7 Lokale Netze über das Internet sicher verbinden

Bis in die 1990er-Jahre wurden hauptsächlich **Mietleitungen**[1] angeschafft, um zwei Netzwerke miteinander zu koppeln (verbinden). Neben den hohen Kosten stellte sich bei dieser Lösung aber der aufwendige Bestell- und Installationsprozess als nachteilig heraus. Die Ursachen dafür lagen vor allem in der monopolartigen Struktur der Telekom-Industrie. Mit dem Aufkommen des Internets gegen Ende der 1990er-Jahre ist die Zahl der **Service Provider** und der entsprechenden Angebote markant gestiegen. Dadurch hat sich die Situation grundlegend geändert. Heute spielen finanzielle und zeitliche Aspekte bei der Koppelung von Netzwerken eine eher untergeordnete Rolle; das Augenmerk liegt vielmehr auf den Bereichen Leistung und Sicherheit. Insbesondere die Verfügbarkeit und die Sicherheit der Firmendaten müssen gewährleistet sein. In diesem Kapitel erfahren Sie mehr zum Thema **«Sichere LAN-Koppelung»** auf der Basis von Netzwerksystemen, die eine gültige IP-Konfiguration aufweisen.

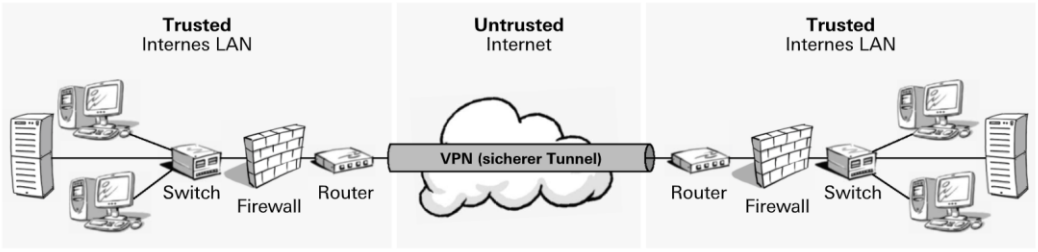
7.1 Virtual Private Network (VPN)

Für externe Zugriffe auf interne Firmennetzwerke über unsichere Verbindungen kommen heute meistens Virtual Private Networks zum Einsatz. Im Folgenden lernen Sie das Funktionsprinzip dieser Technik und verschiedene Verbindungsarten kennen.

7.1.1 Funktionsprinzip

Ein **VPN** ist ein **virtuelles**[2] **Netzwerk,** das physisch nicht vorhanden ist, den Benutzern aber real erscheint, weil es funktional wirksam ist. **Privat** ist dieses Netzwerk insofern, als die übertragenen Daten nur vom **VPN-Betreiber**[3] genutzt werden können, d. h., nur dieser kann auf die Daten in ihrer ursprünglichen, unverschlüsselten Form zugreifen. Andere Personen oder Systeme sind möglicherweise auch in der Lage, auf die Daten im Tunnel zuzugreifen, können sie aber nicht nutzen, weil sie verschlüsselt und somit unkenntlich sind. Ein VPN kann also mit einem unsichtbaren Tunnel verglichen werden, der eine sichere Datenübertragung über unsichere Übertragungsstrecken (wie z. B. das öffentliche Internet) erlaubt. Folgende Grafik soll dieses Prinzip verdeutlichen:

[7-1] VPN-Prinzip: Tunnel für Datenübertragungen durch unsichere Netzwerkbereiche



[1] Englischer Fachbegriff: Leased Line.

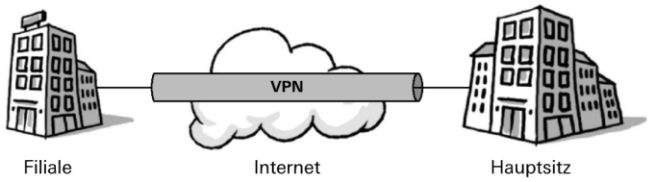
[2] Im Sinne von: nicht echt oder wirklich existierend, aber echt bzw. wirklich erscheinend.

[3] Der VPN-Betreiber ist die Stelle oder Person, die sicherstellen muss, dass die übertragenen Daten von Unbefugten nicht gelesen werden können.

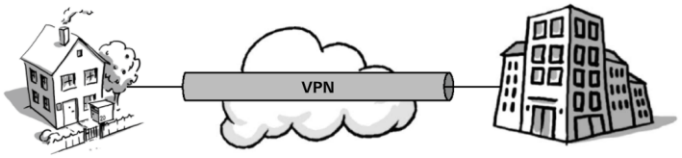
7.1.2 Verbindungsarten

Beim Einsatz eines VPN lassen sich folgende **Verbindungsarten** unterscheiden:

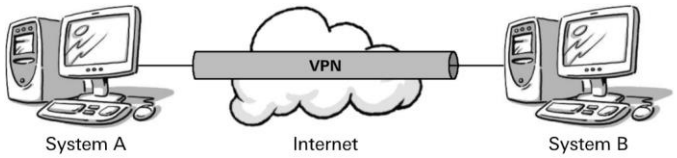
- **Site-to-Site:** Über diese Verbindungsart können getrennte Netzwerkbereiche bzw. Subnetze permanent miteinander verbunden werden (z. B. Koppelung des LANs einer Filiale mit dem Firmennetzwerk am Hauptsitz). Entsprechend wird diese Verbindungsart für die **Standortvernetzung** eingesetzt. Vergleichen Sie dazu auch das Kapitel 6.2.1, S. 102.



- **End-to-Site:** Über diese Verbindungsart können Benutzer von unterwegs oder von zu Hause aus auf die Daten und Applikationen der eigenen Firma zugreifen. Beispiel: Koppelung des WLANs beim Kunden oder des Home Office mit dem Firmennetzwerk am Hauptsitz. Diese Verbindungsart erlaubt also einen **Remote Access**[1]. Vergleichen Sie dazu auch das Kapitel 6.2.2, S. 104.



- **End-to-End:** Über diese Verbindungsart können zwei Rechnersysteme direkt miteinander verbunden werden, wobei keine zusätzlichen VPN-Komponenten wie z. B. Router benötigt werden. Die VPN-Clients (Software) auf den Endsystemen verwalten alle Funktionen selbstständig.



[1] Englisch für: Fernzugriff (autorisiert).

7.3 Praktische Anwendungen eines VPN

Nachfolgend werden wichtige Schritte und Einstellungen gezeigt, die beim Aufbau eines VPN in unserem Fallbeispiel vorzunehmen sind. Dabei kommen folgende Anwendungen zur Sprache:

- Aufbau eines Site-to-Site-VPN
- Aufbau eines End-to-Site-VPN
- Aufbau eines SSL-VPN

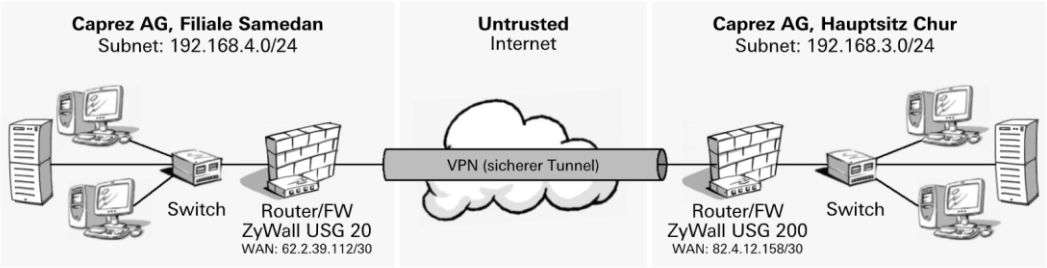
Hinweis

▷ Auch wenn es inzwischen eine fast unüberschaubare Anzahl von Komponenten und Software für VPN gibt, sind die Konfigurationsschritte und -einstellungen bei den meisten Produkten ähnlich, da alle auf IPsec basieren.

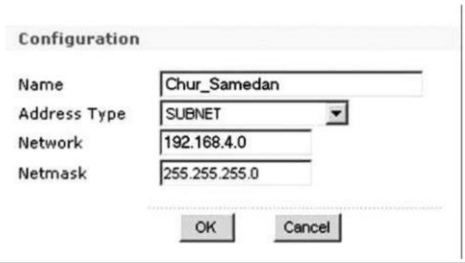
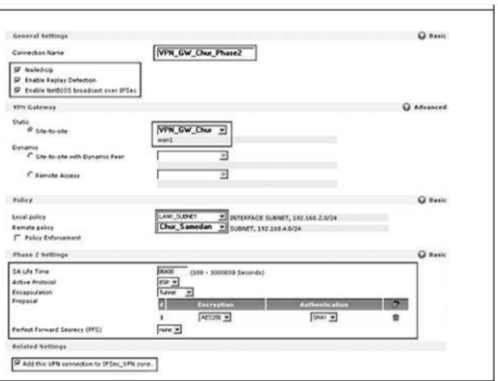
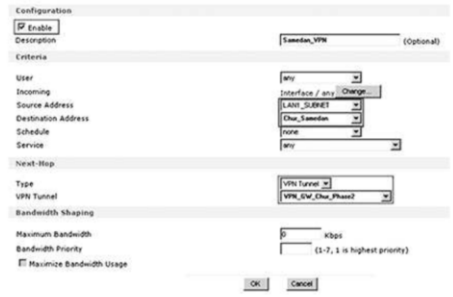
7.3.1 Site-to-Site-VPN einrichten

Zwischen dem Hauptsitz der Firma Caprez Ingenieure AG in Chur und der Filiale in Samedan soll ein Hardware-basierendes **Site-to-Site-VPN** eingerichtet werden. Das entsprechende Netzwerkschema kann vereinfacht wie folgt dargestellt werden:

[7-4] Site-to-Site-VPN (Beispielschema)



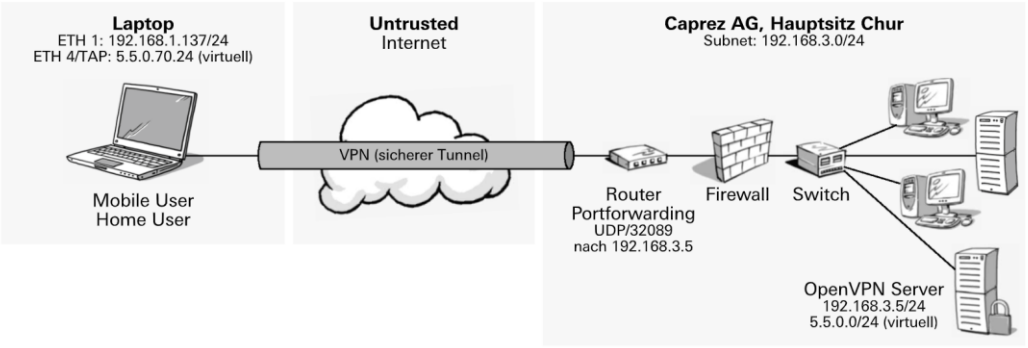
Die nachfolgend aufgezeigten Schritte und Einstellungen beziehen sich auf IKEv1:

Konfiguration auf dem VPN-Gateway in Chur (ZyXEL ZyWall USG 200)	
1. Schritt: Festlegen eines Namens für die neue VPN-Verbindung, der Art der Netzwerkverbindung (Subnetz = Site-to-Site) und der IP-Adresse des entfernten Subnetzes (VPN-Gegenstelle).	
2. Schritt: Angeben der Bezeichnung des lokalen VPN-Systems (Gateway), Definieren des zu verwendenden Netzwerkinterfaces und von dessen IP-Adresse. Danach Definieren eines Pre-Shared Key (PSK) und der Parameter bezüglich Verschlüsselung, Authentification und der Gültigkeitsdauer der Schlüssel. Nach Ablauf dieser Zeit werden automatisch neue Schlüssel vereinbart. «Dead Peer Detection» (DPD) muss wenn gewünscht auf beiden VPN-Komponenten aktiviert sein, da sonst die VPN-Verbindung nach Ablauf des DPD-Timers abgebaut wird.	
3. Schritt: Definieren, ob die VPN-Verbindung ständig online ist (Nailed-Up), also auch wenn keine Daten übertragen werden. Aktivieren des Schutzes gegen «Replay»-Attacken und Zulassen von Weiterleiten von NetBIOS-Broadcasts über die VPN-Strecke. Angeben der gewünschten VPN-Typs (Site-to-Site), Festlegen der lokalen und der entfernten Richtlinien (Policies). Nochmals Bestätigen der Parameter für die Verschlüsselung, der Authentication, der Gültigkeitsdauer und zusätzlich des IPsec-Protokolls (ESP im Tunnel-Modus).	
4. Schritt: Zum Schluss muss das Routing aktiviert und die benötigten Netzwerkinfos (Sende- und Ziel-IP-Adressen) angegeben werden. «Schedule none» bedeutet, dass diese Routingstrecke 7 x 24 Stunden in Betrieb sein soll und für alle Dienste (Service = any). Zum Schluss wird nochmals der VPN-Typ (VPN Tunnel) bestätigt. Für diese VPN-Verbindung wird kein Bandbreitenmanagement aktiviert.	

7.3.2 End-to-Site-VPN einrichten

Zwischen dem Hauptsitz der Firma Caprez Ingenieure AG in Chur und den Mitarbeitenden, die zu Hause arbeiten (Home User) oder im Aussendienst tätig sind (Mobile User), soll ein Software-basierendes **End-to-Site-VPN** eingerichtet werden. Das Netzwerkschema auf der Basis von OpenVPN kann vereinfacht wie folgt dargestellt werden:

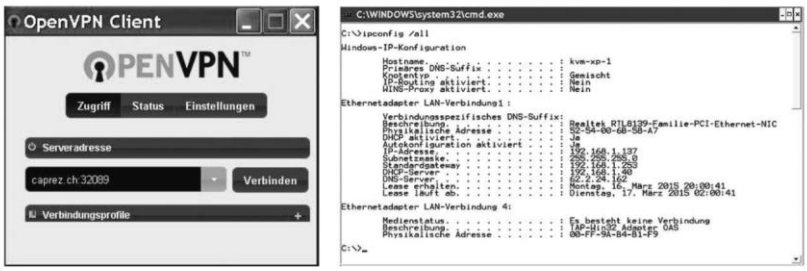
[7-5] End-to-Site-VPN (Beispielschema)



OpenVPN ist eine auf Open Source basierende Software für eine End-to-Site-Lösung, die ein Firmennetzwerk bis zum Rechner eines Benutzers erweitert. Dabei greift der **VPN-Client** nicht einfach via Remote Access auf das Zielnetzwerk zu, sondern wird als zusätzliches Subnetz in das Firmennetzwerk integriert.

Zu diesem Zweck wird der VPN-Client um ein sogenanntes **TAP**[1]**-Device** erweitert, das das OpenVPN-Subnetz bildet. Der **OpenVPN-Client** besitzt neben der physischen Netzwerkschnittstelle also auch eine virtuelle Netzwerkkarte. Der **OpenVPN-Server** routet die Daten der VPN-Clients nach ihrer Entschlüsselung in das LAN und auch in umgekehrter Richtung an den VPN-Client weiter. Folgende Screenshots zeigen den OpenVPN-Client (links) sowie die Netzwerkkonfiguration (rechts) jeweils vor dem Verbindungsaufbau mit dem OpenVPN-Server:

[7-6] Statusinformationen bei OpenVPN während der Verbindung (Beispiel)



Die Vorteile dieser VPN-Lösung bestehen u. a. darin, dass der Server einfach aufgesetzt werden kann, der Datenaustausch standardmässig via UDP abgewickelt wird und OpenVPN somit auch bei VoIP- und Video-Streaming-Applikationen eingesetzt werden kann.

[1] Abkürzung für: Tunnel Adapter. Virtuelle Netzwerkschnittstelle, die mittels Software eine Netzwerkkarte simuliert.

VPN-Lösungen, die vornehmlich auf TCP basieren, eignen sich dagegen kaum für solche zeitkritischen Anwendungen.

Hinweise

▷ Der **OpenVPN-Server** läuft primär auf Linux, kann aber dank der virtuellen Appliances problemlos auch auf anderen Systemen wie z. B. VMware oder MS Windows Hyper-V eingesetzt werden.

▷ Die **OpenVPN-Client SW** gibt es für alle gängigen Betriebssysteme in Mac OS X und Android. OpenVPN findet sich oft als eine «embedded» Variante auf FW/Routern. Nähere Informationen über OpenVPN finden Sie unter www.openvpn.net.

7.3.3 SSL-VPN einsetzen

SSL-VPNs basieren auf den standardisierten Verschlüsselungstechniken **SSL**[1] bzw. **TLS**[2]. SSL-VPNs werden mehrheitlich als End-to-End-Lösung für **Fernzugriffe**[3] von Clients und weniger für die Kopplung von Netzwerken eingesetzt. Ein SSL-VPN kann mittels **Internetbrowser** aufgebaut werden. Dieser verfügt prinzipiell über alle Komponenten, die für eine **sichere Datenverbindung** benötigt werden.

SSL-VPNs bietet gegenüber anderen VPN-Techniken folgende **Vorteile:**

- Clientseitig muss i. d. R. keine zusätzliche Software installiert werden.
- Clientseitig ist i. d. R. kaum Administrationsaufwand erforderlich.
- Firewall-Regeln müssen i. d. R. nicht angepasst werden, da die Verschlüsselung auf den gleichen Routinen beruht, die bereits für die anderen Internetdienste zum Einsatz kommen (z. B. für das Onlinebanking).
- Bei Bedarf werden Softwarebibliotheken genutzt, die vom Browser während des Betriebs automatisch nachgeladen werden.

Demgegenüber ist der Einsatz von SSL-VPNs mit dem **Nachteil** verbunden, dass der vergleichsweise langsame Verbindungsaufbau und die i. d. R. benötigten Java-Applets oder Aktive-X-Komponenten meist höhere Anforderungen an die HW-Ausstattung der Rechner stellen.

Eine interessante **SSL-VPN-Lösung** auf Open-Source-Basis ist SoftEther VPN. Dieses Produkt wurde an der Tsukuba University in Japan entwickelt. Nähere Informationen darüber finden Sie unter: www.softether.org.

[1] Abkürzung für: Secure Socket Layer. Obwohl SSL heute unter dem Begriff TLS weiterentwickelt wird, ist die Bezeichnung SSL-VPN immer noch weitverbreitet.

[2] Abkürzung für: Transport Layer Security.

[3] Remote Access.

Mit dem Durchbruch des Internets sind auch die Anforderungen an die **Koppelung von Netzwerken** stark gestiegen. Als Antwort darauf werden heute häufig virtuelle private Netzwerke, sogenannte **VPNs,** verwendet. Diese kommen i. d. R. in folgenden Situationen zum Einsatz:

- **Site-to-Site-VPN:** Hier werden ganze Netzwerke miteinander verbunden.
- **End-to-Site-VPN:** Hier werden Fernzugriffe (Remote Access) auf Netzwerke möglich.
- **End-to-End-VPN:** Hier werden zwei Rechnersysteme miteinander verbunden.

VPN bietet folgende **Sicherheitsfunktionen:**

- Verschlüsselung der übertragenen Daten
- Authentisierung einer Nachricht auf dessen Echtheit bzw. Unverfälschtheit
- Authentisierung der Kommunikationspartner
- Verwaltung der verwendeten Schlüssel für die Verschlüsselung und Authentisierung

In einem VPN kommt i. d. R. das standardisierte Sicherheitsprotokoll **IPsec** zum Einsatz. Dieses bietet je nach Bedarf unterschiedliche Verschlüsselungsroutinen: Während für die Verschlüsselung der Daten der **Advanced Encryption Standard (AES)** zum Einsatz kommt, wird für den sicheren Austausch der Schlüssel zwischen zwei Kommunikationspartnern meistens das **Diffie-Hellman-Protokoll** eingesetzt. Für die Datenübertragung bietet IPSec zudem folgende Sicherheitsoptionen:

- **Authentication Header (AH)** gewährleistet die Authentizität und Integrität der Datenpakete.
- **Encapsulated Security Payload (ESP)** gewährleistet die Verschlüsselung der Datenpakete.

Die meisten VPNs laufen eingebettet auf einem Router und sind eng mit dem Hersteller und dem entsprechenden Produkt verzahnt. **OpenVPN** dagegen ist eine auf Open Source basierende Softwarelösung, die auf einem Rechner im Netzwerk betrieben werden kann.