysctl.conf add net.ipv4.ip_forward= 1 and **restart the network service** (systemctl restart networking on Ubuntu & Debian based distributions)

2. Add iptables rules to **nat table** and **PREROUTING chain** that match packets that should be NATed, specify the external interface using **-o** option and use **-j SNAT --to-source public_ip_address** or **-j MASQUERADE targets**

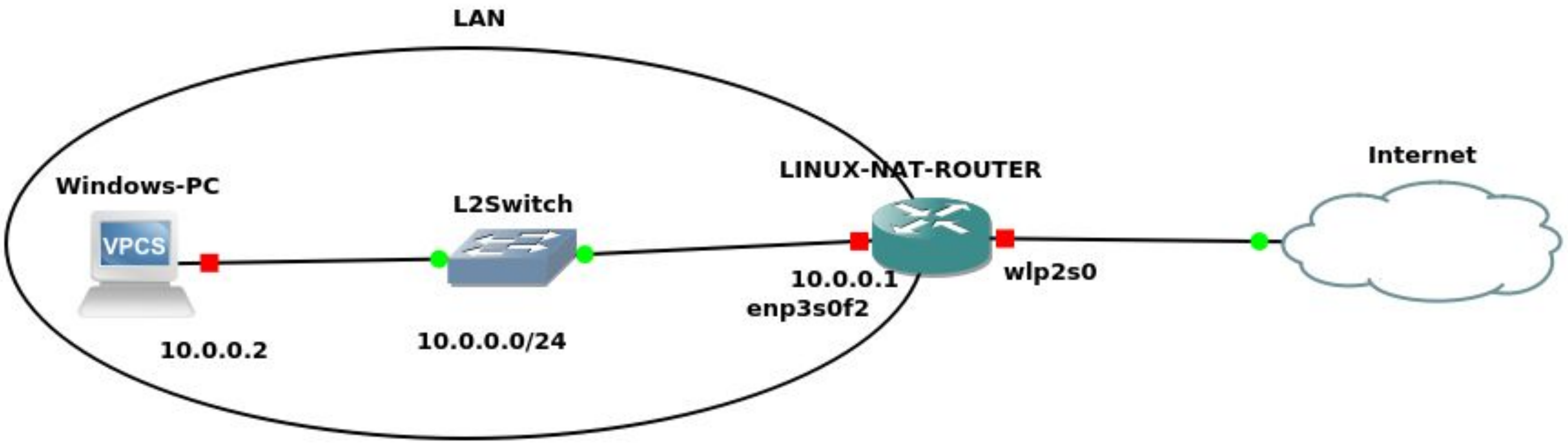
Example:

```
echo "1" > /proc/sys/net/ipv4/ip_forward
iptables -t nat -A POSTROUTING -s 10.0.0.0/24 -o eth0 -j SNAT --to-source 80.0.0.1
```

or

```
iptables -t nat -A POSTROUTING -s 10.0.0.0/24 -o eth0 -j MASQUERADE
```

NAT/MASQUERADE



Configuration:

1. Enable routing on Linux NAT Router
2. Define iptables rules that match NAT traffic and use -j SNAT --to-source IP or -j MASQUERADE targets

DNAT(Port Forwarding)

- Permits connections from the Internet to servers with private IP addresses inside LAN

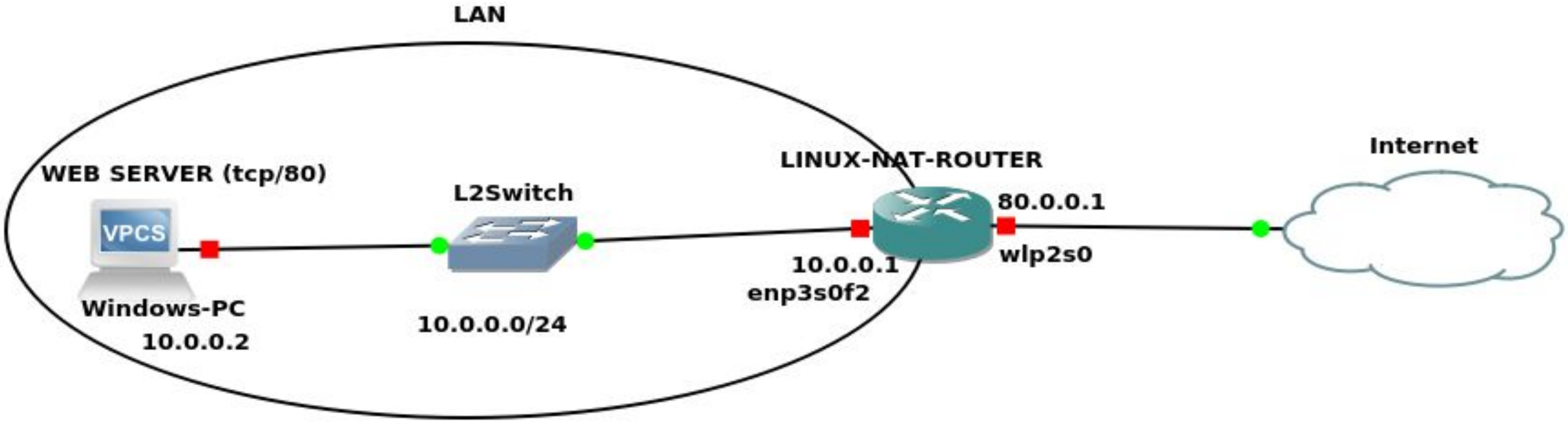
- The client connects to the public IP address of the DNAT Router which in turn redirects traffic to the private server

- The server with the private IP address stays invisible

- DNAT uses nat table and PREROUTING chain

- Target used is -j DNAT --to-destination *private_ip_address*

DNAT(Port Forwarding)



Configuration:

1. It’s assumed that SNAT is already configured for traffic generated from the LAN server to the Internet
2. Define the iptables rule that matches traffic that comes from the Internet and use -j DNAT --to-destination LAN_SERVER_IP target