Use case 3: a Swiss organisation with locations abroad

A Swiss organisation needs to exchange business oriented traffic with its foreign locations. Some of its applications are latency sensitive (voice, video, VDI...), some are bandwidth intensive (application or security updates, e-learning...) and some have no specific needs (emails, CRM, HR...) but are sensitive. They are hosted either in a private Datacenter, or in the cloud. Classically, organisations have two options for their WAN:

1. Using the public internet as a transport for encrypted tunnels, like an IP VPN
2. Building an international private network, like a VPN MPLS

(Note: or a combination of both with SD-WAN)

Public versus private networks is a dilemma hard to overcome in B2B networking.

International private networks are robust, efficient and secure, but they are relatively expensive, tedious to deploy and upgrade, not flexible, nor pervasive. Most of these problems result from the limited footprint of service providers (SPs) via their own infrastructure. Thus, to offer a global reach, most of the SPs are partnering with global telcos which are also in partnership with local loop providers in each country. The number of intermediaries leads to latency in processing and margin stacking.

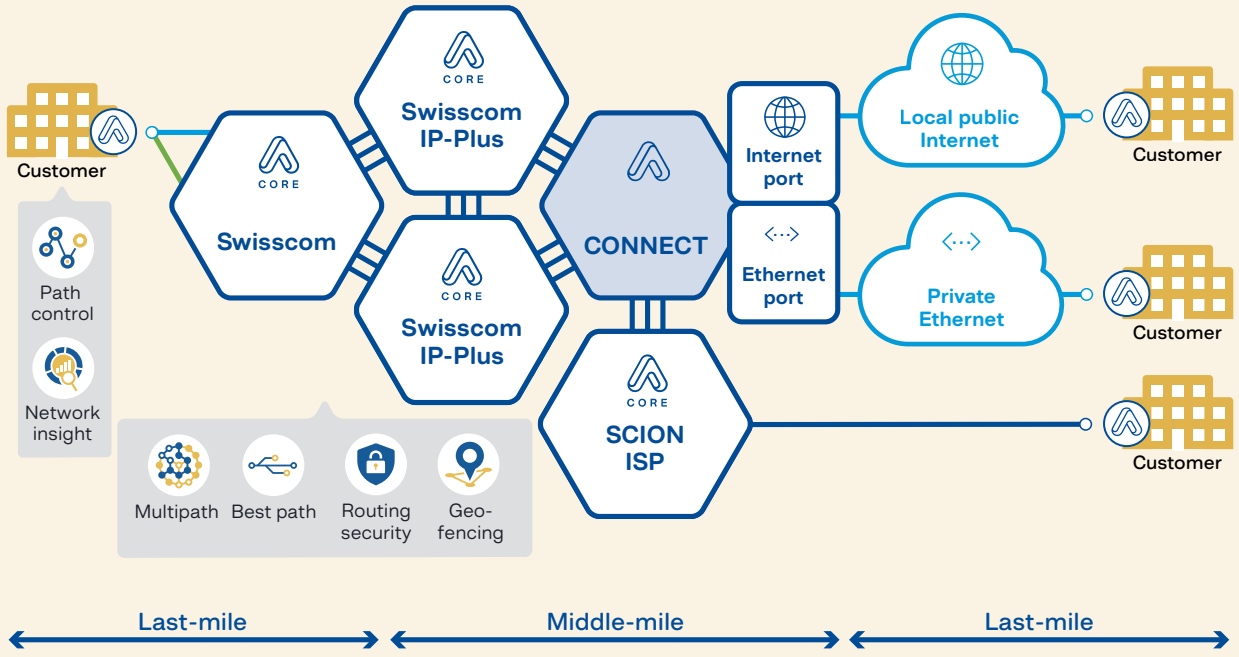
On the other hand, the public internet is a flexible, ubiquitous and cost effective alternative. But, in addition to the security concerns overseen in the previous use case, international contexts emphasize the internet's so-called "middle-mile problem". Risks of traffic hijacking, poor performance or important variations, convergence time, sensitive traffic transported via untrusted carriers or areas are amplified issues due to long-distance connections.

Solving the middle-mile problem with the next-generation internet

The SCION-Internet brings concrete solutions to the middle-mile problem on a **public network**. We already mentioned that the protocol offers increased **business continuity** and **trust in the network**, thanks to its **verifiability** and **sovereignty**.

In addition to these already compelling advantages it offers:

Routing security	thanks to the cryptographic authentication of all segments composing a path, the next-generation internet is immune to routing attacks, such as BGP hijacking
A real end-to-end path control	organisations can choose in which jurisdictions their traffic should stay, for compliance reasons, or simply avoid, to reduce the risks in untrusted areas (geofencing)
Application-specific performance optimisation	the sender can choose the paths that correspond to its real needs. Going from Bern to Sydney: use the shortest paths going through the Suez Canal for videoconferencing and the cheapest one going through the USA for the application update
More stability	multiple paths are possible: the EDGE is constantly monitoring which is the most efficient and can switch without packet loss: you also optimise the stability of your network metrics at long distance.
No more **convergence time**	in case of node failure, also thanks to multipathing and fast-failover
Deeper network insights	as you have a view on all the segments you go through, you can identify where the problems come from beyond the first hop



How to benefit from the SCION-Internet outside Switzerland?

Outside Switzerland, as of mid-2020, this next-generation internet is present in more than 10 countries in Europe and Asia, and extensions are planned, including in the Middle-East and in North America. In these regions as for Switzerland, you can benefit from its unique properties by joining through a last-mile connection to the closest enabled Point of Presence (POP) complemented with an EDGE.

Last-mile connections are mainly depending on the level of security expected and on your location:

- The most common option to hook-up via an internet-access: a tunnel is built to the closest POP.
- You can also acquire a private circuit (e.g. ethernet line) from any local network operator to the closest POP. As gateways are present in an important number of carrier-neutral data centres, this option is usually a good compromise between security and costs.
- In some countries network service providers (like Swisscom in Switzerland) are offering SCION-native accesses: it means that you are part of the SCION-Internet at the floor of your building!

Outside Switzerland, Swisscom benefits from its **highly performant IP Plus backbone,** present in the key cities in Europe, Asia-Pacific, Americas, Middle-East and Africa. This backbone is designed to allow peering with other ISPs and provide a highly secure SCION connectivity, where SCION POPs are already rolled-out.

The combination of Swisscom's IP Plus backbone and Anapaya's technology, allows Swisscom to offer its customers an optimal latency on international connections, a fast access to Swisscom owned secure infrastructure and to secure connectivity for international business communications.

Internationally, Swisscom can provide different types of Managed Services:

- **Full bundled services**
  In order to allow the customer to focus on its business, Swisscom can take ownership for all the components of the solution, from acquiring local access to fully managing the EDGE devices and providing an end-to-end SLA.
- **Flexible services**
  Customers can decide to procure local access and/or manage the EDGE devices by themselves.