Secur IT y
made in Germany
Trust Seal
www.teletrust.de/itsmig

NCP

SASE, Zero Trust, SD-WAN, SSE …
Modernes VPN vereint maximale Flexibilität mit höchster Sicherheit

Insbesondere das Thema „Cloud" hat in den letzten Jahren dazu beigetragen, dass IT-Security-Netzwerke flexibler und digitaler werden. Gleichzeitig bewegen sie sich auch weiter von den klassischen, vertrauten Lösungen weg. Fest steht jedoch: Cloudlösungen in Unternehmen müssen genauso lückenlos abgesichert sein wie eine On-Prem-Infrastruktur.

Wo früher ein einfacher VPN-Server noch das Maß aller Dinge in Sachen professioneller IT-Sicherheit darstellte, steht mittlerweile alles unter dem Zeichen „Cloud". Der Serverraum in der Firmenzentrale weicht vielerorts einem entfernten Rechenzentrum, verwaltet von einem firmenfremden Managed Service Provider. Statt „VPN-Tunnel" säumen Schlagwörter wie „Zero Trust", „Single Sign-On" oder „SD-WAN" die IT-Security-Berichterstattung. Doch wieso eigentlich? Weil sich virtuelle private Netzwerke und Cloudanbindung von vornherein ausschließen? Mitnichten! Entscheidet man sich für die richtige Lösung, harmonieren zeitgemäße VPN-Strukturen und digitale Cloud-Technik ganz wunderbar. Mehr noch: Richtig eingesetzt lassen sich sogar ihre jeweiligen Stärken zu einem mächtigen IT-Security-Instrument kombinieren.

Sicherheit und Kompatibilität

Die meisten Unternehmen schätzen an der Cloud vor allem, dass sie sich nicht im eigenen Unternehmen befindet und daher auch nicht selbst gewartet oder verwaltet werden muss. Dennoch ist eine Cloud im Grunde nichts anderes als ein Rechenzentrum, das durch die gewachsenen Ansprüche an Sicherheit und Zugriffskontrollen mindestens genauso gut, wenn nicht sogar besser abgesichert sein will als lokale Netzwerklösungen. Dafür wurden in den letzten Jahren neue Cybersicherheitskonzepte, allen voran SASE (Secure Access Service Edge), ins Leben gerufen, die Computernetzwerke und Sicherheitslösungen wie Zero Trust in einem Cloud-Servicemodell verbinden. Klassische, starre VPN-Ansätze haben in diesem dynamischen Verbund aus modernsten IT-Security-Lösungen augenscheinlich keinen Platz. Doch was, wenn die VPN-Lösung genauso dynamisch wie die Cloud-Techniken wäre und gleichzeitig noch ein erheblich höheres Sicherheitsniveau mitbringen würde? Damit dies gelingt, müssen vor allem zwei Punkte erfüllt sein: Hochsichere Datenkommunikation über einen IPsec-Tunnel und vollständige Kompatibilität mit allen gängigen Cloud-Technologien.

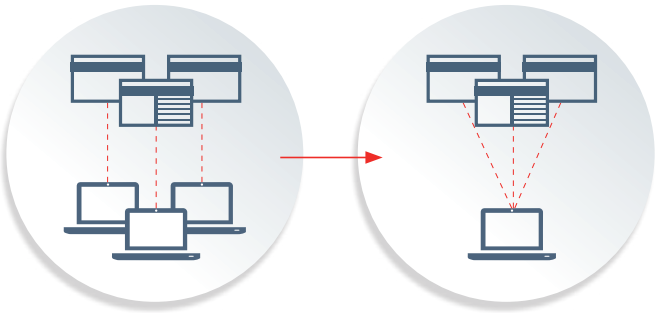
Security auf einer neuen Stufe

Das entsprechende Sicherheitslevel kommt bei einer cloud-integrierten VPN-Lösung durch das Gateway in Verbindung mit einem Management-System zustande. Dies kann z.B. der NCP Virtual Secure Enterprise VPN Server (vSES) in Kombination mit dem NCP Secure Enterprise Management (SEM) sein. Dieser Zusammenschluss hat zwei große Vorteile: Zum einen werden darüber geleitete Verbindungen nicht SSL-, sondern IPsec-basiert übertragen. Dadurch sind Datenpakete hochsicher verschlüsselt, während bremsende Handshakes entfallen und User die volle Geschwindigkeit für den Datentransfer nutzen können. Zum anderen liegt das Gateway nicht direkt in der Cloud, sondern bildet hinter der Firewall eine abgesicherte Umgebung direkt auf dem Server. In puncto Server empfiehlt es sich außerdem, ein Rechenzentrum in Deutschland zu wählen. So erhalten Sie die maximale Transparenz über Ihre Datenflüsse und bewahren Ihre digitale Souveränität ohne Backdoors.

VPN kann auch Cloud!

Wie eingangs erwähnt müssen VPNs nicht nur hochsicher sein, sondern sich vor allem nahtlos mit den mittlerweile etablierten Cloud-Services verwenden lassen. Dies funktioniert nur, wenn dieser Einsatzzweck bei der Entwicklung der VPN-Lösung von Grund auf mitbedacht und an jeder Stelle integriert wurde. Dies ist unter anderem bei den Enterprise-VPN-Lösungen von NCP gegeben, die z. B. mühelos als Teil einer SASE-, SD-WAN- oder SSE-Infrastruktur eingesetzt werden können. Auch hier stehen Gateway und VPN-Management im Zentrum, die als reine Software-Komponenten auf praktisch jeder Server-Hardware lauffähig sind. Dadurch ist diese Art von VPN bereits von Natur aus „cloudfähig" und kann mit entsprechenden Cloudanwendungen interagieren.

Single Sign-On (SSO)



Gateway und Management bilden damit gewissermaßen das Eingangstor für den Cloud-Remote-Access. Wie die Zugangsanfragen authentisiert werden, kann vom Admin frei definiert werden. Abseits von reinen Einzelabfragen mit Multi-Faktor-Authentifizierung, wie man sie von zeitgemäßen On-Premise-Modellen kennt, bietet sich im Cloud-Kosmos vor allem die Verwendung von komplexeren Systemen wie SAML (Security Assertion Markup Language) an. Hier wird der Nutzer am SSO-Portal (Single Sign-On) in der Cloud einmal authentisiert. Diese Authentisierung gilt dann durch den VPN-Tunnel sowohl für interne Dienste als auch externe Cloudanwendungen. So genießen Administratoren und Nutzer weiterhin alle Vorteile ihrer SAML-Schnittstelle, sind jedoch gleichzeitig über einen hochsicheren IPsec-Tunnel geschützt, der verschlüsselte Datenübertragung in voller Geschwindigkeit zulässt. Dieser Tunnel bietet außerdem einen wirtschaftlichen Vorteil für das Unternehmen. Mit einem passenden Lizenzmodell wird die IPsec-Absicherung nur kostenpflichtig, wenn der Tunnel auch tatsächlich aufgebaut wird. Dadurch erhalten Sie auch in dieser Hinsicht maximale Remote-Flexibilität.

Volle Kontrolle dank Zero Trust

Technologien wie SAML/SSO sind oft auch Bestandteil einer übergeordneten Zero-Trust-Strategie, die ebenfalls immer häufiger in cloudbasierten IT-Security-Infrastrukturen zum Einsatz kommt. Dabei haben Nutzer nur Zugriff auf die Anwendungen, die sie für ihre unmittelbare Arbeit benötigen (Least-privilege-Prinzip). In der Praxis wird dies mithilfe granular definierter Firewall-Regeln ermöglicht, die alle Zugriffe am VPN-Gateway kontrollieren. Hierbei profitieren Administratoren von einer Management-Komponente wie dem NCP Secure Enterprise Management (SEM), durch die alle Zugriffsrechte von Nutzergruppen und einzelnen Anwendern zentral konfigurierbar sind. Auch wenn Sie die Zero-Trust-Komponenten nicht im Zusammenspiel mit einer SAML/SSO-Access-Verwaltung betreiben, bietet eine gute VPN-Lösung übrigens von Haus aus eine mächtige User-Authentisierung mittels Multifaktor oder Benutzerzertifikatsüberprüfung. Zusätzlich profitieren Sie durch den Funktionsumfang der VPN-Software von weiteren Features wie zentralen Updates, Endpoint Policy Checks oder Traffic-Management-Funktionen, die den Zero-Trust-Gedanken nicht nur erfüllen, sondern sogar weiterführen.

Aus „Basic" wird „Advanced"

Die genannten Features sollten nicht außer Acht gelassen werden, denn erst durch sie wird aus einer grundlegenden Sicherheitssoftware eine allumfassende Cloud-Security-Lösung. So helfen Funktionen wie der NCP VPN-Bypass oder Split Tunneling dabei, innerhalb eines SAML-Systems Datenströme zu managen, indem datenhungrige Applikationen wie z.B. Videostreams, die nicht zwingend verschlüsselt werden müssen, am VPN-Tunnel vorbei ins Internet gesendet werden. Auf diese Weise wird der Server entlastet und es bleibt mehr Rechenleistung für die sichere Übertragung von relevantem Traffic übrig. Für die Sicherheit des gesamten Netzes sind neben Multifaktor-Authentifizierungen auch Endpoint Policy Checks unerlässlich. Hier werden die Endgeräte der User vor jedem Login-Versuch auf vordefinierte Security-Parameter hin überprüft. Erfüllt beispielsweise ein Laptop die Vorgaben nicht, weil Virenscanner oder Betriebssystem veraltet sind, wird die Verbindung erst nach Abschluss der notwendigen Updates aufgebaut. Dieser Kreis schließt sich, wenn der Administrator durch die VPN-Management-Komponenten mit wenigen Klicks Policies, Firewall-Änderungen und Software-Updates an einzelne Nutzergruppen oder die gesamte Organisation verteilen kann. Dadurch bleiben auch große Anwenderzahlen und WAN-Systeme, die mit der Cloud verbunden sind, immer auf dem neuesten Sicherheitsstand!

NCP

Sie haben Fragen oder möchten einen Termin für eine Produktdemonstration vereinbaren? Dann kontaktieren Sie uns!

NCP engineering GmbH
Dombühler Straße 2
90449 Nürnberg

Tel.: +49 911 9968-0
vertrieb@ncp-e.com
www.ncp-e.com

Wir freuen uns auf ein Gespräch mit Ihnen!

Weitere Infos auf unserer Webseite!