Introduction

Most Internet Service Providers are now operating carrier-grade Network Address (and Port) Translators (NAT/NAPT) in restricted mode: barring downstream traffic from Internet hosts unless upstream traffic was previously sent to them. The user device obtains a **private** IP address, which is translated to a public IP address (and port block) on the external side of the carrier-grade NA(P)T.

However, it is only a minority of ISPs who also operate a Stateful Firewall for user equipment (gateways, cable modems or other customer premises equipment) to which **public** IPv4 addresses or IPv6 addresses are assigned. Similar to a restricted NA(P)T, a stateful firewall protects the equipment by preventing internet-initiated traffic to reach it.

A NA(PT) can also be found inside today's user equipment. It shields the Local Area Network (LAN) from the internet when a public IP address is granted to the user equipment and when the ISP operates no stateful firewall.

The pitfalls with public IP addresses on gateways

Attacking the gateway

Unless the ISP operates a stateful firewall, any gateway with a public IP address is directly exposed to attacks, like for example DDOS and port scanning. That means that measures have to be taken by the gateways that has limited processing power and a lower memory footprint to mitigate those attacks . If the gateway gets attacked, it will not be able to function properly anymore.

Fixed IP address

Another disadvantage is that the public IP address is usually granted for a long period (fixed) so once the attacker knows the address , it can concentrate his attack on this gateway. The impact can be twofold:

- Because of the constant flooding the gateway is no longer accessible and able to perform normally. This could lead to possible blackmail by the attacker to give up his attacks.
- Secondly, the attacker could try to enter the gateway by scanning for open ports, exploiting any OS weakness and cracking the password.

Weak passwords

With a public IP address, the first line of defense is to block the access to the gateway. That is normally enforced with a strong password. In some cases, people forget to change the default password or choose a password that is not hard to guess. This leads to direct access to the gateway and all its information and functions.

Data protection

All traffic needs to be encrypted to ensure that nobody is able to eavesdrop and read the data. This requires that the security mechanisms for secure communication with the outside world should already be in place much in the same way as required for a VPN tunnel. All information exchange between the devices and your platform should be secured, even the operator providing the connectivity service should not be able to read your data.

Solution

The most pragmatic solution is to work with private IPv4 addresses) and let each gateway set up a VPN tunnel that allows secure access and communication over the public internet (IPSec or SSL tunnel through the NAPT). The operator can provide a first line of defense for your devices by hiding them from the outside world and only allowing outbound traffic. This reduces the exposure to DDOS and other attacks.

Secondly the VPN tunnel will allow secure end-to-end two-way communication (privacy and integrity) between your devices and your platform, even though the devices have an *outer* private IPv4 address assigned. Within the VPN tunnel each device can be assigned a second (private) IPv4 address and/or IPv6 prefix: the *inner* IP address, in the same subnet as your platform.

Another advantage is that the solution is operator independent, which prevents an operator lock-in and allows you to negotiate the best possible deals for your data communication. For example, it is easy to replace or complement the fixed broadband connection with mobile (4G LTE) access.