7 Voraussetzungen für einen reibungslosen VPN Client Einsatz

Virtual Private Networks – zu deutsch virtuelle private Netzwerke oder kurz VPN – sind der Schlüssel zum Schutz Ihres Netzwerks! VPNs so zu managen, dass sie wirkungsvoll vor Bedrohungen schützen, ist schon bei stationären Endgeräten eine zwar zeitraubende, aber wichtige Aufgabe. Unverzichtbar wird ein effizientes und einfaches VPN-Management allerdings, wenn mobile Geräte wie Smartphones, Tablets oder Notebooks dazukommen, die sich über ein halbes Dutzend unterschiedlicher Medien mit dem VPN-Gateway verbinden sollen.

Ein zuverlässiges VPN-Management ist nicht nur eine Frage der Sicherheit. Reibungslos laufende Prozesse und ein geringer Aufwand sparen auch Kosten. Experten weisen darauf hin, dass die Möglichkeiten zum Management der VPN-Lösung den größten Einfluss auf die Kaufentscheidung haben sollten: Je einfacher die Verwaltung, desto kostengünstiger kann das VPN mittel- und langfristig betrieben werden.

VPN-Prüfstand

Um Probleme beim Einsatz von VPN-Clients zu vermeiden, stellen Sie Ihre VPN-Umgebung am besten genau auf den Prüfstand: Erfüllt sie die folgenden sieben Anforderungen?

1. Für alle gängigen Betriebssysteme
2. Unterstützung sämtlicher Verbindungsarten
3. Anpassungsfähige Software-Lösung
4. Integration in eine bestehende Infrastruktur
5. Single Point of Administration
6. Unterstützung für IPsec- und SSL-Protokolle
7. Die Zwei-Faktoren-Authentifizierung

1. Für alle gängigen Betriebssysteme

Um flexibel agieren zu können, sollte Ihre VPN-Technologie den Fernzugriff für die gängigen Betriebssysteme von Desktops und Mobilgeräten ermöglichen. Dazu zählen Windows, Apple, Android und Linux. Darüber hinaus werden im Idealfall auch kleinere Plattformen unterstützt.

Deutschland: NCP engineering GmbH • Dombühler Str. 2 • 90449 Nürnberg • Fon +49 911 9968-0 • Fax +49 911 9968-299
Americas: NCP engineering, Inc. • 444 Castro Street, Suite 711 • Mountain View, CA 94041 • Phone: +1 (650) 316-6273 • www.ncp-e.com

7 Voraussetzungen für einen reibungslosen VPN Client Einsatz

VPN-Technologien mit einheitlichen Client-Oberflächen auf sämtlichen Geräten und Betriebssystemen haben gewichtige Vorteile: Zum einen ist dies der universelle Support, zum anderen sind es weitere bedeutende Effizienzgewinne. So ist es zum Beispiel nicht nötig, für jedes Betriebssystem und jedes Gerät Anleitungen bereitzuhalten. Darüber hinaus ist die Bedienung auf jedem Gerät – vom Laptop über das Smartphone bis hin zum heimischen Desktop – für den Nutzer immer sehr ähnlich. So wird der Helpdesk entlastet und die Produktivität der Mitarbeiter erhöht.

2. Unterstützung sämtlicher Verbindungsarten

Greifen Ihre Mitarbeiter von einem mobilen Hotspot, über öffentliche WLAN-Netze oder über die Mobilfunkstandards 3G oder 4G/LTE auf das Unternehmensnetzwerk zu, müssen Sie das Netzwerk vor unbefugtem Zugriff schützen. Ihr Anspruch an die Sicherheit des Netzes sollte dabei genauso hoch sein wie bei der sicheren LAN-Infrastruktur im Büro: Ihre VPN-Lösung muss Ihre Daten während der Übertragung komplett abschirmen und wirkungsvoll verschlüsseln. Nur so ist die Integrität Ihrer Unternehmensdaten sichergestellt – und das gilt für jede Art von Verbindung.

Ein guter VPN-Client sollte auch bei einem Wechsel von einer Verbindungsart zu einer anderen nicht schwächer werden. Das sollte gewährleistet sein, ohne dass eine Anpassung der Einstellungen erforderlich wird. Am besten stellen Sie Ihren Nutzern dafür die Seamless Roaming-Technologie zur Verfügung. So können sie von ihrem heimischen WLAN-Netzwerk unterwegs zu einem 3G oder 4G-Netzwerk oder auch zu einem Hotspot in einem Café wechseln. Und zwar ohne erneuten Verbindungsaufbau.

3. Anpassungsfähige Software-Lösung

Soll die VPN-Verbindung für unterschiedlich lange Zeitfenster offenbleiben, weil sich externe Mitarbeiter über Mobiltelefone oder Tablets mit Ihrem Netzwerk verbinden, sind eventuell die Einstellungen Ihres Back-Ends anzupassen. Das liegt daran, dass zum Beispiel ein Mobiltelefon aller Voraussicht nach öfter inaktiv sein wird als ein Laptop.

In dieser Situation haben Sie zwei Möglichkeiten: Entweder wird die Verbindung des Mobiltelefons zum VPN-Tunnel nach jeder Nutzung unterbrochen, um ein unbefugtes Eindringen in Ihr Netzwerk weitestgehend zu verhindern. Oder Sie entscheiden sich dafür, die Verbindung über einen definierten Zeitraum aufrechtzuerhalten, damit Mitarbeiter in diesem Zeitfenster leichter auf das VPN zugreifen können.

Deutschland: NCP engineering GmbH • Dombühler Str. 2 • 90449 Nürnberg • Fon +49 911 9968-0 • Fax +49 911 9968-299
Americas: NCP engineering, Inc. • 444 Castro Street, Suite 711 • Mountain View, CA 94041 • Phone: +1 (650) 316-6273 • www.ncp-e.com

Wieder anders werden Ihre Anforderungen aussehen, wenn Sie eine VPN-Lösung benötigen, die M2M-Verbindungen – also Verbindungen mit Scannern, Verkaufsautomaten, Geldautomaten und ähnlichen Maschinen – ohne menschliche Interaktion verarbeiten kann.

Sie sehen: Die Anforderungen an eine VPN-Lösung können sehr unterschiedlich sein. Setzen Sie deshalb auf ein Konzept, das Ihre unterschiedlichen Anforderungen flexibel erfüllen kann. Ideal sind Lösungen, die dank ihrer zentralen Management-Funktionen die VPN-Konfigurationen auf dem Client-Gerät automatisiert steuern und die außerdem die VPN-Software ebenso automatisiert distribuieren.

4. Integration in eine bestehende Infrastruktur

Die Angriffe auf Netzwerke von Unternehmen und anderen Organisationen werden immer raffinierter. Die Kommunikation zwischen Netzwerk und Sicherheitskomponenten ist daher inzwischen unverzichtbar. Stellen Sie sicher, dass Ihre VPN-Technologie solide in Ihre Infrastruktur integriert ist und dass Sie keine Netzwerkkomponenten ersetzen müssen. Ihre VPN-Lösung sollte mit VPN-Gateways von beispielsweise Cisco, Juniper, Check Point oder Fortinet kompatibel sein. So ist Ihre Investition geschützt und Sie haben es erfolgreich vermieden, sich von einem Hersteller abhängig zu machen. Die Kombination von Lösungen verschiedener Anbieter eröffnet Ihnen zudem den Zugang zu multiplen Verteidigungsschichten, die das mehrstufige Defense-in-Depth-Konzept Ihrer Netzwerkumgebung zusätzlich optimieren.

5. Single Point of Administration

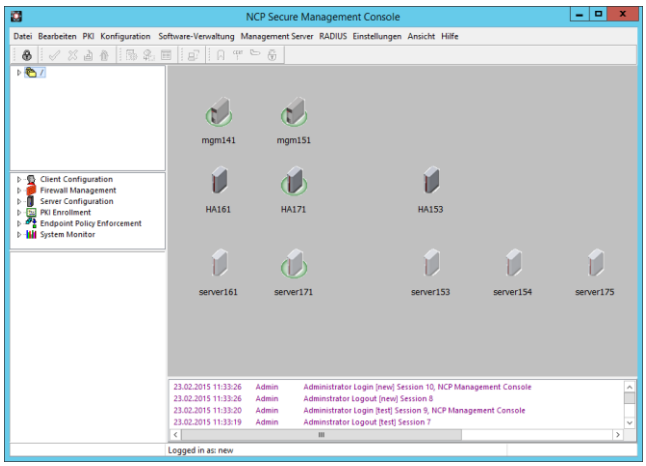
Wächst Ihr Unternehmen, muss sich Ihre VPN-Lösung den veränderten Bedürfnissen Ihrer Organisation anpassen. Sie müssen in jedem Fall die Kontrolle behalten. Setzen Sie auf zentrale Management-Funktionalitäten, die einen einfachen Support von 50 bis 50.000 Verbindungen simultan ermöglichen. Ein Single Point of Administration ist Ihre optimale Ausgangsbasis für

- den automatischen Rollout von VPN Client-Konfigurationen, Personal Firewall Konfigurationen und VPN-Software-Updates,
- die Ausgabe, Verwaltung und Pflege von Zertifikaten sowie
- die Überwachung der Richtlinieneinhaltung.

Integriert Ihre VPN-Lösung darüber hinaus auch Ihre bestehende Nutzerdatenbank, können Sie ganz leicht Nutzerkonten erstellen oder löschen. Das funktioniert zum Beispiel mit Active Directory oder LDAP.

Deutschland: NCP engineering GmbH • Dombühler Str. 2 • 90449 Nürnberg • Fon +49 911 9968-0 • Fax +49 911 9968-299
Americas: NCP engineering, Inc. • 444 Castro Street, Suite 711 • Mountain View, CA 94041 • Phone: +1 (650) 316-6273 • www.ncp-e.com

7 Voraussetzungen für einen reibungslosen VPN Client Einsatz



Dank des zentralen Managements ist ein manueller, individueller Client-Support nicht mehr nötig. Die Wahrscheinlichkeit, dass Nutzern Fehler unterlaufen, sinkt ebenso wie die Anzahl der Helpdesk-Anfragen rund um Ihre VPN-Lösung. Jetzt stellen Sie den Nutzern keine Konfigurationsanweisungen mehr zur Verfügung. Stattdessen betten Sie deren Konfigurationsprofile in Ihr Installationsprogramm ein. Nun können die Nutzer den Client leicht installieren und sich sofort in das VPN einloggen.

6. Unterstützung für IPsec- und SSL-Protokolle

Ihre Mitarbeiter müssen effizient arbeiten können. Und zwar unabhängig davon, welche Anwendung sie verwenden oder von wo aus sie sich mit dem Netzwerk verbinden. Benötigen externe Mitarbeiter die gleichen Zugriffsmöglichkeiten, die sie in der Unternehmenszentrale hätten, ist eine IPsec-Verbindung zu bevorzugen. IPsec steht für „Internet Protocol Security“. Für sichere webbasierte Anwendungen und Kommunikationen ist eine SSL-Verbindung – Secure Sockets Layer – möglicherweise ausreichend.

Eine VPN-Lösung, die beiden Verfahren gerecht wird, kann die Bedürfnisse sämtlicher Nutzer erfüllen: Homeworker, Mitarbeiter im Außendienst, Vertrieb und Service, Lieferanten und externe Partner werden gleichermaßen zufrieden sein. Außerdem kann solch eine Lösung die Verwaltung eines sicheren Netzwerks erleichtern.

7. Die Zwei-Faktoren-Authentifizierung

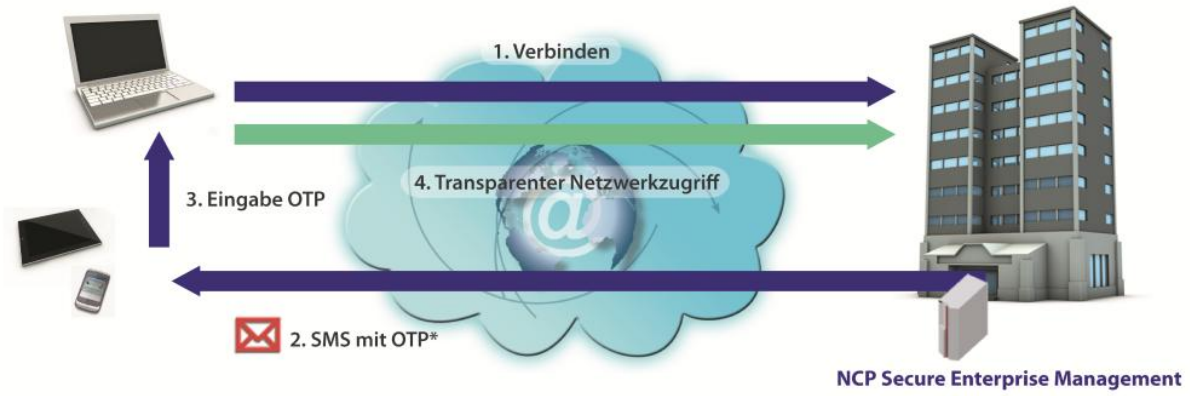
Angesichts der vielen Bedrohungen für Ihr Netzwerk reichen Nutzername und Passwort nicht mehr aus, um unerlaubte Fernzugriffe zu verhindern. Sie brauchen ein stabiles VPN, das hochmoderne Verfahren zur Authentifizierung nutzt. Doch welches Sicherheitsniveau ist nötig?

Sie könnten eine VPN-Lösung mit Authentifizierung durch zwei Faktoren erwägen. Diese Lösung kann zum Beispiel auf dem Besitz eines Token und auf dem Wissen von Nutzername und Passwort

Deutschland: NCP engineering GmbH • Dombühler Str. 2 • 90449 Nürnberg • Fon +49 911 9968-0 • Fax +49 911 9968-299
Americas: NCP engineering, Inc. • 444 Castro Street, Suite 711 • Mountain View, CA 94041 • Phone: +1 (650) 316-6273 • www.ncp-e.com

7 Voraussetzungen für einen reibungslosen VPN Client Einsatz

basieren. Es liegt nahe, dass Installation und Verwaltung des zweiten Faktors zur Authentifizierung zusätzliche Ressourcen erfordern. Stellen Sie unbedingt sicher, dass Ihre Lösung den Rollout von Zertifikaten mit vorhandenen Geräten automatisch durchführen kann. Das können beispielsweise Smart Cards oder Smartphones als Empfänger für Einmalpasswörter, sogenannten OTPs, sein. Moderne Tools sollten die Authentifizierungsmechanismen managen.



Ein zuverlässiges VPN kann den sicheren Remote Access – den sicheren Fernzugriff – zu Ihrem Netzwerk gewährleisten. Sogar bei einem Wechsel des Gerätes, des Ortes oder der Verbindungsart. Eine optimale Lösung vereint alle wichtigen Management-Aufgaben in einer Konsole und entlastet Mitarbeiter wie Administratoren von zeitraubenden Routineaufgaben, von Schulungen und Support. Ihre Expertise und ihre Innovationsstärke können diese Mitarbeiter nun effizient in andere Projekte einbringen. Die Sicherheit des Firmennetzwerks ist trotzdem zu keinem Zeitpunkt gefährdet.

Zwar genügt selbst ein stabiles VPN nicht, um sämtliche Cyber-Angriffe abzuwehren. Eine VPN-Lösung in Verbindung mit Firewalls, Intrusion-Prevention-Systemen, Virenscannern und weiteren Netzwerksicherheitskomponenten schützt die Infrastruktur Ihres Netzwerks hingegen sehr wohl vor Eindringlingen. Und mit proaktivem Handeln können Ihre IT-Administratoren von Anfang an adäquat auf Bedrohungen reagieren.

Bleiben Sie auf der sicheren Seite: Bleiben Sie wachsam!

Sie haben Fragen oder möchten einen Termin für eine Produktdemonstration vereinbaren?
Dann rufen Sie uns jetzt unter +49 (0)911 99 68 0 an
oder schreiben Sie eine E-Mail an vertrieb@ncp-e.com.

Wir freuen uns auf das Gespräch mit Ihnen!

Deutschland: NCP engineering GmbH • Dombühler Str. 2 • 90449 Nürnberg • Fon +49 911 9968-0 • Fax +49 911 9968-299
Americas: NCP engineering, Inc. • 444 Castro Street, Suite 711 • Mountain View, CA 94041 • Phone: +1 (650) 316-6273 • www.ncp-e.com