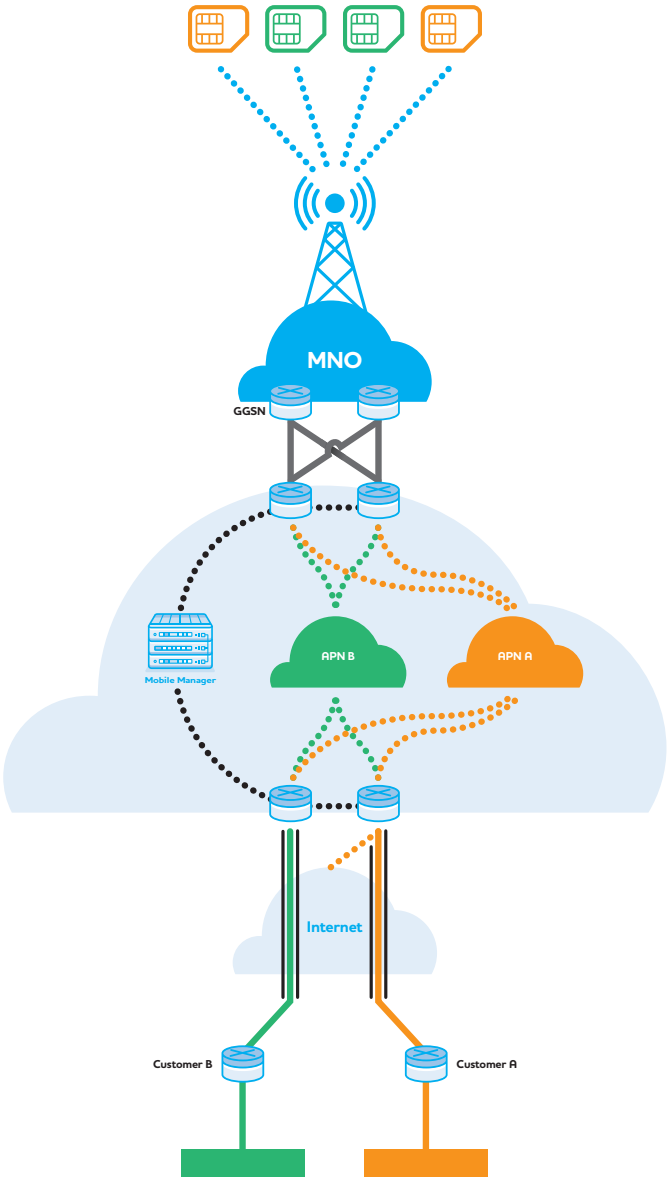


Example Solution A

Access to the Internet with remote access to the device

In this example the customer application needs SIMs that connect to the Internet, but they also need to be able to remotely connect to the devices for admin purposes. Traditionally, there are two ways to achieve this:

Mobile Broadband VPN

Use standard SIMs in a VPN capable router and then configure a VPN tunnel from every remote device to a central firewall. Internet traffic would route out via the Mobile Operators public APN and remote access to the the devices could be achieved via the VPN tunnel. The problem with this solution is that mobile routers with VPN capability are more expensive than standard mobile routers and there is a reasonable amount of time required to properly configure all the VPN tunnels.

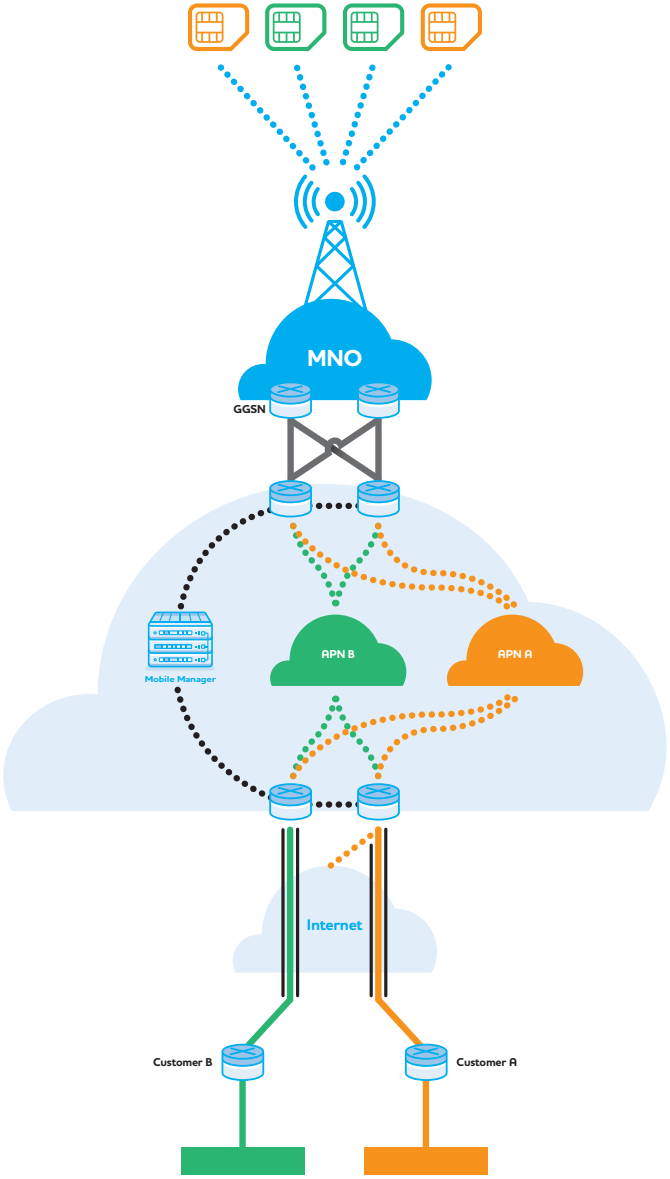
Static IP SIMs

These SIMs include a static public IP address as standard. They provide access to the Internet and using the static public IP address can be directly connected to from anywhere on the Internet without the need for a complex VPN setup. The problem with this solution is that the remote devices are open to attack from the Internet and require very careful configuration to avoid being hacked. It is very common for static IP SIMs to be hacked. Also, static IP SIMs cost more than normal Mobile Broadband SIMs as IPv4 Internet addresses are scarce and therefore valuable.

Our recommended solution in this scenario would be to use a private APN with central Internet breakout and an IPSec tunnel. This would allow the SIMs to access the Internet via the centrally hosted Internet Breakout whilst also allowing the customer to directly connect to any of the SIMs via the single VPN tunnel. All traffic in and out would also automatically benefit from Cloudflare DDOS protection.

In this diagram the orange SIMs will be able to access anything on the Internet via the Internet breakout and anything on the orange Customer A LAN via the IPsec tunnel.

Anything on the orange Customer A LAN will also be able to access any device that has an orange SIM installed in it.



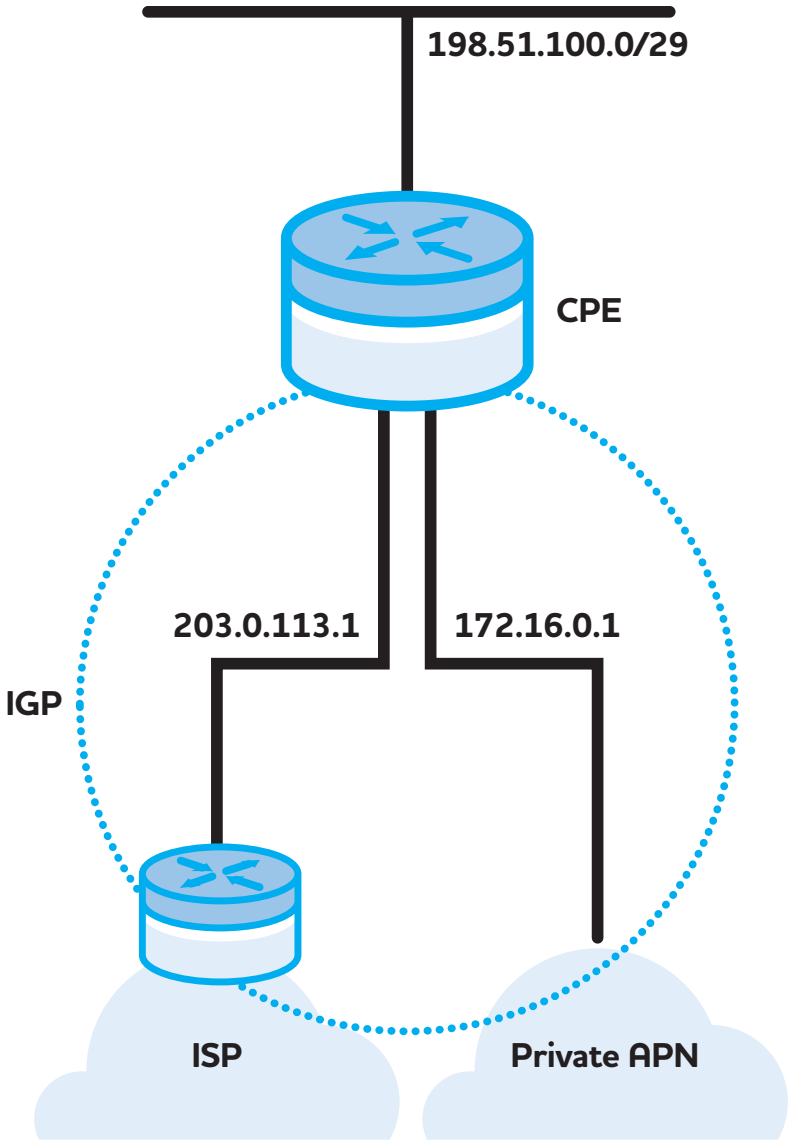
Example Solution B

Private network with no access to the Internet

In this example the customer application is hosted on a private network and devices need to access this application without needing any Internet access at all. Traditionally this would require a Private APN to be supplied directly by an MNO directly. The problem with this solution is that MNOs often charge hefty upfront and ongoing charges to setup a private APN and lead times of 3-6 months are not unheard of. Also, having a Private APN directly with an MNO means you're committed to that MNO in the long term, if one of your sites doesn't happen to have a good signal with that MNO, what then?

Our recommended solution would be to take Jola Private APN with an IPSec tunnel and don't choose the Internet breakout option. The APN will be available within 2 working days and once established, SIMs can be added and removed from the solution within seconds. All traffic in and out would also automatically benefit from Cloudflare DDOS protection.

In the diagram below, the green SIMs will be able to directly access anything on the green Customer B LAN and anything on the Customer B LAN will be able to directly access the device that has the green SIM installed in it. All without any direct access to the Internet possible from or to the SIM.



Example Solution C

ISP Backup with single CPE and BGP

In this example an ISP wants to provide a 4G backup service for a fixed line Internet access service such as a leased line or broadband circuit. If the primary connectivity fails, then the traffic should flow via the mobile network and the customer should continue to be able to access the Internet and be reachable via their ISP issued static IP address. The Jola and MNO infrastructure is the same for this solution as the previous examples, so the diagram below is simplified to provide more detail about the end-to-end solution.

The example shows a single piece of customer CPE with an Ethernet WAN interface and a cellular WAN interface. The customer subnet is 198.51.100.0/29 and point-to-point Ethernet WAN interface has the address 203.0.113.1 and the point-to-point cellular interface has the address 172.16.0.1.

An IGP routing protocol (commonly BGP or OSPF) is being used between the CPE and the ISP network. The ISP would therefore be receiving two alternative routes for the same customer subnet. The ISP could use various techniques to prefer the Ethernet route with the end-result that the cellular route would only be used if that primary route no longer existed due to the primary connectivity failing.

The CPE would be responsible for detecting the failure of the primary WAN access and routing everything via the cellular interface, however the IGP could play a part here also if the ISP advertised a default route.

The same solution could be used to provide cellular backup for Internet access services or for private WAN services such as MPLS.