SASE, Zero Trust, SD-WAN, Cloud ...
Modern VPN with maximum flexibility and the greatest security

In recent years, the cloud has helped IT security networks prepare for digital transformation in a flexible way. Although the trend has ventured away from classic and trusted IT solutions, cloud products and services used by companies must be as secure as an on-premise infrastructure.

In the past, VPN gateways used to be the measure of all things in terms of professional IT security but now one could believe they have been surpassed by cloud technology. In many instances, server rooms in the office have been replaced by a remote data center, managed by an external service provider. IT security talk is pepped with new concepts like Zero Trust, Single Sign-On or SD-WAN rather than VPN tunnels. What's behind the trend? Is cloud connectivity replacing VPN? The answer couldn't be further from the truth. Companies that opt for the right solution benefit from contemporary VPN structures and digital cloud technology harmonizing perfectly. And there's more: Set up correctly, their strengths can be combined to form a powerful IT security solution.

Enhanced security and compatibility

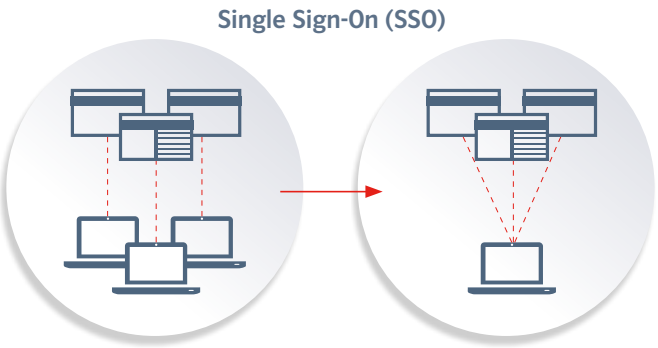
Most companies value the fact that the cloud avoids the burden of owning and managing their own infrastructure. But the cloud is still basically a data center that needs to be at least as secure, if not more secure than local network solutions due to the growing demands on security and access controls. In recent years, new cybersecurity concepts have been launched, especially SASE (Secure Access Service Edge), which connects computer networks and security solutions such as Zero Trust in a cloud service model. Classic VPNs may seem to be out of place in this dynamic network of state-of-the-art IT security solutions. But what if VPN solutions are just as dynamic as cloud technology and can even boost security? For this to be successful, two conditions must be met: Highly secure data communication via an IPsec tunnel and full compatibility with all major cloud technologies.

Next level security

Maximum security is achieved with a cloud-integrated VPN solution accessed through the gateway combined with a management system. This could be, for example, the NCP Virtual Secure Enterprise VPN Server (vSES) in combination with the NCP Secure Enterprise Management (SEM) system. This combination has two key benefits: It routes connections via the IPsec protocol and not SSL. Data packets are encrypted in a highly secure manner, and IPsec avoids slow handshakes meaning that users can leverage the full speed for data transfer. In this case, the gateway is not located directly in the cloud, but forms a secure environment directly on the server behind the firewall. In terms of servers, it is also advisable to carefully choose a data center location considering the local stance on privacy. This maximizes data transfer transparency and maintains digital sovereignty without backdoors.

VPN can also be cloud-based

As mentioned at the top of the page, VPNs must not only be highly secure, but must work seamlessly with cloud services. Keeping the cloud in mind when developing all VPN components from the ground up is key to all pieces working well together.NCP's enterprise VPN products can effortlessly be used as part of a SASE or SD-WAN infrastructure. These solutions focus on gateway and VPN management, which can run as pure software components on any (virtual) server hardware. Consequently, this type of VPN is cloud-ready by nature and can interact with cloud applications.



NCP Gateway and Secure Enterprise Management server are an ideal entry point for cloud remote access. IT administrators can freely configure how access requests are authenticated. Apart from individual requests with multi-factor authentication, as with on-premise models, the use of more complex systems such as SAML (Security Assertion Markup Language) is particularly suitable in the cloud. Here, the user is authenticated a single time via the SSO portal (Single Sign-On) in the cloud. This authentication then applies through the VPN tunnel to both internal services and external cloud applications. Administrators and users continue to enjoy all the benefits of their SAML interface, but at the same time are protected via a highly secure IPsec tunnel avoiding any latency inherent with other protocols. This type of connection also has cost benefits for the organization. With a suitable license model, IPsec tunnels are only billed when connected. In this way, companies benefit from maximum flexibility in their remote access solution.

Full control thanks to Zero Trust

Technologies such as SAML/SSO are often part of a higher-level Zero Trust strategy, which is increasingly implemented in cloud-based IT security infrastructures. Users have access only to the applications they need for their immediate work (least privilege principle). In practice, this is made possible by granularly defined firewall rules, which control access to the VPN gateway. Administrators benefit from a management component such as NCP Secure Enterprise Management (SEM) for configuring access rights of user groups and individual users centrally. Even if SAML/SSO access management is not combined with Zero Trust components, a good VPN solution offers powerful user authentication by means of multi-factor or user certificate verification. Companies also benefit from VPN software features such as central updates, endpoint policy checks or traffic management functions that extend the Zero Trust concept.

If you would like to find out more about modern cloud VPN security for your company, please visit our website at: **www.ncp-e.com/en/solutions/cloud-vpn/**

From basic to advanced

Software features should not be overlooked, as they are essential to making the transition from basic security software to a universal cloud security solution. Features such as the NCP VPN Bypass or split tunneling help to manage data streams within a SAML system by sending data heavy applications such as video streams, which do not necessarily need to be encrypted, past the VPN tunnel to the Internet. This reduces server loads and more computing power is left for the secure transmission of relevant traffic. For the security of the entire network, endpoint policy checks are essential in addition to multi-factor authentication. User end devices are checked for predefined security parameters before each login attempt. If, for example, a laptop does not meet the requirements because virus scanners or the operating system have not been updated, the connection is only established after the required updates have been applied. Administrators can also ensure compliance by distributing policies, firewall changes and software updates to individual user groups or the entire organization with just a few clicks through the VPN management components. Thanks to these powerful features, large numbers of users and WAN systems that are connected to the cloud are protected by the most advanced security available.

NCP

Do you have any questions or would you like to make an appointment for a product demonstration? Please connect with us.

Europe, Asia and Pacific

NCP engineering GmbH

Dombuehler Str. 2
90449 Nuremberg
Germany

+49 911 9968-333

sales@ncp-e.com
www.ncp-e.com

The Americas

NCP engineering, Inc.

19321 US Highway N, Suite 401
Clearwater, FL 33764
USA

+1 650 316-6273

sales@ncp-e.com
www.ncp-e.com

We look forward to discussing your VPN needs with you.