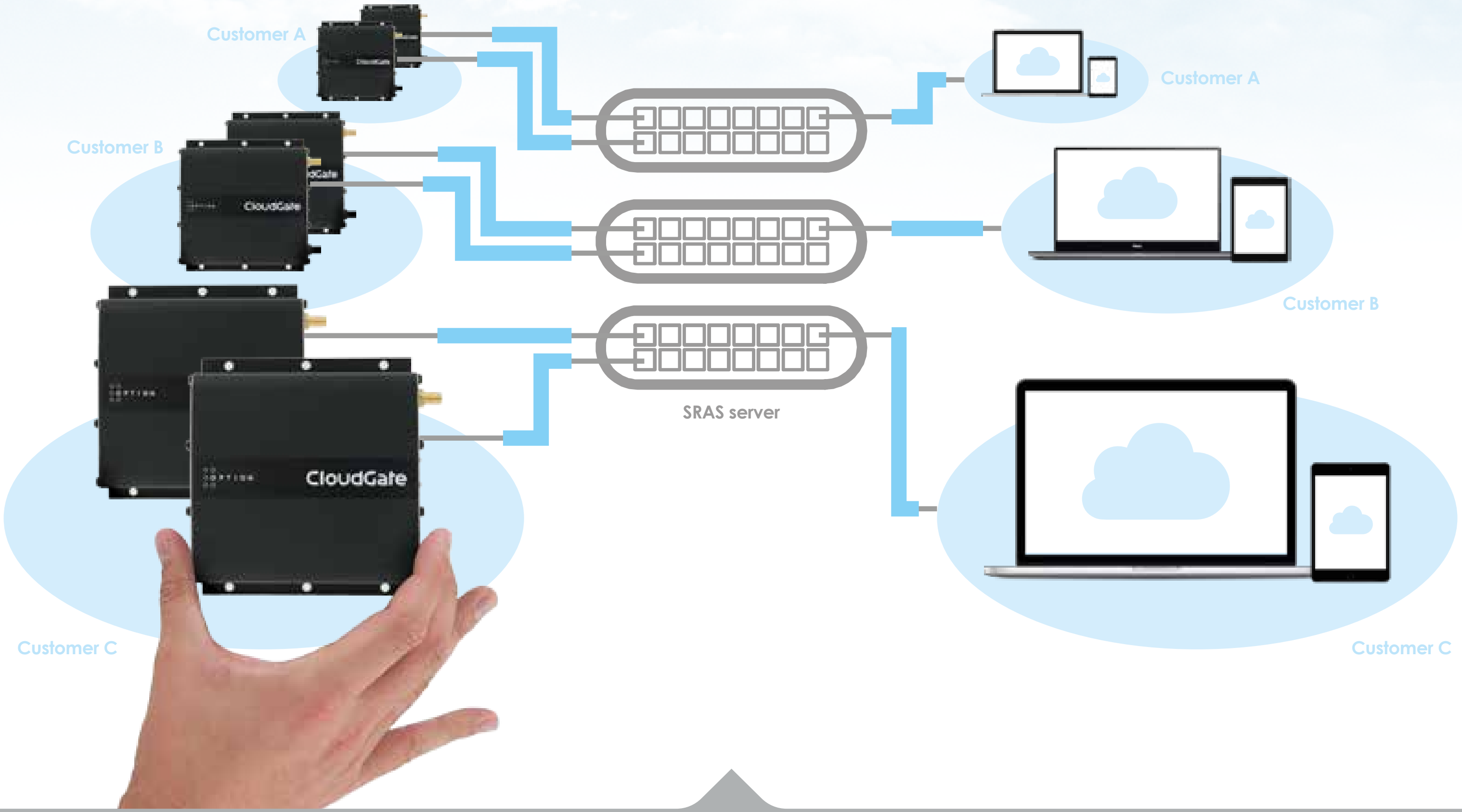
SRAS

SECURE REMOTE ACCESS SERVICE



BACKGROUND
The demand for secure remote access is growing rapidly driven by the new wave of Internet of Things. More and more systems are automated and require maintenance, troubleshooting, upgrades and remote access in a secure way. It is no longer economically viable to physically go onsite and connect locally to perform these tasks. This is especially true in case of control systems that are deployed in large numbers and only require access on an occasional basis.

CURRENT VPN SOLUTIONS:
Every remote access solution requires three components, the client on the connecting system, the server and the client on the remote device. The VPN server will connect both sides (tunnels) of the client together to allow remote access. A number of challenges are associated with the current solutions:

On the user client side:
For the most solutions dedicated clients are required. This implies that for different operating systems (Linux, MAC, Windows) and devices (iOS, PC, Android) dedicated clients need to be available and maintained, including support for different operating systems flavours and versions. Moreover the setup of such clients is not always straightforward and requires a fair amount of technical knowledge/support.

The server side:
A permanent tunnel is created from the remote device to the VPN server as most devices have connections that do not have a publically accessible IP address and are therefore not directly reachable (they receive a private IP address and are behind NAT/NAPT). Maintaining a permanent VPN tunnel to the VPN server requires high-end, dedicated server hardware (VPN concentrator) and makes the solution complex and expensive. Also, to connect different customers (multi-tenant support) and ensure clear network separation, a complex network setup is required.

The remote device:
The remote device is permanently connected to the VPN server (as explained in the previous point). The traffic associated to keep the VPN tunnel open can be large especially in mobile networks.

OPTION

SRAS
SECURE REMOTE ACCESS SERVICE

INTRODUCTION

The Option SRAS service provides a complete solution that removes most of the restrictions imposed by current solutions and adds simplicity. The Option Cloudgate™ gateway connects to the SRAS server over mobile (LTE, 3G, 2G), fixed or WiFi networks.

- The gateway can create VPN tunnels upon request from the server and does not need a permanent VPN tunnel. This reduces the data traffic associated with secure remote access.
- Access to the devices behind the gateway within the same LAN is possible simply by configuring the forwarding rules to the devices you want to access. (e.g. Cameras, PLCs, etc). This allows simple yet secure access to remote devices.
- Each user gets access to multiple devices available via the same client tunnel simplifying connectivity and avoiding wasted time switching between managed devices.
- The server solution is completely virtualised, can be hosted in the cloud and does not require any dedicated hardware. The cost of the solution scales in a linear fashion depending on number of clients. There are no "step-up" costs at any number of clients. This allows for predictable costs, quick setup and limited management overhead.
- The management portal gives an overview of the gateways with their connection status. The portal supports multi-tenancy where super-accounts have access to all sub account devices. This allows resellers selling support services to have simple access to all customer devices while maintaining security.
- The setup and teardown of the VPN tunnel from the gateway can be controlled via the portal reducing data consumption.
- In the detailed view, the user can access the gateway with just one click on the link that takes them to the landing page of the gateway.
- The forwarding rules configured on the gateway are synchronized with the management portal so that all the devices behind the gateway are also reachable in the same way.
- The built-in VPN client of most popular Operating Systems like Windows, Mac and Linux but also iPad and Android devices is used to setup the VPN tunnel to the server. Once the connection is established, full access to all devices is available, just one click away. No special VPN software is required on any client device.

Whether you only need remote access to one device, or need support for access to hundreds of devices, the solution is the same. Different deployment options are available based on the customer requirements for security, latency, price and availability.

The following choices can be made:

- Publicly hosted Cloud solution (dedicated solution on shared infrastructure)
- Public hosted solution with data center chosen by the customer with optionally dedicated virtual machine(s)
- Privately hosted solution on customer premise (only available for larger quantities and subject to setup)

This solution is attractive to:

- Customers who need an affordable, easy VPN solution
- Service providers willing to offer a cloud-based solution instead of investing in large VPN concentrators.
- Value Added distributors willing to offer end-to-end solutions and services.

TRADITIONAL CUSTOMER BENEFITS	OPTION CUSTOMER BENEFITS
Dedicated VPN clients increase operational costs, limit OS and device support and require updates and maintenance.	Leverages built-in clients of major OS suppliers and device manufacturers which makes live cycle management much easier, robust and cost effective.
Permanent VPN tunnels consume bandwidth and require termination on the network side	Tunnel established when needed avoids connection charges and allows for more efficient network setup.
Upfront investments and operational cost incurred in line with forecasted capacity and size.	Flexible scaling on-the-fly achieved through full virtualisation and de-duplication of the solution.
Significant rollout effort and cost to setup and configure each device.	Self provisioning and support for bulk device provisioning via Webbased UI.
IP addressing knowledge required to connect to target device.	Full Qualified Domain Names used to obtain access to the device.
	Multi-tier support allowing users and groups access to devices based on permissions.
	Solution hosted by a public hosting provider in a shared or dedicated setup, a public hosting provider chosen by the customer or privately hosted(subject to conditions).