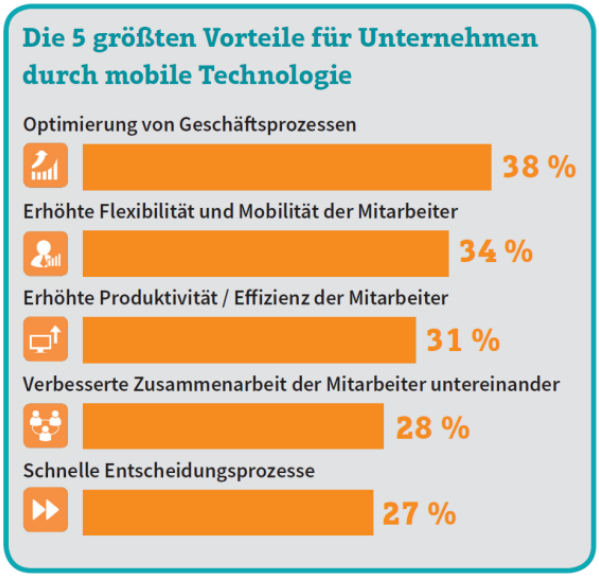
"Seamless" Roaming im VPN-Umfeld

Always on

Ein Kernproblem beim Fernzugriff auf das Firmennetz von Windows Notebooks aus besteht darin, dass häufig unterschiedliche Verbindungstypen zum Zuge kommen: ein Wireless-LAN am Flughafen, ein 4G-Mobilfunknetz bei der Fahrt ins Hotel und ein LAN in der Firmenfiliale. Eine Remote-Access-Lösung muss garantieren, dass das Roaming zwischen diesen unterschiedlichen Netzen reibungslos funktioniert, und zwar ohne Kompromisse in Bezug auf die Sicherheit. Entsprechende Lösungen sind bislang allerdings Mangelware.

Der klassische "Bürokrieger", der ausschließlich an seinem Schreibtisch im Unternehmen tätig ist, wird in wenigen Jahren Seltenheitswert haben. Das Marktforschungsunternehmen IDC schätzt, dass im Jahr 2015 über 1,3 Milliarden zur Kategorie der "Mobile Worker" zählen. Sie erledigen ihre Aufgaben nicht mehr vorzugsweise vom Büro in der Firma aus, sondern nutzen Notebooks, Smartphones und Tablets, um auf einer Dienstreise, im Hotel oder im Home Office E-Mails zu bearbeiten oder auf Unterlagen zuzugreifen, die im Firmennetz lagern.



Vorteile durch mobile Technologie:
Der Einsatz mobiler Endgeräte erhebliche Vorteile. Quelle: IDC

Es sind beileibe nicht nur Großunternehmen, die ihren Mitarbeitern Mobilgeräte an die Hand geben. Laut einer Umfrage des Netzwerks Elektronischer Geschäftsverkehr unter kleinen und mittelständischen

"Seamless" Roaming im VPN-Umfeld

Firmen in Deutschland stattet ein Fünftel dieser Unternehmen die Mehrzahl ihrer Mitarbeiter mit Firmen-Handys, Smartphones oder mobilen Rechnern aus. Insbesondere Geschäftsführer sowie Vertriebs- und Servicemitarbeiter nutzen mobile Geräte, um von unterwegs aus über ein VPN (Virtuelles Privates Netz) Zugang zu Unternehmensinformationen zu erhalten.

Seamless Roaming ist gefordert

Doch in der Praxis ist es alles andere als einfach, eine VPN-Verbindung durchgängig aufrecht zu erhalten. Der Grund dafür ist, dass die meisten Business-Notebooks sowohl mit einem Wireless-LAN-Modul als auch einem Mobilfunk-Chip ausgestattet sind. Ebenso besitzen sie einen LAN-Adapter, über den sie sich über ein drahtgebundenes Netz mit dem Corporate Network verbinden können, etwa vom Heimbüro aus oder in einer Firmenaußenstelle.
Mobilgeräten stehen somit drei Techniken zur Verfügung, um sichere VPN-Tunnel (Virtual Private Network) zu einem Firmennetz aufzubauen: das traditionelle drahtgebundene Ethernet-LAN, Wireless LAN (WLANs) in öffentlichen Hotspots, Hotels oder Unternehmen und Mobilfunkverbindungen. Beim Mobilfunk müssen wiederum unterschiedliche Technologien unterstützt werden, vom GSM-Netz über 3G-Verbindungen (UMTS) bis hin zu High-Speed-Verbindungen über 4G-Netze (LTE, Long Term Evolution).
Für den Anwender ist es ein Vorteil, wenn er nicht auf ein Verbindungsmedium festgelegt ist.
Eine Remote-Access-Lösung stellt diese Flexibilität jedoch vor eine Herausforderung. Sie muss

- den automatischen Wechsel des Verbindungsmediums unterstützen,
- beim Wechsel des Mediums einen bestehenden VPN-Tunnel dynamisch umleiten und
- verhindern, dass Anwendungssitzungen (Sessions) abbrechen.

Der Wechsel zwischen unterschiedlichen Netztypen und Verbindungsarten, Stichwort Seamless Roaming, ist beileibe kein Ausnahmefall. Ein Bespiel: Ein Mitarbeiter möchte mit dem ICE zu einem Treffen mit seinen Kollegen in einer Außenstelle reisen. Zunächst stellt er auf dem Bahnhof über ein Wireless LAN an einem Hotspot von seinem Notebook aus eine Verbindung zum Firmennetz her, um E-Mails und Dokumente zu bearbeiten. Während der Fahrt steht je nach Aufenthaltsort des Zuges eine 3G/4G-Verbindung zur Verfügung, dann sinkt die Übertragungsrate auf GSM-Niveau, und in abgelegenen Regionen reißt die Verbindung ganz ab. Sobald er in der Filiale angekommen ist, klinkt sich der Mitarbeiter über das dort vorhandene drahtgebundene Local Area Network (LAN) oder WLAN in das Firmennetz ein.

"Seamless" Roaming im VPN-Umfeld

Instabile Anwendungen durch Verbindungsabbruch

Etliche Remote-Access-Lösungen und VPN-Clients reagieren auf solche Wechselspiele, indem sie den VPN-Tunnel abbauen, wenn die Verbindungsart wechselt, also beispielsweise von einem WLAN zu UMTS/3G oder umgekehrt. Dasselbe passiert, wenn eine Verbindung zeitweilig nicht zur Verfügung steht, etwa wenn der Nutzer im Zug eine Region mit schlechtem Mobilfunkempfang durchquert. Für den Anwender heißt das, er muss nochmals eine Verbindung aufbauen und sich erneut authentifizieren – ein zeitraubender Vorgang.

Damit nicht genug: Noch problematischer ist, dass die meisten Netzwerk-Anwendungen auf den Wechsel von Verbindungsarten und die damit verbundenen kurzzeitigen Unterbrechungen allergisch reagieren. Wenn die physische Verbindung zu einem Server ausfällt, können sie in einen instabilen Zustand übergehen. Das kann zum Verlust von Daten führen.

Die "Application Persistence" sicherzustellen, also nach einer Unterbrechung den vorherigen Zustand einer Anwendung wiederherzustellen, ist daher eine zentrale Anforderung, die eine Seamless-Roaming-Lösung bieten muss. Das ist auch dann der Fall, wenn es zum Roaming zwischen einer schnellen und einer langsameren Verbindungsart kommt, etwa von einem Wireless LAN mit 50 MBit/s Bandbreite zu einer HSPA-Mobilfunk-Connection (High Speed Packet Access) mit 3,6 oder 7,2 MBit/s beim Herunterladen von Daten: "In diesem Fall ist es erforderlich, die Anwendung gewissermaßen zeitweilig zu 'beruhigen', damit keine Daten verlorengehen", sagt Jörg Hirschmann, CTO bei NCP engineering. Außerdem sei es erforderlich, die Unterbrechungszeiten beim Wechsel der Verbindungsmedien so kurz wie möglich zu halten.

VPN-Tunnel umleiten

Damit ein VPN-Tunnel beim Wechsel des Mediums weiterhin bestehen bleibt, muss die IP-Konfiguration des Tunnels im System beibehalten werden. Sobald andere IP-Adressen ins Spiel kommen, ist ein Neuaufbau der VPN-Verbindung die Folge. Zudem erfordert das Roaming von VPN-Verbindungen, dass auch die IKE-Protokolle 1 und 2 (Internet Key Exchange), die in IPsec-VPNs für das Aushandeln der Verschlüsselungsverfahren und den Austausch der Keys zuständig sind, das Umleiten der VPN-Tunnel unterstützen. Bei IKEv2 lässt sich dies mithilfe von MobIKE erreichen, einer Erweiterung, die einen Wechsel der IP-Adresse des Host-Systems z.B. beim Wechsel des Netzwerk-Interfaces erlaubt. Ein Anwender kann somit beispielsweise in einem Büro über ein kabelgestütztes LAN eine VPN-Verbindung aufbauen, später das Netzwerkkabel entfernen und in einem anderen Gebäude oder Raum über ein WLAN dieselbe VPN-Verbindung weiter nutzen. Die Anwendungen bleiben von dem Wechsel unberührt.

"Seamless" Roaming im VPN-Umfeld

Seamless Roaming mit NCP

Seamless Roaming stellt die meisten VPN-Lösungen vor Probleme. Als einer der ersten IPsec VPN-Clients weltweit unterstützt die Software von NCP in Verbindung mit dem NCP Enterprise VPN Server das nahtlose Weiterreichen von VPN-Verbindungen über unterschiedlichen Medien. Die Lösung stellt sicher, dass auch beim Abbruch einer Verbindung, etwa wenn während einer Zugfahrt keine Mobilfunkverbindung verfügbar ist, der VPN-Tunnel bis zum nächsten Wiederaufbau der physischen Verbindung erhalten bleibt. Die logische Connection besteht in diesem Fall weiterhin, auch wenn der VPN-Client keinen Zugang zum VPN-Server hat. Den Nutzer informiert die Client-Software über den zeitweiligen Ausfall der physischen Verbindung, indem sie den Status des VPN-Tunnels im Client-Monitor von Grün auf Gelb setzt. Dabei steuert die Software im Seamless Roaming-Betrieb dynamisch das DPD-Handling, sodass im Fall einer Unterbrechung der physikalischen Verbindung weder Gateway noch Client die VPN-Verbindung terminieren. DPD (Dead Peer Detection) ist ein Verfahren, das erkennt, ob eine VPN-Verbindung auf Basis von IPsec unterbrochen wurde und das den Neuaufbau des Tunnels ermöglicht.

Verbindung auf Knopfdruck

Wichtig ist beim VPN-Zugang über Mobilfunk, siehe das Beispiel Zugfahrt, dass die VPN-Lösung die Verbindung automatisch wieder aufbaut, sobald das Netz wieder verfügbar ist. Für den Anwender sollte dieser Vorgang transparent ablaufen, um eine Fehlbedienung zu verhindern und um von dieser Aufgabe zu entlasten.

Zum Bedienkomfort trägt außerdem bei, wenn sich der Benutzer des VPN-Clients nicht mit der Frage beschäftigen muss, welches Medium das "beste" ist, etwa WLAN oder Mobilfunknetz. Im Idealfall sollte der Anwender nur einen "Connect"-Button drücken, und die Client-Software wählt auf Basis der "Policies", die der Netzwerkmanager vorgegeben hat, den passenden Verbindungstyp aus.

Fazit

Seamless Roaming ist kein Luxus, sondern in einer Berufswelt, die immer "mobiler" wird, eine Notwendigkeit. VPN-Lösungen, die diese Funktion nicht bieten, sind schlichtweg nicht mehr zeitgemäß. Denn sie schränken die Arbeitsmöglichkeiten mobiler Mitarbeiter erheblich ein. Und dies kann sich heutzutage kein Unternehmen und keine Organisation mehr leisten.

"Seamless" Roaming im VPN-Umfeld

Checkliste für eine VPN-Client-Lösung

Ein VPN-Client für den Einsatz in Unternehmen sollte nicht nur den unterbrechungsfreien Wechsel zwischen unterschiedlichen Verbindungsarten erlauben. Hier eine Liste der Funktionen, die ein VPN-Client aufweisen sollte:

Support für alle Arten von Netzen:
LANs, Wireless-LANs und eine möglichst breite Palette von Mobilfunktechniken wie GSM, UMTS, High Speed Packet Access (HSPA) sowie 4G-Technologien wie Long Term Evolution (LTE).

Unterstützung von Windows 7 Mobile Broadband:
Die Mobile-Broadband-Schnittstelle von Windows 7 erlaubt es, 3G- und 4G-Mobilfunktechniken wie LTE (Long Term Evolution) zu nutzen.

Seamless-Roaming-Funktionen:
Wechsel zwischen unterschiedlichen Netzen, ohne dass VPN-Tunnel abgebaut und Anwendungssessions beendet werden.

Adaptive Personal Firewall:
Je nach Verbindungsart, etwa über ein ungesichertes WLAN, eine Mobilfunkverbindung oder ein firmeninternes Netz, sollte die Firewall des VPN-Clients die Schutzeinstellungen automatisch anpassen: Das Umschalten der Regeln erfolgt bei Erkennen des Netzwerkes anhand des IP-Adressbereiches, der Mac-Adresse des DHCP-Servers oder eines NCP -FND-Servers. Wichtig: Die Firewall sollte auch IPv6 unterstützen.

Zusammenarbeit mit einer Vielzahl von Sicherheits-Gateways: Eine VPN-Lösung sollte nicht nur mit dem IPsec- oder SSL-Gateway des Anbieters zusammenarbeiten, sondern auch mit Produkten anderer Hersteller, beispielsweise Microsofts Windows Server 2012 R2.

IPsec und SSL:
Unterstützung sowohl von IPsec- als auch SSL-VPNs (Secure Socket Layer). Dies bietet dem Nutzer ein Höchstmaß an Flexibilität.

Fallback-Funktion von IPsec zu HTTPS:
Firewalls blocken häufig IPsec-VPN-Verbindungen. In diesem Fall ist eine Funktion wichtig, die IPsec-Verbindungen über SSL-Connections "tunnelt".

Funktion für Kostenkontrolle:
Im Ideal fall bietet der Client eine Funktion, die dem Nutzer einen Überblick über die anfallenden Verbindungsgebühren gibt. Frei definierbare Grenzwerte verhindern, dass das Budget überschritten wird.
Ein "Muss" einer VPN-Client-Software ist eine dynamische Firewall. Sie passt die Sicherheitseinstellungen automatisch an die zur Verfügung stehen Verbindung an.

"Seamless" Roaming im VPN-Umfeld

Haftungsausschluss

Die in diesem Dokument enthaltenen Informationen können ohne Vorankündigung geändert werden und stellen keine Verpflichtung seitens der NCP engineering GmbH dar. Änderungen zum Zwecke des technischen Fortschritts bleiben der NCP engineering GmbH vorbehalten.

Warenzeichen

Alle genannten Produkte sind eingetragene Warenzeichen der jeweiligen Urheber.

Stand April 2015

Next Generation Network Access Technology

www.ncp-e.com

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