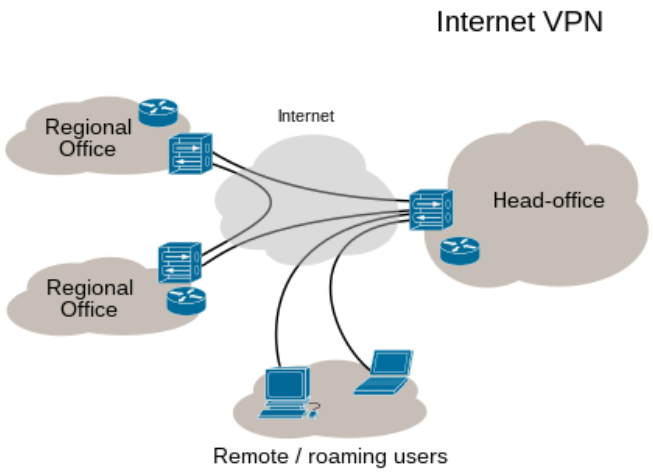
WIKIPEDIA

Virtual Private Network

Virtual Private Network (deutsch „virtuelles privates Netzwerk“; *kurz*: **VPN**) bezeichnet eine Netzwerkverbindung, die von Unbeteiligten nicht einsehbar ist, und hat zwei unterschiedliche Bedeutungen:

- Das konventionelle VPN bezeichnet ein virtuelles privates (in sich geschlossenes) Kommunikationsnetz. Virtuell in dem Sinne, dass es sich nicht um eine eigene physische Verbindung handelt, sondern um ein bestehendes Kommunikationsnetz, das als Transportmedium verwendet wird. Das VPN dient dazu, Teilnehmer des bestehenden Kommunikationsnetzes an ein anderes Netz zu binden.[1]
  So kann beispielsweise der Computer eines Mitarbeiters von zu Hause aus Zugriff auf das Firmennetz erlangen, gerade so, als säße er mittendrin. Aus Sicht der VPN-Verbindung werden dafür die dazwischen liegenden Netze (sein Heimnetz sowie das Internet) auf die Funktion eines Verlängerungskabels reduziert, das den Computer (*VPN-Partner*) ausschließlich mit dem zugeordneten Netz verbindet (*VPN-Gateway*). Er wird nun zum Bestandteil dieses Netzes und hat direkten Zugriff darauf. Die Auswirkung ist vergleichbar mit dem Umstecken des Computer-Netzwerkkabels an das per VPN zugeordnete Netz.
  Dieser Vorgang funktioniert unabhängig von der physischen Topologie und den verwendeten Netzwerkprotokollen selbst dann, wenn das zugeordnete Netz von einer vollkommen anderen Art ist.[1]
  Der sich daraus ergebende Nutzen eines VPNs kann je nach verwendetem VPN-Protokoll durch eine Verschlüsselung ergänzt werden, die eine abhör- und manipulationssichere Kommunikation zwischen den VPN-Partnern ermöglicht.[2]
  Ein verschlüsseltes (virtuelles) Netzwerk über ein unverschlüsseltes Netzwerk herzustellen, kann ein wichtiges Kriterium, mitunter sogar der Hauptgrund für die Verwendung eines VPNs sein.
- SSL-VPN (auch *Web-basierendes VPN*) unterstützt seit 2002 Lösungen, die einen verschlüsselten Fernzugriff auf Unternehmensanwendungen und gemeinsam genutzte Ressourcen realisieren, ohne dass sich die SSL-VPN-Partner dafür an das Unternehmensnetz binden.[3] Hier wird sinnbildlich also nicht das Netzwerkkabel an ein anderes Netz angeschlossen; es wird lediglich ein gesicherter Zugriff auf bestimmte Dienste des anderen Netzes ermöglicht.
  Der Namensbestandteil „VPN“ für diese Lösungen ist umstritten, aber auf dem Markt üblich.[4][5][6] Technisch gesehen basieren sie auf einem Proxy-Mechanismus (*Thin Client SSL VPN*) oder darauf, dass die begehrte Unternehmensanwendung selbst eine Webanwendung ist (*Clientless SSL VPN*), auf die ein SSL-VPN-Partner über eine gesicherte Verbindung zugreifen kann, ohne jedoch einen direkten Zugriff auf das Unternehmensnetz zu erhalten.[7] Darüber hinaus unterstützt SSL-VPN auch einen VPN-Modus im Sinne des konventionellen VPNs (*Fat Client SSL VPN*).[7]

Inhaltsverzeichnis



Struktur eines konventionellen VPNs: Unten abgebildet sind Heimarbeitsplätze („Remote / roaming users“), die sich per VPN durch das Internet hindurch in den Hauptsitz einer Firma einwählen („Head-office“), wobei der blaue Kasten ein *VPN-Gateway* ist (auch *VPN-Einwahlknoten* genannt). Darüber hinaus ist der Hauptsitz per VPN auch mit zwei seiner Filialen verbunden („Regional Office“), wobei das dazwischen liegende Netz auch hier das Internet ist, das dem VPN als Transportweg dient (aus Sicht der VPN-Verbindung wird das Internet auf die Funktion eines Verlängerungskabels reduziert).

Einzelnachweise

Konventionelle VPNs

Grundlagen

Das Netz, an das ein VPN seine Teilnehmer bindet, wird teilweise auch ein *zugeordnetes Netz* genannt. Das zugeordnete Netz kann in einem physischen Netz münden, in das externe Geräte mit Hilfe von VPN über ein spezielles (VPN-)Gateway aufgenommen werden („End-to-Site“-VPN).[8] Die *VPN-Partner* werden dadurch zum Bestandteil des zugeordneten Netzes und sind nun von dort aus direkt adressierbar – praktisch so, als befänden sie sich mittendrin. Aufgrund dieser Illusion spricht man bezüglich der VPN-Partner von einem *virtuellen* Netz.

Das Gateway kann auch auf ein rein virtuelles Netz zeigen, welches lediglich aus weiteren VPN-Partnern besteht („End-to-End“-VPN).[9]

Daneben besteht die Möglichkeit, zwei zueinander kompatible Netzwerke, die an ein und demselben benachbarten Netz angrenzen, miteinander zu verbinden („Site-to-Site“-VPN),[10] wobei auch hier das dazwischen liegende benachbarte Netz von einer vollkommen anderen Art sein kann.[1]

Gegenseitig erreichbare Netze

Sobald mindestens zwei separate Netzwerke über ein Gerät miteinander verbunden sind, handelt es sich um gegenseitig erreichbare Netze. Das Verbindungsgerät ermöglicht eine Kommunikation zwischen den Netzwerken und könnte zum Beispiel ein (NAT-)Router oder ein Gateway sein; bei rein virtuellen Netzen (die in einem anderen Netz eingebettet sind) kann auch einer der Teilnehmer diese Funktion übernehmen.

Beispielsweise kann das Verbindungsgerät ein DSL-Router sein, der ein Firmennetz mit dem Internet verbindet. Dank dieses Gerätes kann ein Arbeitsplatzcomputer auch Internetseiten aufrufen. Die Zugriffsmöglichkeit der im Internet befindlichen Teilnehmer auf das Firmennetz bleibt dabei eingeschränkt; im Unterschied zu einem direkt am Firmennetz angeschlossenen Teilnehmer kann ein am Internet angeschlossener Teilnehmer nicht einfach auf alle Netzwerkressourcen der Firma zugreifen (wie Datei- und Druckerfreigaben). Hierfür müsste er am Firmennetz angeschlossen sein. Genau das lässt sich über ein VPN realisieren, wobei sich die Zugriffserlaubnis auf bestimmte Teilnehmer einschränken lässt.

In der klassischen VPN-Konfiguration spielt das Verbindungsgerät eine zentrale Rolle; auf ihm wird eine VPN-Software installiert. Das verbindende Gerät wird dadurch – zusätzlich zu seiner bisherigen Funktion – zu einem *VPN-Gateway* (auch *VPN-Einwahlknoten*).

Routing mit VPN

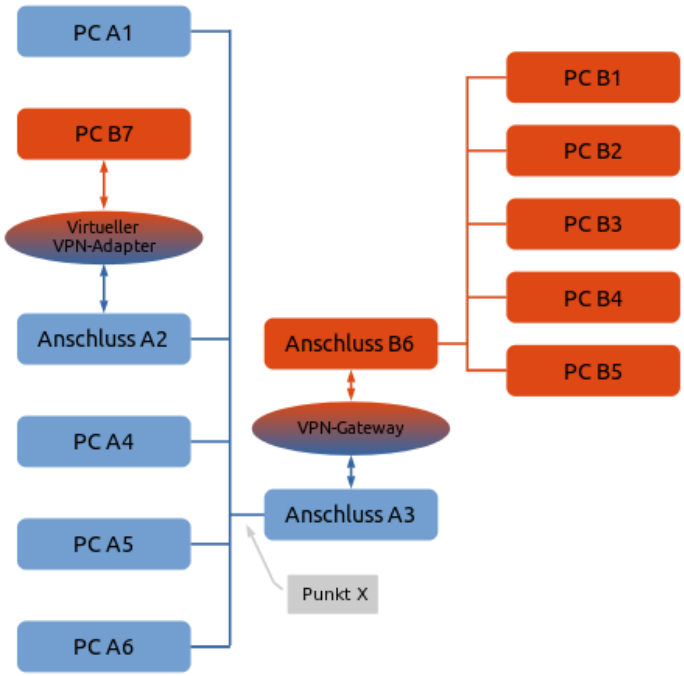
In der Beispielabbildung könnte `Netz A` ein Heimnetzwerk sein, `Netz B` das Internet und `Netz C` ein Firmennetz. Wenn eine Kommunikation mit dem jeweils angrenzenden Netz bis hin zum VPN-Einwahlknoten möglich ist, funktioniert VPN über mehrere Netzwerke hinweg – so können sich also nicht nur Teilnehmer aus `Netz B`, sondern auch Teilnehmer aus `Netz A` per VPN in `Netz C` einwählen.

VPN ist ein reines Softwareprodukt

Die gegenseitig erreichbaren Netze bilden zusammen die Hardware (die Geräte selbst, zuzüglich Kabel) und Software, die wiederum von den Geräten benötigt wird, um ihnen „zu sagen“, was sie überhaupt machen sollen.

Um einen Teilnehmer aus seinem ursprünglichen Netz heraus an ein von dort aus erreichbares Netz zu binden, wird eine VPN-Software benötigt. In der klassischen Konfiguration wird sie zum einen auf dem Gerät installiert, das die Netzwerke miteinander verbindet, und zum anderen auf den einzubindendenen Teilnehmer gebracht. VPN funktioniert, ohne dass dafür ein zusätzliches Kabel verlegt oder sonst irgendetwas an Hardware hinzugefügt werden muss. Vom Konzept her ist VPN daher ein reines Softwareprodukt.[11] Allerdings bedeutet das nicht, dass VPN nicht auch mit separaten Geräten umgesetzt werden *kann*, die für eine solche Lösung optimiert sind. So gibt es Hardware, sogenannte VPN-Appliances, die auf einem speziell gesicherten (gehärteten) Betriebssystem aufsetzen und in denen zum Beispiel ein entsprechender Hardware-Entwurf dabei hilft, Teile der (optionalen) Verschlüsselung zu beschleunigen. Das Hinzuziehen von speziellen VPN-Geräten kann eine durchaus sinnvolle Maßnahme sein. Dennoch ist dies nur eine Option, da sich VPN auch ohne diese Geräte umsetzen lässt.

Funktionsweise



Ein VPN-Partner aus Netz A hat sich in das Netz B eingewählt und kommuniziert mit B2.
Netz A
Netz B

Bezogen auf die Beispielabbildung läuft auf dem Gerät mit `Netzwerk-Anschluss A2` eine VPN-Client-Software, die dem Gerät das `Netz B` zuordnet. Aus vormals `PC A2` wird dadurch der „`Netz B`“-Teilnehmer `PC B7`, unser *VPN-Partner*.

Dieser VPN-Partner schickt nun eine Nachricht an beispielsweise `PC B2`. Die Nachricht wird zur Weiterleitung an den `VPN-Adapter` übergeben, der Teil der VPN-Client-Software ist. Er steckt die Nachricht bildlich gesehen in einen Briefumschlag (Adresse=„`PC B2`“, Absender=„`PC B7`“) und übergibt den Brief dann an `Netzwerk-Anschluss A2`. Dabei wird der Brief in einen weiteren Briefumschlag gesteckt (Adresse=„`Netzwerk-Anschluss A3`“ (`VPN-Gateway`), Absender=„`Netzwerk-Anschluss A2`“) und so dem `Netz A` übergeben.

Der Trick besteht also darin, dass sich die VPN-Pakete unabhängig von ihrem Inhalt und der ursprünglichen Adressierung (innerer Briefumschlag) separat adressieren lassen (äußerer Briefumschlag), um den Brief in einer Form auf den Weg zu bringen, die kompatibel zu `Netz A` ist. Technisch gesehen werden die ursprünglichen Netzwerkpakete (innerer Brief) für den Transport in ein VPN-Protokoll gelegt. Daher spricht man bei VPN vom Tunnel.[12][2]

Der `Netzwerk-Anschluss A3` nimmt den Brief entgegen und übergibt ihn der Software „`VPN-Gateway`“, die auf dem Gerät läuft. Diese Software entfernt den äußeren Briefumschlag und leitet den inneren Brief weiter in das Netz von `Netzwerk-Anschluss B6` hin zum `PC B2` (dem Adressaten des inneren Briefumschlags).

Seine Antwort schickt `PC B2` zurück an `PC B7`. Der `Netzwerk-Anschluss B6` fängt den Brief ab, weil das `VPN-Gateway` erkennt, dass die „`PC B7`“-Adresse zu einem seiner VPN-Partner gehört. Auch dieser Brief wird vom `VPN-Gateway` bildlich gesehen in einen zweiten Briefumschlag gesteckt (Adresse=„`Netzwerk-Anschluss A2`“, Absender=„`Netzwerk-Anschluss A3`“) und in das `Netz A` geleitet. Der `Netzwerk-Anschluss A2` nimmt den Brief entgegen und übergibt ihn dem `VPN-Adapter`. Dieser entfernt den äußeren Briefumschlag und übergibt den inneren Brief an `PC B7`.

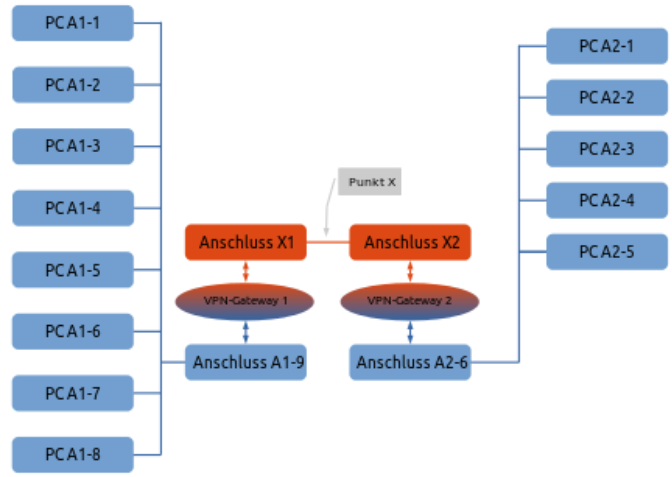
Stark vereinfacht ausgedrückt wurde das `Netz A` aus Sicht des VPN-Partners auf die Funktion eines Verlängerungskabels reduziert, das `PC B7` direkt mit dem `Netz B` verbindet. Für beide Kommunikationspartner, `PC B7` und `PC B2`, sieht es also so aus, als befände sich `PC B7` mitten im `Netz B` und nicht im `Netz A`. Sie bekommen von den dazwischen liegenden Mechanismen nichts mit.

Der sich daraus ergebende Nutzen eines VPNs kann je nach verwendetem VPN-Protokoll durch eine Verschlüsselung ergänzt werden, die dafür sorgt, dass die Kommunikation zwischen `PC B7` und dem `VPN-Gateway` von niemanden aus `Netz A` eingesehen oder gar manipuliert werden kann. Diese optionale VPN-Verschlüsselung ist Bestandteil des äußeren Briefumschlags. Sie reicht also nicht in das `Netz B` hinein, sondern endet bzw. beginnt (Rückweg) am `VPN-Gateway`.

In einer realen Umgebung könnte `Netz B` beispielsweise ein Firmennetz sein und `Netz A` das Internet (in einer hier stark vereinfachten Darstellung), über das sich ein direkt an das Internet angeschlossenes Gerät per VPN in die Firma einwählt. Alternativ dazu könnte `Netz A` auch das private Heim-Netzwerk des Mitarbeiters sein, wobei das Internet dann zwischen `Netz A` und `Netz B` liegen würde (in der Beispielabbildung bezeichnet als „`Punkt X`“). An dieser Stelle können sich durchaus auch mehrere dazwischen liegende Netze befinden, die der Brief dank des äußeren Briefumschlags passieren wird, ehe er zum `VPN-Gateway` gelangt.

VPN funktioniert weitgehend unabhängig von der physischen Topologie und den verwendeten Netzwerkprotokollen auch dann, wenn das zugeordnete `Netz B` von einer vollkommen anderen Art ist. Denn da die tatsächlichen Netzwerkpakete in dem VPN-Protokoll verpackt sind, müssen sie (die inneren Briefe, also die „`Netz B`“-Netzwerkprotokolle) nur von den VPN-Partnern verstanden werden, nicht aber von den dazwischen liegenden Netzwerkkomponenten aus `Netz A`. Diese müssen lediglich die Transportdaten des äußeren Briefumschlags verstehen, also das für den Transport verwendete Netzwerkprotokoll kennen.

Netzwerke verbinden



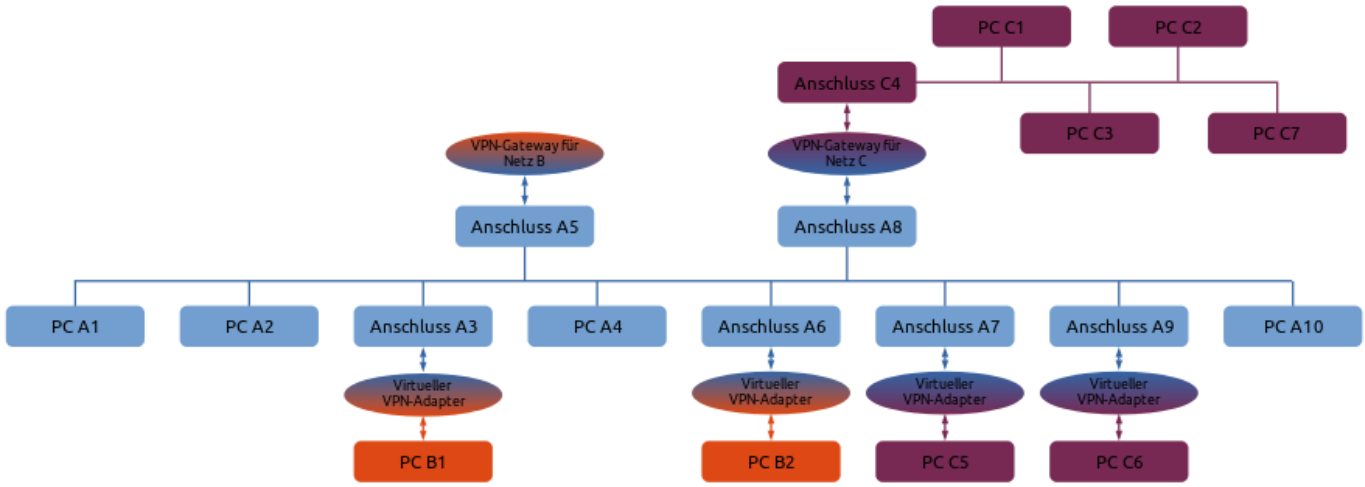
Zwei Filialen sind über ein oder mehrere benachbarte Netze per VPN miteinander verbunden.

Netz A
Netz X

Gegenüber anderen Tunnelarten eines TCP/IP-Netzes zeichnet sich der VPN-Tunnel dadurch aus, dass er unabhängig von höheren Protokollen (HTTP, FTP etc.) *sämtliche* Netzwerkpakete weiterleitet. Auf diese Weise ist es möglich, den Datenverkehr zweier Netzkomponenten praktisch uneingeschränkt durch ein anderes Netz zu transportieren, weshalb damit sogar komplette Netzwerke über ein oder mehrere benachbarte Netze hinweg (in der Abbildung bezeichnet als `Punkt X`) miteinander verbunden werden können. So kann zum Beispiel auch eine Datenbankverbindung auf dem entfernten Rechner verwendet werden.

Sobald das `VPN-Gateway 1` erkennt, dass eine Nachricht an einen Teilnehmer aus `Filiale 2` gerichtet ist (`PC A2-...`), wird sie gemäß der oben beschriebenen Funktionsweise sinnbildlich in den zweiten Briefumschlag gesteckt und an `VPN-Gateway 2` geschickt. Erkennt dagegen `VPN-Gateway 2`, dass eine Nachricht an einen Teilnehmer aus `Filiale 1` gerichtet ist (`PC A1-...`), schickt er diese nach demselben Prinzip zum `VPN-Gateway 1`.

Gekapseltes Netz



Verkapselung von drei Netzwerken.

Netz A
Netz B
Netz C

In der Beispielabbildung befinden sich in `Netz A` neben seinen üblichen Teilnehmern (z. B. `A1`) auch zwei virtuelle Netze (hier `Netz B` und `Netz C`). Jedes davon ist ein privates (in sich geschlossenes) Netz, das seinen eigenen Regeln folgt, angefangen von der Art der Adressierung und Aufteilung bis hin zum verwendeten Kommunikationsprotokoll. Dennoch teilen sie sich (zumindest teilweise) dieselbe physische Leitung und Infrastruktur, was gemäß der oben beschriebenen Funktionsweise sinnbildlich durch den zweiten Briefumschlag ermöglicht wird.

Bezogen auf die `VPN-Partner`, inklusive des `VPN-Gateway`, kann man sagen, VPN ist ein eigenständiges Netz, gekapselt in einem anderen Netz.

Das kann sich auf das komplette Netz beziehen, wenn es ausschließlich aus VPN-Partnern besteht, wie das in `Netz B` der Fall ist. Es kann sich aber auch auf nur einen Teil der Kommunikationsstrecke beziehen, wie das in `Netz C` der Fall ist. Dort mündet das VPN in einem eigenen physischen Netz; bei der Kommunikation eines direkt am `Netz C` angeschlossenen Teilnehmers (z. B. `C1`) mit einem „`Netz C`“-VPN-Partner (z. B. `C6`) beginnt bzw. endet (Rückweg) die Kapselung hier am `VPN-Gateway`.

Ihrem Ursprung nach bilden VPNs innerhalb eines öffentlichen Wählnetzes solche in sich geschlossenen virtuellen Netze.[1] Das sind unter anderem Netze der Sprachkommunikation, X.25, Frame Relay und ISDN,[12] die dank dieses Konzepts über ein und dieselbe physische Infrastruktur, das öffentliche Wählnetz, parallel betrieben werden können.[1] Sie sind zwar physisch (zumindest teilweise) in dem darüber liegenden Wählnetz eingebettet, aber für die Teilnehmer sieht es so aus, als würde jedes Netz über seine eigene Leitung verfügen.

Heute wird VPN alltagssprachlich gebraucht, um ein (meist verschlüsseltes) virtuelles IP-Netz zu bezeichnen, welches nicht in einem Wählnetz, sondern innerhalb eines anderen IP-Netzes (meist dem öffentlichen Internet) eingebettet ist.[12]

Eigenschaften eines VPNs

VPN bildet ein eigenes logisches Netz, welches sich in ein physisches Netz einbettet und die dort üblichen Adressierungsmechanismen nutzt, datentechnisch aber eigene Netzwerkpakete transportiert und so vom Rest dieses Netzes losgelöst arbeitet. Es ermöglicht die Kommunikation der darin befindlichen VPN-Partner mit dem zugeordneten Netz, basiert auf einer Tunneltechnik, ist individuell konfigurierbar, kundenspezifisch und in sich geschlossen (daher „privat“).[1]

Praktischer Nutzen eines VPNs

Sobald ein Computer eine VPN-Verbindung aufbaut, ist der Vorgang vergleichbar mit dem Umstecken seines Netzwerkkabels von seinem ursprünglichen Netz an das neu zugeordnete Netz, mit allen Auswirkungen wie geänderten IP-Adressen und Unterschieden beim Routing.

Ruft der Computer zum Beispiel eine Webseite auf, so wird die Anfrage nun aus dem neu zugeordneten Netz heraus in das Internet geleitet. Die Anfrage unterliegt so den Restriktionen des zugeordneten Netzes und nicht mehr denen des ursprünglichen Netzes. Das nutzen zum Beispiel Journalisten in Ländern, in denen der freie Zugriff auf das Internet nicht möglich ist, um die Zugriffsbeschränkung zu umgehen. Die einzige Voraussetzung besteht darin, dass der Computer aus seinem ursprünglichen Netz heraus eine Verbindung zum VPN-Gateway aufbauen kann. Das VPN-Gateway befindet sich hierfür in der Regel in einem anderen Land bzw. einem Netz mit freiem Internetzugang. Man spricht davon, dass die Internetanfragen (wie auch sämtliche weitere Netzwerkanfragen) über VPN *getunnelt* werden.

Ein weiterer Grund, um Internetzugriffe zu tunneln, besteht im Schutz der Privatsphäre. Für das Handy, das Notebook, Tablets und andere Geräte gilt gleichermaßen, dass der Datenverkehr von Dritten leicht mitgelesen werden kann, sobald für den Internetzugriff ein öffentlicher Zugang genutzt wird. Nicht jeder Zugriff lässt sich über den direkten Weg verschlüsselt aufbauen, und selbst wenn der Anwender für

bestimmte Vorgänge eine verschlüsselte Verbindung nutzt, bleibt die Information, wohin er eine Verbindung aufgebaut hat, einsehbar. Ein VPN-Tunnel löst beide Probleme, da (je nach VPN-Protokoll) hier eine Verschlüsselung *sämtlicher* Netzwerkpakete bis zum Ausgang des VPN-Tunnels möglich ist. Zudem kann derjenige, der den Datenverkehr des öffentlichen Zugangs möglicherweise mitliest, nur noch eine Verbindung zum VPN-Gateway erkennen. Das tatsächliche Ziel bleibt ihm verborgen, da er nicht einsehen kann, wohin von dort aus die Verbindung weitergeleitet wird.

Dies sind lediglich zwei Beispiele, die zum einen den Nutzen bezüglich des Netzwerkwechsels aufzeigen und zum anderen auf den Nutzen einer möglichen Verschlüsselung eingehen. Die sich daraus ergebenden Anwendungsmöglichkeiten sind vielfältig.

Anwendungsmöglichkeiten

- Über VPN können lokale Netze mehrerer Geschäftsstellen über das Internet auf eine sichere Art miteinander verbunden werden (eine sogenannte *Site-to-Site*-Verbindung).
- Der Computer eines Mitarbeiters kann über VPN von zuhause aus einen gesicherten Zugriff auf das Firmennetz erlangen. Dazu baut er eine Verbindung zum Internet auf. Dann startet er eine VPN-Software (den VPN-Client, der die Beschaffenheit des Firmennetzes auf dem lokalen Computer virtuell nachbildet). Diese baut über das Internet eine Verbindung zum VPN-Gateway der Firma auf. Nach der Authentifizierung hat der Mitarbeiter Zugriff auf das Firmennetz – gerade so, als säße er mittendrin. Diese Verbindungsart wird *End-to-Site* genannt. Das Verfahren wird auch verwendet, um WLAN und andere Funkstrecken zu sichern.
- In Abgrenzung zum End-to-Site-VPN wird von einigen Herstellern (zum Beispiel bei MSDN,[13] bei VoIP-Info.de,[14] auf tomsnetworking.de[15]) Mobile VPN als Bezeichnung für ein VPN genutzt, welches nahtloses Roaming zwischen zum Beispiel GPRS, UMTS und WLAN unterstützt. Dadurch soll eine dauerhafte Netzwerkverbindung ohne ständiges Neueinwählen ermöglicht werden.
- Es ist auch möglich, dass sich der Rechner des Mitarbeiters per VPN nicht in ein entferntes physisches Firmennetz hängt, sondern direkt an einen Server bindet. VPN dient hier dem gesicherten Zugriff auf den Server. Diese Verbindungsart wird *Ende-zu-Ende* (englisch *end-to-end*) genannt. Auf diese Weise ist es auch möglich, ein logisch (jedoch nicht physisch) abgekapseltes virtuelles Netz aufzubauen, welches lediglich aus weiteren VPN-Partnern besteht, die sich ebenfalls mit dem Server verbunden haben. Die VPN-Partner können nun gesichert miteinander kommunizieren.
- Es besteht auch die Möglichkeit, dass sich zwei Server über VPN miteinander unterhalten können, ohne dass die Kommunikation durch Dritte eingesehen werden kann (das entspricht einer Ende-zu-Ende-Verbindung, welche für einen solchen Fall mitunter auch *Host-to-Host* genannt wird).
  FreeS/WAN sowie dessen Nachfolger Openswan und strongSwan bieten noch die Möglichkeit der sogenannten *„opportunistic encryption“*: Es wird zu jedem Computer, mit dem der eigene Computer Daten austauscht, ein Tunnel aufgebaut, wenn dieser einen Schlüssel per DNS bereitstellt.
- Ähnlich wie bei der Einwahl von zu Hause in ein Firmennetz können sich auch beliebige Clients aus dem Firmennetz in ein separates, speziell gesichertes Netz innerhalb der Firma per VPN einwählen: ein privates (datentechnisch abgekapseltes) Netz innerhalb des Firmennetzes also, bei dem die Clients bis zum VPN-Gateway dieselbe physikalische Leitung verwenden wie alle anderen Clients des Netzes auch – mit dem Unterschied, dass sämtliche VPN-Netzpakete bis zum Gateway verschlüsselt übertragen werden können.
- Computerspiele, deren originale Infrastruktur über das Internet nicht mehr verfügbar ist, die aber einen LAN-basierten Mehrspielermodus haben, können mithilfe von VPN weiter über das Internet gespielt werden. VPN-Lösungen für diesen Zweck sind z. B. LogMeIn Hamachi und Tunngle.
- Bei der frei verfügbaren Spieleplattform Voobly, die eine einfache Administration von Multiplayerspielen bietet (vorwiegend Age of Empires II), kann bei Benutzung eines VPNs der „Fast Proxy“ verhindert werden. Dies ist vor allem für Spieler hilfreich, in deren lokalen Netzwerk NAT aktiviert ist.

Sicherheit

Durch die Verwendung von Passwörtern, öffentlichen Schlüsseln oder durch ein digitales Zertifikat kann die Authentifizierung der VPN-Endpunkte gewährleistet werden. Daneben werden auch Hardware-basierte Systeme wie bei SecurID angeboten.

Verschlüsselung

Abhängig vom verwendeten VPN-Protokoll lassen sich die Netzwerkpakete meist verschlüsseln. Da die Verbindung dadurch abhör- und manipulationssicher wird, kann eine Verbindung zum VPN-Partner durch ein unsicheres Netz hindurch aufgebaut werden, ohne dabei ein erhöhtes Sicherheitsrisiko einzugehen.[2] Alternativ dazu lassen sich über VPN auch ungesicherte Klartextverbindungen aufbauen.[1][2]

Einbeziehung fremder Computer in das VPN

Bestimmte VPN-Verbindungen werden unter Einbindung separat betriebener Server hergestellt. Dieses dient u. a. dazu, die gegenseitige Erreichbarkeit der per VPN verbundenen Teilnetze auch mit wechselnden IP-Adressen für den Anwender einfach zu gestalten. Auch bei nicht genutzter VPN-Verbindung kommt es vor, dass mit solcher VPN-Software installierte Hintergrundprogramme fortwährend Daten mit

dem extern betriebenen Server austauschen. Die Umleitung sensibler Daten durch solch ein System erfordert eine Beurteilung der zusätzlich entstehenden Risiken für die Datensicherheit, z. B. hinsichtlich Standort und Vertrauenswürdigkeit des Diensteanbieters sowie zu benutzender Verschlüsselungsverfahren.

Wechselwirkung mit anderen Sicherheitskomponenten

Die Software zur Herstellung der VPN-Verbindung funktioniert unabhängig von bestimmten Sicherheitseinstellungen des physikalisch für den Verbindungsaufbau benutzten Geräts. Z. B. kann eine Software in den Firewall-Einstellungen eines Routers ausdrücklich davon ausgenommen werden, Internetverbindungen verwenden zu dürfen, jedoch trotzdem die VPN-Verbindung herstellen.

Grenzen des VPN

Allerdings lässt sich auch an den verschlüsselten Paketen erkennen, welche VPN-Gegenstellen an der Kommunikation beteiligt sind; die Zahl und Größe der Datenpakete lässt u. U. Rückschlüsse auf die Art der Daten zu.[16] Daher ist diesbezüglich ein mitunter verwendetes Gleichnis mit einem *nicht einsehbaren Tunnel* irreführend; ein Vergleich mit einer Milchglasröhre ist treffender. Auch wenn die Einrichtung eines VPN mit moderner Software einfach und schnell durchzuführen ist, erfordert der Betrieb eines VPN stets eine sachkundig durchgeführte Risikobeurteilung hinsichtlich der Datensicherheit.

Implementierungen

VPNs setzen auf folgenden zugrunde liegenden Protokollen auf:

- DMVPN für den Aufbau von IPsec-basierten VPNs.
- fastd von Matthias Schiffer geschriebenes auf Layer 2 oder Layer 3 operierendes VPN mit kleinem Ressourcenbedarf und daher guter Eignung für eingebettete Systeme, insbesondere bei Mesh-Netzwerken wie z. B. Freifunk.
- getVPN von Firma Cisco entwickelte Methode die IPsec-Tunnel mit Hilfe eines zentralen Schlüsselservers auf allen zum Verbund gehörenden Routern praktisch automatisch einzurichten.
- IPsec eignet sich sowohl für Site-to-Site-VPNs als auch für End-to-Site-VPNs.
- PPPD (PPP-Daemon) und SSH in Kombination kann den gesamten IP-Verkehr durch einen Tunnel leiten. Die Lösung ist ähnlich dem PPTP ohne dessen Sicherheitsprobleme.
- PPTP (gebrochen) und L2TP (Layer-2-VPN-Protokolle)
- SSTP von Microsoft in Windows Server 2008 und Windows Vista Service Pack 1 eingeführtes Secure Socket Tunneling Protocol. SSTP tunnelt den PPP- oder L2TP-Verkehr durch einen SSL-3.0-Kanal.[17]
- TLS/SSL werden hauptsächlich für End-to-Site-VPNs eingesetzt.
- ViPNet eignet sich besonders für End-to-End-VPNs, erlaubt aber auch End-to-Site- und Site-to-Site-VPNs.
- SVR eignet sich für Site-to-Site-VPNs, dass sitzungsbasierte Konzept wurde vom SBC abgeleitet[18]

Viele moderne Betriebssysteme enthalten Komponenten, mit deren Hilfe ein VPN aufgebaut werden kann. Linux enthält seit Kernel 2.6 eine IPsec-Implementierung, ältere Kernel benötigen das KLIPS-IPsec-Kernelmodul, das von *Openswan* und *strongSwan* zur Verfügung gestellt wird. Auch BSD, Cisco IOS, z/OS, macOS und Windows sind IPsec-fähig.

Siehe auch: SSL-VPN, OpenVPN, CIPE

Der virtuelle Netzwerkadapter einer VPN-Sitzung

Die eingesetzte VPN-Software stellt den Eingang zum VPN-Tunnel üblicherweise als zusätzlichen virtuellen (nicht als Hardware vorhandenen) Netzwerkadapter bereit. Auf diese Weise besteht aus Sicht des Betriebssystems und der Anwendungssoftware kein Unterschied zwischen dem VPN-Tunnel und einem physikalisch vorhandenen Netzwerk. Der virtuelle Netzwerkadapter kann genauso in das Routing einbezogen werden wie der echte Netzwerkadapter und kann genau wie dieser Pakete aller Dienste transportieren.

Geschlossener Tunnel
: Dabei kann die Defaultroute (Standard-Gateway) auf den VPN-Netzwerkadapter verändert werden. Dies ist oft erwünscht, weil so sichergestellt ist, dass tatsächlich *alle* Verbindungen der Anwendungssoftware über den VPN-Netzwerkadapter und damit in die VPN-Software geleitet werden, die sie verschlüsselt, bevor sie danach über einen als Hardware vorhandenen Netzwerkadapter gezielt aus dem Rechner zur VPN-Gegenstelle (VPN-Gateway/-Einwahlknoten) geschickt werden. Dabei sind Internetanfragen noch immer möglich, allerdings nicht mehr direkt. Diese werden jetzt zunächst in das zugeordnete Netz geleitet (z. B. das Firmennetz). Erlaubt das zugeordnete Netz den Internetzugriff, so wird von dort aus die Anfrage an den kontaktierten Internetserver geschickt. Abhängig von der Art der Internetschnittstelle bemerkt der Anwender diesen Unterschied mitunter nicht einmal (für ihn sieht es so aus, als könne er noch immer direkt auf das Internet zugreifen).

Split Tunneling
: Schwierigkeiten ergeben sich, wenn man nur einzelne Kommunikationspartner über den VPN-Tunnel erreichen will (z. B. Rechner eines Firmennetzwerks), parallel aber andere Kommunikationspartner ohne VPN ansprechen muss

(Drucker oder Rechner im eigenen LAN). Hier muss man die Routingtabellen für das Erreichen des Firmennetzwerkes entsprechend anpassen und die Defaultroute auf den in Hardware vorhandenen Netzwerkadapter belassen.
Wenn die VPN-Software den zu benutzenden Nameserver auf einen Nameserver im VPN umstellt, besteht die Schwierigkeit darin, dass dieser keine Namen außerhalb des VPNs auflösen kann. Auch hier ist eine Konfiguration von Hand nötig, indem dem Netzwerkadapter ein weiterer Namensserver des eigenen LANs hinzugefügt wird. Dabei kann jedoch ein sogenannter DNS-Leak entstehen, der eine Identifizierung des Benutzers von einer Seite außerhalb des Netzwerks ermöglicht. Dies passiert, wenn die Anfragen zur Namensauflösung nicht zuerst über das gesicherte, sondern weiterhin über das ungesicherte Netz erfolgen. In diesem Fall besteht – trotz VPN-Verbindung – für eine Seite außerhalb des Netzwerks die Möglichkeit des Mitschneidens der kompletten Anfrage. Folglich ist es daher möglich, die IP-Adresse des Nutzers auszulesen.[16] Die Behebung des Problems lässt sich bewerkstelligen, indem dem Netzwerkadapter ein DNS-Server aus dem VPN-Netz zugewiesen wird, der eine höhere Priorisierung hat als der DNS-Server des eigenen LANs.[19]
Siehe auch: Split Tunneling

Nachteile eines VPNs

Die Nutzung eines VPN-Service bedeutet zusätzlichen Aufwand, da die gesamte Kommunikation verschlüsselt wird. Aus diesem Grund ist die Bandbreite bei der Verwendung von VPN immer etwas höher. Wie groß der Performanceunterschied ist, hängt vor allem vom verwendeten VPN-Service und der Entfernung des Providers ab.

Trotz der Benutzung von VPN kann der Nutzer nicht von einer hundertprozentigen Anonymität ausgehen. Für den VPN-Provider besteht die Möglichkeit, die gesamten Aktivitäten, die über seinen Server laufen, nachzuvollziehen. Außerdem gibt es das Risiko eines Datenleaks auf Seiten des VPN-Servers. Deswegen spielt die Vertrauenswürdigkeit des Providers besonders bei sensiblen Daten eine große Rolle.[20]

Das von der Mozilla Foundation 2021 für Deutschland geplante VPN unter Nutzung der Software von Mullvad und WireGuard wird voraussichtlich – wie in anderen Ländern auch – kostenpflichtig sein.[21]

VPN auf Routern

Mit dem zunehmenden Einsatz von VPNs haben viele Unternehmen begonnen, VPN-Konnektivität auf Routern für zusätzliche Sicherheit und Verschlüsselung der Datenübertragung unter Verwendung verschiedener kryptographischer Techniken einzusetzen.[22] Heimanwender setzen VPNs in der Regel auf ihren Routern ein[23], um Geräte wie Smart TVs oder Spielekonsolen zu schützen, die nicht von einheimischen VPN-Clients unterstützt werden. Unterstützte Geräte sind nicht auf diejenigen beschränkt, die einen VPN-Client ausführen können.[24]

Viele Routerhersteller liefern Router mit integrierten VPN-Clients aus. Einige verwenden Open-Source-Firmware wie *DD-WRT*, *OpenWRT* und *Tomato*, um zusätzliche Protokolle wie *OpenVPN* zu unterstützen.

SSL-VPNs

→ *Hauptartikel: SSL-VPN*

SSL-VPNs nutzen das gesicherte SSL- oder TLS-Protokoll für die Übertragung ihrer Daten.[25]

Auch wenn hier ein vollumfängliches VPN im Sinne des konventionellen VPNs möglich ist, wurden *Site-to-Site*-Lösungen fast vollständig von IPsec-basierenden VPNs abgelöst.

Das gilt jedoch nicht für *End-to-Site*-VPNs. Ein sogenannter **Fat Client SSL VPN** (ein vollumfängliches konventionelles VPN) kann beispielsweise einem mobilen Computer Zugang auf ein Firmennetz verschaffen. Dies ist eine gebräuchliche VPN-Variante, weil das auch in Umgebungen funktioniert, in denen ein Mitarbeiter aufgrund der Beschränkungen bei einem Kunden keinen IPsec-Tunnel aufbauen kann.[7] Genau wie bei anderen konventionellen VPNs üblich, ist es auch hier notwendig, auf dem Computer eine VPN-Client-Software zu installieren, die dort das zugeordnete Netz virtuell nachbildet (siehe VPN-Adapter). Darüber ist es dann möglich, den kompletten Netzwerkverkehr der VPN-Partner über die verschlüsselte SSL-Verbindung zu übertragen und so den PC an das entfernte Netz zu binden.

Bei allen anderen SSL-VPNs entfällt die Installation der sonst üblichen VPN-Client-Software zumindest teilweise.

Ein **Thin Client SSL VPN** benötigt lediglich ein Plug-in (eine Art Erweiterungsbaustein) für einen Webbrowser, wobei der Browser auf den gängigsten Betriebssystemen bereits vorinstalliert ist. Das heruntergeladene Plugin arbeitet auf dem Client als Proxy und ermöglicht so den Zugang zu entsprechenden Netzwerkdiensten aus dem entfernten Netz.[7]

Ein **Clientless SSL VPN** greift ohne spezielle Softwareerweiterungen über einen Browser auf Webseiten des Internetservers eines Unternehmens zu.[3] Der Fernzugriff ist hierbei lediglich auf Webanwendungen des Servers möglich. Der Webserver des Unternehmens kann intern eine Umsetzung für die Kommunikation mit anderen Unternehmensanwendungen realisieren und so als Schnittstelle zu diesen Anwendungen fungieren.[7] Jedoch ist der Web-Zugriff darauf oft nur bedingt möglich, wenn diese Anwendungen nicht ebenfalls Web-basierend sind.

Siehe auch

- Mobile VPN
- Netzwerksicherheit
- Corporate Network
- VRF-Instanz
- VLAN
- DirectAccess

Literatur

- Joseph Davies, Elliot Lewis: *Virtuelle Private Netzwerke mit Windows Server 2003. (Sichere Netzwerkanbindung mit VPNs).* Microsoft Press, Unterschleißheim 2004, ISBN 3-86063-962-5 (*Fachbibliothek*).
- Kai-Oliver Detken, Evren Eren: *Extranet. VPN-Technik zum Aufbau sicherer Unternehmensnetze.* Addison-Wesley, München u. a. 2001, ISBN 3-8273-1674-X (*Datacom-Akademie*).
- Gerhard Lienemann: *Virtuelle Private Netzwerke. Aufbau und Nutzen.* Vde-Verlag, Berlin u. a. 2002, ISBN 3-8007-2638-6.
- Manfred Lipp: *VPN – Virtuelle Private Netzwerke. Aufbau und Sicherheit.* Vollständig überarbeitete und ergänzte Auflage. Addison-Wesley, München u. a. 2006, ISBN 3-8273-2252-9 (*net.com*).
- Ralf Spenneberg: *VPN mit Linux. Grundlagen und Anwendung virtueller privater Netzwerke mit Open-Source-Tools.* 2. vollständig aktualisierte Auflage. Addison-Wesley, München u. a. 2010, ISBN 978-3-8273-2515-0 (*Open Source Library*)
- Daniel Bachfeld: *VPN-Knigge*. (https://www.heise.de/security/artikel/VPN-Knigge-270796.html) In: *c't*, 07/06, S. 114

Weblinks

- Vergleich der wichtigsten Anonymisierungswerkzeuge für das Internet - Tor, JonDo, VPN und Web-Proxies. (http://artikel.softonic.de/anonym-surfen-tor-jondo-vpn-und-web-proxies-im-vergleich) 31. Juli 2013
- Risiken im Zusammenhang mit Virtuellen Privaten Netzwerken (VPN) (https://www.ncsc.admin.ch/melani/de/home/themen/vpn.html) – Informationen des Nationalen Zentrums für Cybersicherheit der schweizerischen Bundesverwaltung
- Internet: Warum VPNs für die meisten mittlerweile sinnlos und oftmals sogar problematisch sind (https://www.derstandard.at/story/2000131466992/warum-vpns-fuer-die-meisten-mittlerweile-sinnlos-und-oftmals-sogar) Artikel von Andreas Proschofsky auf derStandard.at

Einzelnachweise

1. Paul Ferguson, Geoff Huston: *What is a VPN?* (http://www.potaroo.net/papers/vpn.pdf) (PDF; 652 kB) April 1998
2. *Tunneling Protokolle für VPN* (http://www.tcp-ip-info.de/tcp_ip_und_internet/tunneling_protokolle.htm) von tcp-ip-info.de
3. *Making way for the new VPN* In: *Network World* vom 23. Dezember 2002, ISSN 0887-7661, Band 19, Nr. 51, S. 64(eingeschränkte Vorschau (https://books.google.de/books?id=QhkEAAAAMBAJ&pg=PA64#v=onepage) in der Google-Buchsuche).
4. Beispiel für Verwendung des Begriffes „VPN“ im Sinne von “Reverse Web-Proxy”: Cisco ASA: *Clientless SSL VPN (WebVPN) on ASA Configuration Example (http://www.cisco.com/en/US/products/ps6120/products_configuration_example09186a00806ea271.shtml)*. Abgerufen am 20. Oktober 2013: „Clientless SSL VPN […] A remote client needs only an SSL-enabled web browser to access http- or https-enabled web servers on the corporate LAN. […] A good example of http access is the Outlook Web Access (OWA) client.“
5. Beispiel für Verwendung des Begriffes „VPN“ im Sinne von “Reverse Web-Proxy”: Citrix Access Gateway: *How to Configure Clientless VPN to Sharepoint Access (http://support.citrix.com/article/CTX119965)*. Abgerufen am 20. Oktober 2013: „Clientless mode VPN access to SharePoint provides a secure, feature-rich, and zero client footprint solution to accessing company resources.“ (Seite nicht mehr abrufbar, Suche in Webarchiven (http://timetravel.mementoweb.org/list/2010/http://support.citrix.com/article/CTX119965)) **Info:** Der Link wurde automatisch als defekt markiert. Bitte prüfe den Link gemäß Anleitung und entferne dann diesen Hinweis.
6. Beispiel für Verwendung des Begriffes „VPN“ im Sinne von “Reverse Web-Proxy”: Check Point: *Access Web Portal Check Point Remote Access Solutions (https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk67820#Mobile)*. Abgerufen am 20. Oktober 2013: „The Mobile Access Portal is a clientless SSL VPN solution. […] The Mobile Access Portal supplies access to web-based corporate resources.“
7. Die Wahl der richtigen VPN-Technik (http://www.tecchannel.de/netzwerk/wan/1737650/tipps_zur_wahl_der_richtigen_vpn_technik/index10.html), von Jürgen Hill, Computerwoche, 2. November 2007, archiviert auf tecchannel.de
8. End-to-Site-VPNs (http://www.teco.edu/~zimmer/vpn/node17.html) aus *Virtuelle private Netze – weltweite LANs* von Tobias Zimmer, 1999, teco.edu
9. End-to-End-VPNs (http://www.teco.edu/~zimmer/vpn/node13.html) aus *Virtuelle private Netze – weltweite LANs* von Tobias Zimmer, 1999, teco.edu
10. Site-to-Site-VPNs (http://www.teco.edu/~zimmer/vpn/node14.html) aus *Virtuelle private Netze – weltweite LANs* von Tobias Zimmer, 1999, teco.edu

11. Sichere Datenübertragung trotz Internet – Virtuelle Private Netzwerke (http://www.tomshardware.com/de/Remote-Access-VPN-Vista,testberichte-239975-2.html) von Marcel Binder, März 2008, auf tomshardware.de
12. *VPN: virtual private network: Virtuelles privates Netzwerk.* (http://www.itwissen.info/definition/lexikon/virtual-private-network-VPN-Virtuelles-privates-Netzwerk.html) In: *itwissen.info.* 8. April 2012, abgerufen am 9. Februar 2015.
13. *Mobile VPN.* (http://msdn.microsoft.com/en-us/library/cc440255.aspx) In: *msdn.microsoft.com.* Abgerufen am 9. Februar 2015 (englisch).
14. 3GSM: SafeNet mit neuem VPN-Client für mobile Geräte (https://web.archive.org/web/20100211135454/http://www.voip-info.de/news/newsartikel__3085.php) (Memento vom 11. Februar 2010 im *Internet Archive*) In: *voip-info.de*
15. Götz Güttich: *Test NetMotion Wireless Mobility XE 8.5 : VPN ohne Stottern.* (http://www.tomsnetworking.de/content/tests/j2009a/test_netmotion_wireless_mobility_xe_8_5/index.html) In: *tomsnetworking.de.* 26. Juni 2009, abgerufen am 9. Februar 2015.
16. Sudhanshu Chauhan, Nutan Kumar Panda: *Hacking Web Intelligence: Open Source Intelligence and Web Reconnaissance Concepts and Techniques*. Syngress, 2015, ISBN 978-0-12-801912-2, S. 167 (eingeschränkte Vorschau (https://books.google.de/books?id=5u2cBAAAQBAJ&pg=PA167#v=onepage) in der Google-Buchsuche).
17. Mitch Tulloch: *SSTP Makes Secure Remote Access Easier.* (http://biztechmagazine.com/article.asp?item_id=377) In: *biztechmagazine.com.* 22. Januar 2008, abgerufen am 9. Februar 2015.
18. *Fixing the Internet Using Secure Vector Routing.* (https://www.128technology.com/blog/fixing-internet-using-secure-vector-routing/) In: *128 Technology.* 8. Juni 2017, abgerufen am 10. Februar 2020 (amerikanisches Englisch).
19. *DNS-Leak vermeiden.* (https://www.spyoff.com/dns-leak-vermeiden/) In: *spyoff.com.* Abgerufen am 4. Februar 2016.
20. m whites: *Complete guide to the advantages and disadvantages of VPNs.* (https://medium.com/@mwhites9/complete-guide-to-the-advantages-and-disadvantages-of-vpns-f58f354cb6e5) In: *Medium.* 25. April 2017, abgerufen am 5. Februar 2019.
21. Computerbild-Nachricht vom 3. Februar 2021 (https://www.computerbild.de/artikel/cb-News-Sicherheit-VPN-Mozilla-VPN-Dienst-Deutschlandstart-Termin-25166821.html)
22. *How VPNs Work.* (https://computer.howstuffworks.com/vpn.htm) 14. April 2011, abgerufen am 7. Februar 2019 (englisch).
23. How to install a VPN on your router (https://nordvpn.com/blog/setup-vpn-router/)
24. *VPN.* (https://www.draytek.co.uk/information/our-technology/vpn-overview) Abgerufen am 7. Februar 2019.
25. Daniel Bachfeld: *VPN-Knigge – VPN-Protokolle und Standards (https://www.heise.de/security/artikel/Abloesung-271446.html)*. c't. 13. April 2006. Abgerufen am 7. März 2011.
