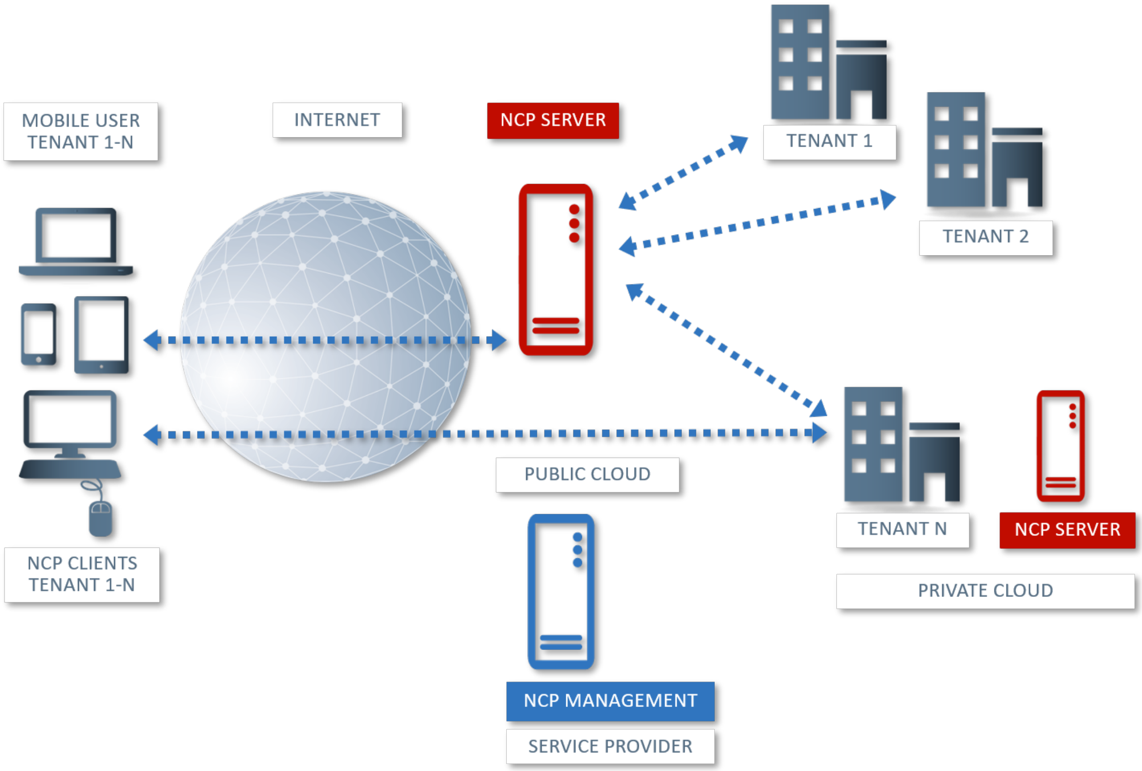
Multi-tenancy

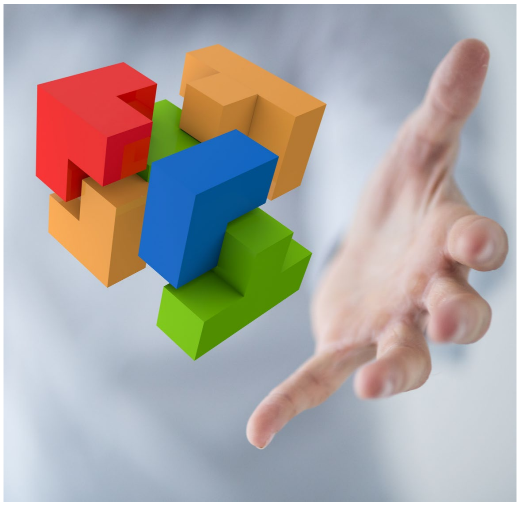
– an often underestimated remote access feature

Multi-tenancy refers to an architecture in which a single software application can be used by several customers without access to each other's data – the idea behind this is maximizing resources. Companies can optimize their hardware and software utilization with multi-tenancy solutions. The NCP Secure Enterprise Solution has full multi-tenancy support. But what is so special about multi-tenancy?

Colocation data centers, virtualization and middleware sharing are some examples of sharing resources with similar goals of reducing costs while maximizing efficiency. What distinguishes multi-tenancy is its effectiveness in achieving the same goals in a scalable and efficient way.

Enterprises, hosting providers or managed security service providers can choose from a wide range of products and implementation options to offer a VPN service. In any case, it is important that the solution used and its gateways support multi-tenancy. This allows different customers to be served separately across physical or virtual systems. Due to the high load requirements that an arise when hosting many





thousands of VPN tunnels, the gateways be scalable and support load balancing. The NCP Management Console can handle multiple gateways per customer as well as separate customers and supports both the vendor's processes and the customer's security needs. Whether they accept a shared VPN gateway or require a separate solution is determined by the customer's security concept. VPN cloud providers can usually deliver both.

Multi-tenancy means that the user accounts and transferred data of one customer are not visible to other customers on the same VPN gateway. Here a well thought-out and practice-oriented management strategy benefits customers in two ways: Customers can easily perform basic management tasks on the hosted virtual VPN gateway without employing a specialist. And the operator is given an easy way to bill for the service, monitor service levels and still guarantee a high level of security for their customers.

There are no limits to the size and complexity of client networks for NCP's solution. High availability services ensure maximum uptime. Geographically distributed redundant systems are easy to implement.

IT administrators can also benefit from multi-tenancy, especially in the IIoT environment. Companies can only access their own production sites and organizational units – access to external and protected areas is denied. Specific access rights can be granted for different support levels with minimal effort – Administrators can either be assigned special or department-related rights.

About NCP

Since it was founded in 1986, NCP has been developing universally applicable software components enabling end devices to connect to the corporate network easily and securely via public networks with a fully automated central remote access VPN management. NCP's Secure Communication Products are made for many different scenarios e.g. mobility, M2M, IoT and classic VPN scenarios.