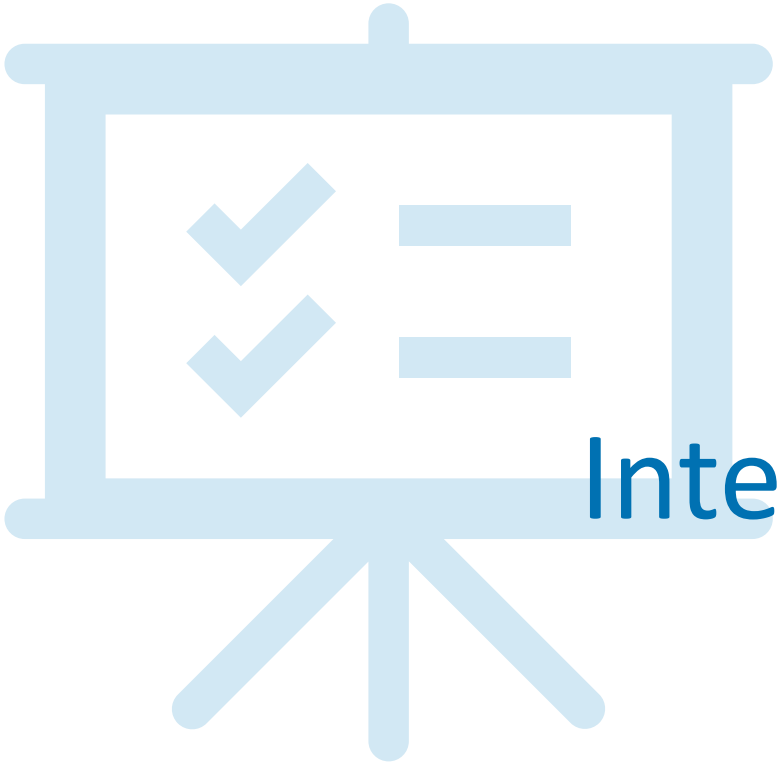

Netzwerke und Internettechnologien 2

VPN
(Virtual Private Network)

Netzwerke und Internettechnologien 2

Lernziele

1

VPN
Grundlagen, Funktion

2

VPN
Verbindungsarten

3

RDP
Remotedesktop-
gateway

VPN (Virtual Private Network)

Bedeutung

- Als „Virtual Private Network“ wird ein Verfahren bezeichnet, bei dem ein virtuelles Netzwerk innerhalb eines öffentlichen Netzes simuliert wird.
- Dieses Netz ist „privat“, von außen nicht zugänglich, wie z.B. das gut geschützte Intranet einer Firma.
- Über ein VPN kann ein sicherer Datenaustausch gewährleistet werden, zwischen
  - den Standorten eines Unternehmens.
  - den Außendienstlern und dem Unternehmensnetzwerk.
  - den Mitarbeitern im Homeoffice und dem Unternehmensnetzwerk.

VPN (Virtual Private Network)

VPN-Tunnel

- Virtuelle Verbindungen, wie sie ein VPN erzeugt, werden als Tunnelverbindungen, kurz Tunnel, bezeichnet.
- Dabei wird für den Transport ein Protokoll in ein anderes Protokoll eingebettet/eingekapselt.
- Durch die Kapselung wird die ursprüngliche Kommunikation verschleiert.
- Zusätzlich erfolgt eine Verschlüsselung, womit dann die Daten abhör- und manipulationssicher übertragen werden können.
- Für den Aufbau des Tunnels wird an beiden Tunnelenden eine Tunnelsoftware benötigt.

VPN (Virtual Private Network)

VPN-Tunnel

Beispiel 1

- Ein Home-Office-Mitarbeiter ist über seinen lokalen Provider mit dem Internet verbunden.
- Über einen VPN-Client nimmt er mit dem VPN-Gateway seiner Firma Kontakt auf.
- Beide handeln die Bedingungen aus, unter denen der Datenverkehr erfolgen soll.
- Über den Tunnel bekommt der Client eine Adresse aus dem Firmennetzwerk zugewiesen. Damit wird der Client virtuell ein Mitglied des Firmennetzes.

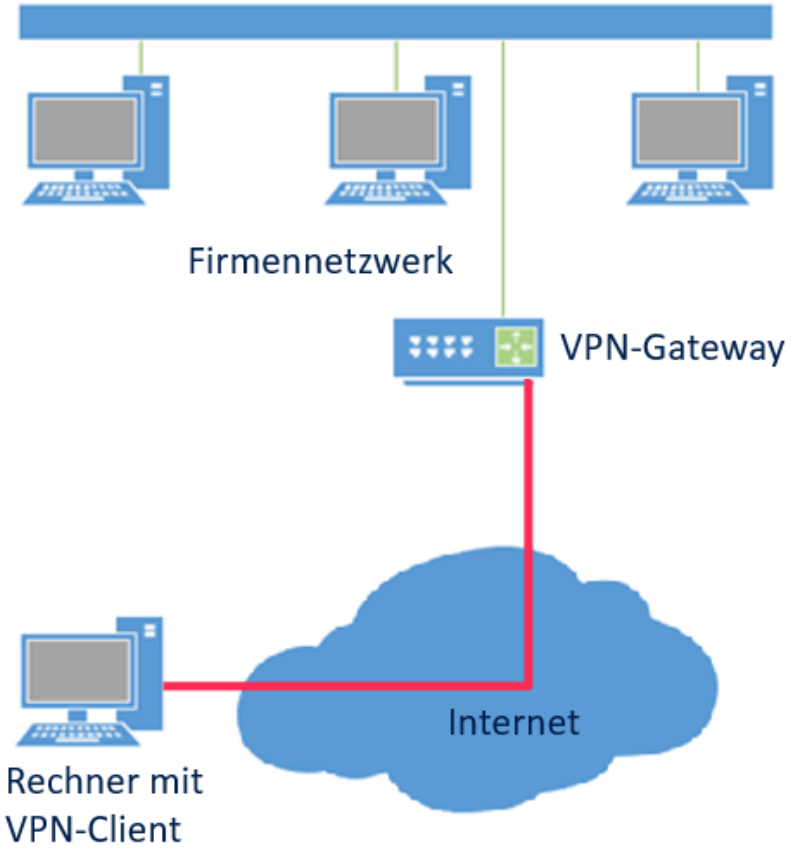

Abbildung 1: VPN-Tunnel (eigene Darstellung)

VPN (Virtual Private Network)

VPN-Tunnel

Beispiel 2

- Werden Standorte miteinander verknüpft, läuft die Kommunikation über zwei VPN-Server, die miteinander kommunizieren und ganze Netzwerke ständig verbinden.
- Entfernte Filialen werden so sicher miteinander verbunden.
- An den Endpunkten des Tunnels wird die Verschlüsselung decodiert, man sagt, der VPN-Tunnel wird terminiert. Im Firmen-netzwerk wird nur der „normale“ unverschlüsselte Verkehr gesehen.

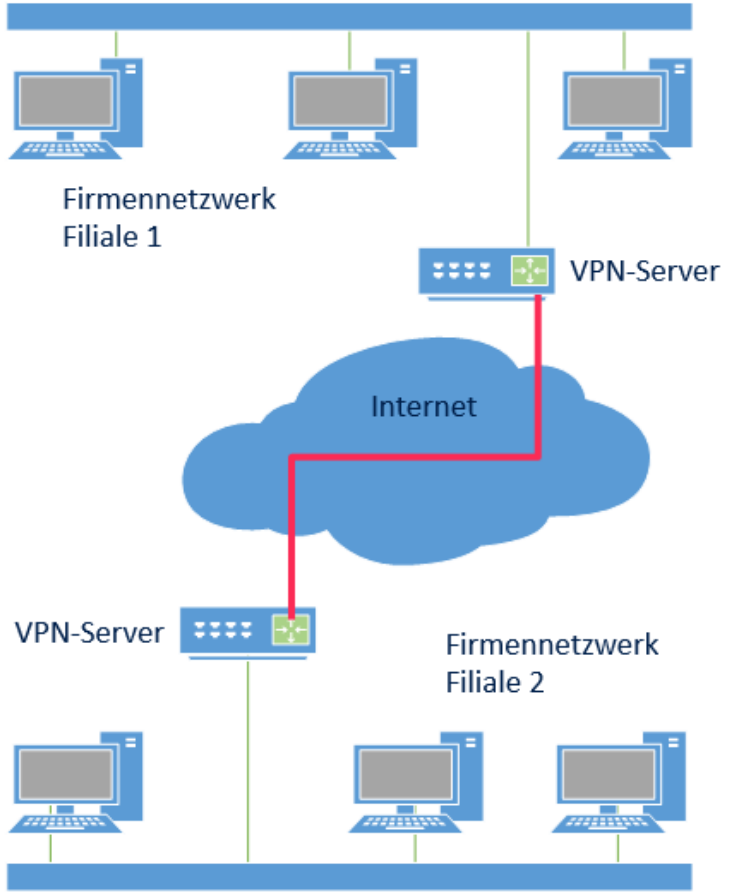

Abbildung 2: VPN-Tunnel (eigene Darstellung)

VPN (Virtual Private Network)

Schema für den VPN-Verbindungsaufbau

- Der Client nimmt über das Internet Verbindung zum VPN-Server auf.
- Der Client muß sich am Server authentifizieren. Dies kann durch verschiedene Verfahren geschehen, zum Beispiel durch Username/Passwort, Zertifikate oder andere Mechanismen.
- Nach erfolgreicher Authentifizierung werden untereinander noch Parameter ausgehandelt, wie die Art der Verschlüsselung, die Gültigkeitsdauer der Schlüssel etc.
- Im Anschluss wird die Tunnelverbindung aufgebaut.
- Durch die Tunnelverbindung sollen die drei Schutzziele Authentizität, Vertraulichkeit und Integrität bei der Datenübertragung sichergestellt werden.

VPN (Virtual Private Network)

Split oder Closed Tunneling

- Bei normalen VPN-Verbindungen, „Closed Tunneling“ wird der gesamte Internetdatenverkehr über den Tunnel geleitet. Für die Dauer der Verbindung besteht kein Zugriff auf auswärtige und lokale Webdienste sowie lokale Geräte, wie zum Beispiel Netzwerkdrucker.
- Bei Closed-Tunneling ist, sobald der Tunnel aufgebaut wird, der Rechner von seinem lokalen Netzwerk und dem Internet völlig isoliert.
- Die meisten VPN-Clients können auch so konfiguriert werden, dass sie lokalen Verkehr trotzdem erlauben. In diesem Fall spricht man von einem „Split Tunneling“.
- Beim „Split Tunneling“ werden nur die Verbindungen durch den Tunnel geleitet, die als Ziel die Geräte am anderen Tunnelende haben.

VPN (Virtual Private Network)

Split oder Closed Tunneling

- „Split Tunneling“ stellt ein Sicherheitsrisiko dar.
  - Ein Client, der über VPN verbunden ist, ist virtuell ein Bestandteil des Firmennetzes. Dringt ein Hacker in diesen Rechner ein, hat er vollen Zugriff, nicht nur auf den lokalen Rechner, sondern auf das gesamte Intranet der Firma.
  - Der Rechner ist virtuell direkt im Netz. Sicherheitsmechanismen, die das Firmennetzwerk schützen, greifen nicht mehr.
  - Der VPN-Kunde ist virtuell ein Mitglied des Firmennetzwerkes, er taucht also hinter der Firewall auf! Mit „Open/Split Tunnel“ öffnet man somit unkontrollierte Wege ins eigene Netzwerk.

VPN (Virtual Private Network)

Firewall

- VPN durch Firewalls
  - In eine VPN-Verbindung Firewalls einzuschalten, ist nicht geeignet, um die Sicherheit zu erhöhen. Die Verbindung ist im Closed Tunnel sowieso nur Punkt zu Punkt zwischen Server und Client beziehungsweise zwischen VPN-Servern möglich.
  - Daher senkt eine Firewall lediglich die Performance.
  - Da der gesamte Inhalt der Pakete verschlüsselt ist, kann auch mit Prüfmechanismen höherer Layer nichts erreicht werden.
  - Sollte VPN trotzdem über Firewalls verlaufen, müssen die Ports offen gehalten werden, durch die kommuniziert wird.

VPN (Virtual Private Network)

Firewall

- Eine bessere Lösung ist, das VPN-Gateway vor die Firewall zu setzen, alle verschlüsselten Datenpakete zu entschlüsselt und erst danach die Prüfung auf ungewollte Verbindungen durchführen.

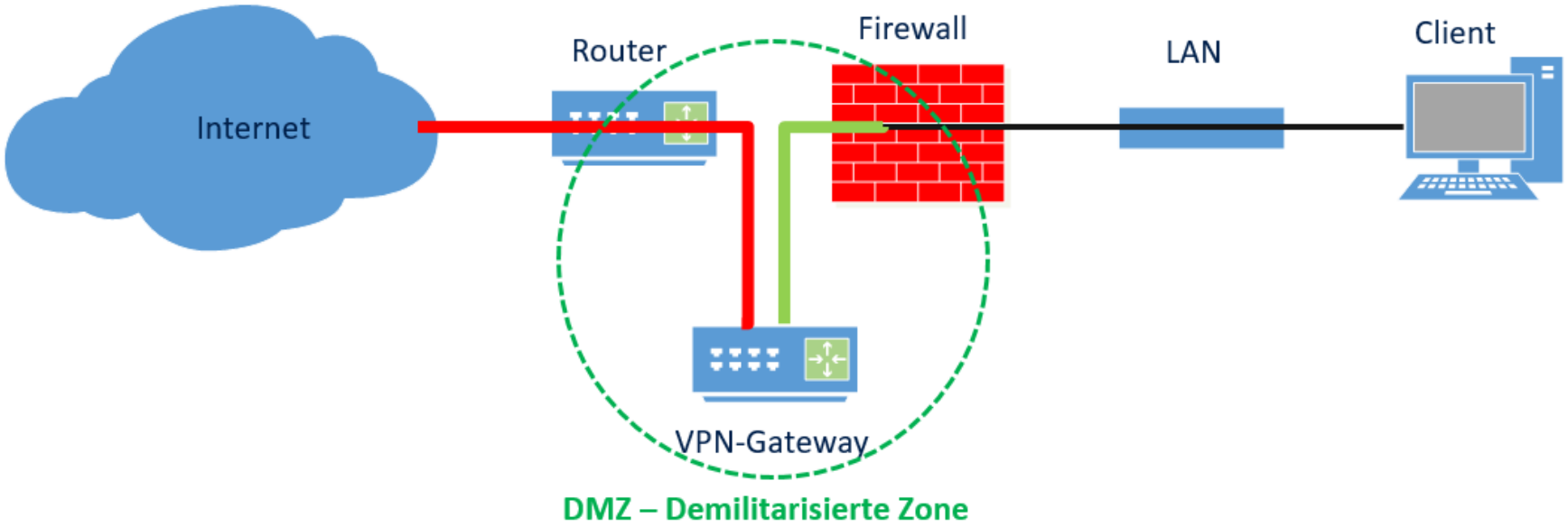

Abbildung 3: VPN und Firewall (eigene Darstellung)

VPN - Verbindungsarten

VPN - Verbindungsarten

End-to-Site-VPN / Remote-Access-VPN

- End-to-Site-VPN beschreibt ein VPN-Szenario, bei dem Heimarbeitsplätze oder mobile Benutzer (Außendienst) in ein Unternehmensnetzwerk eingebunden werden.
- Die VPN-Technik stellt eine logische Verbindung, den VPN-Tunnel, zum entfernten lokalen Netzwerk über ein öffentliches Netzwerk her. Hierbei muss ein VPN-Client auf dem Computer des externen Mitarbeiters installieren sein.
- Der externe Mitarbeiter kann so arbeiten, als ob er sich direkt im Unternehmensnetzwerk befindet.

VPN - Verbindungsarten

End-to-Site-VPN / Remote-Access-VPN

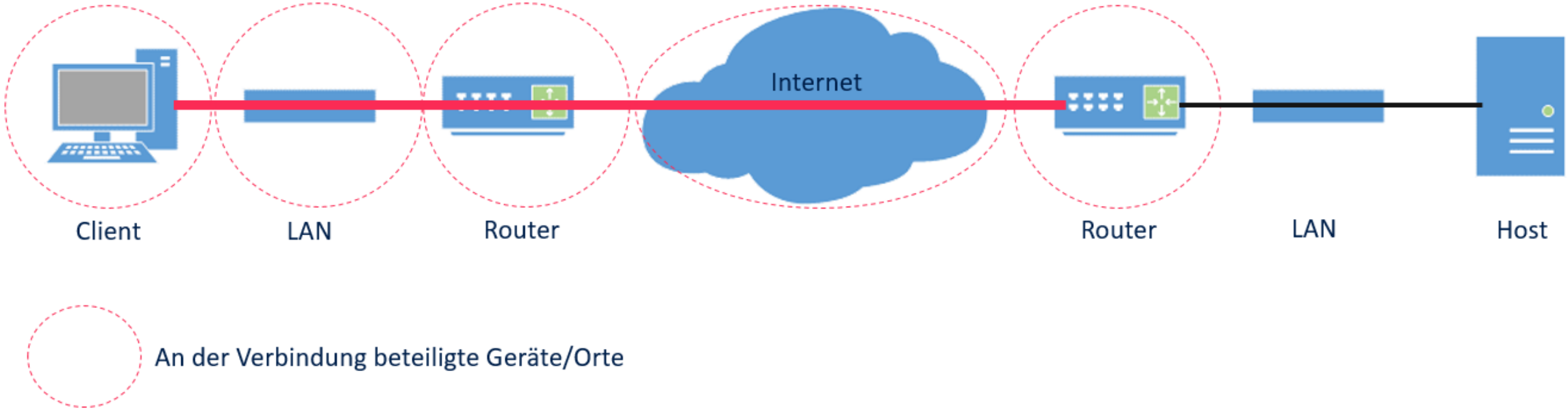

Abbildung 4: End-to-Site (eigene Darstellung)

VPN - Verbindungsarten

Site-to-Site-VPN / LAN-to-LAN-VPN

- Site-to-Site-VPN oder LAN-to-LAN-VPN , sind VPN-Szenarien, um mehrere lokale Netzwerke von Außenstellen oder Niederlassungen zu einem virtuellen Netzwerk über ein öffentliches Netz zusammenzuschalten.
- Virtuelle private Netze werden immer öfter über das Internet aufgebaut. Das Internet wird so zur Konkurrenz zu den klassischen WAN-Diensten der Netzbetreiber.

VPN - Verbindungsarten

Site-to-Site-VPN / LAN-to-LAN-VPN

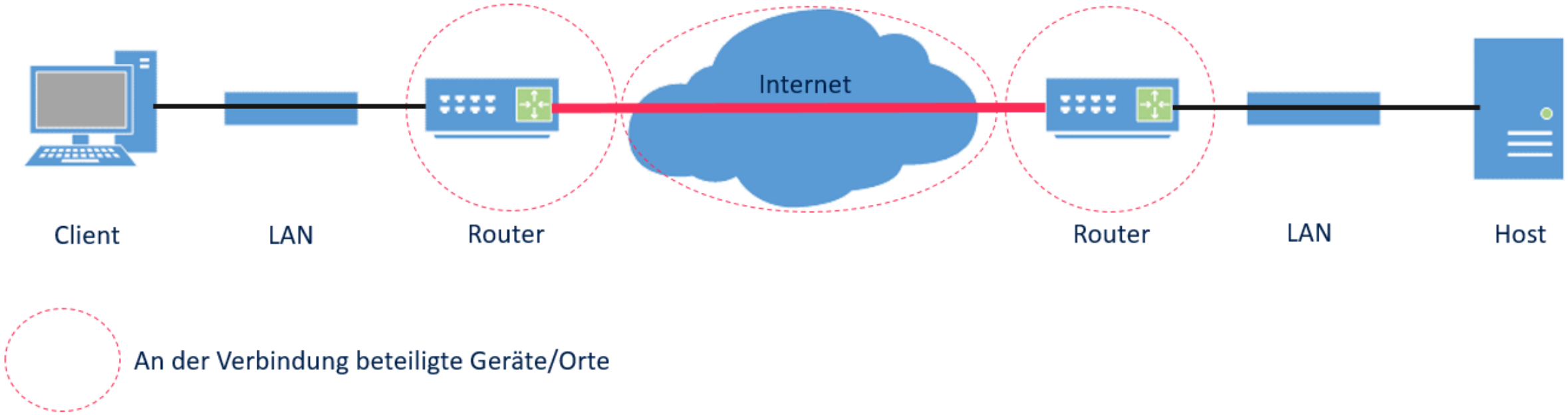

Abbildung 5: Site-to-Site (eigene Darstellung)

VPN - Verbindungsarten

End-to-End-VPN / Host-to-Host-VPN

- End-to-End-VPN beschreibt ein VPN-Szenario, bei dem ein Client auf einen anderen Client in einem entfernten Netzwerk zugreift. Auf beiden Seiten muss eine entsprechende VPN-Software installiert und konfiguriert sein.
- In der der Regel ist der Verbindungsaufbau nur durch die Unterstützung einer zwischengeschalteten Station möglich.
- Das bedeutet, eine direkter Verbindungsaufbau von Host zu Host ist nicht möglich. Stattdessen bauen beide Seiten eine Verbindung zu einem Gateway auf, dass die beiden Verbindungen dann zusammenschaltet.

VPN - Verbindungsarten

End-to-End-VPN / Host-to-Host-VPN

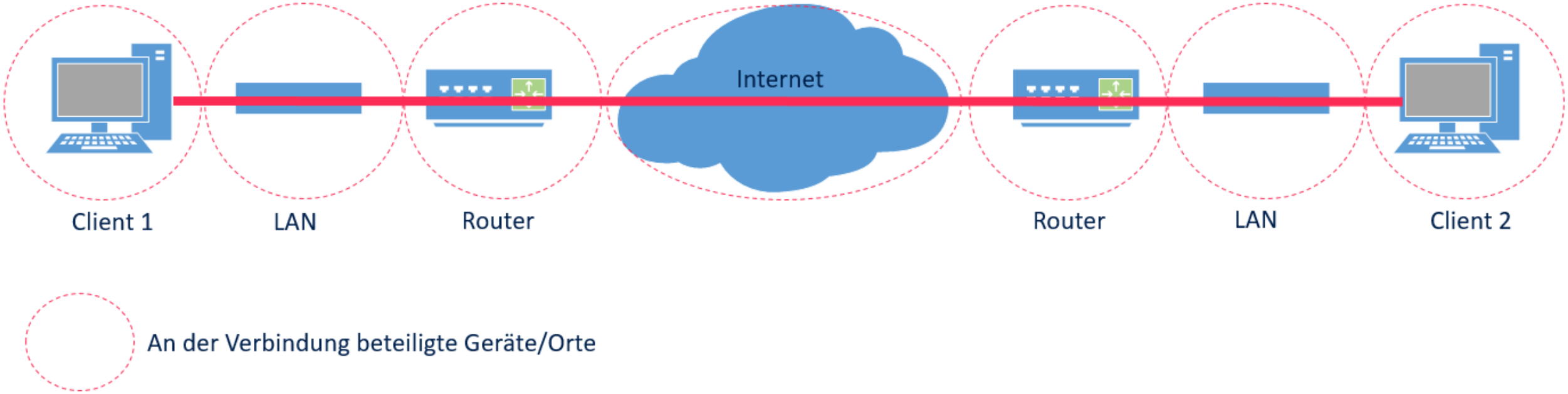

Abbildung 6: End-to-End (eigene Darstellung)

Remote Desktop Gateway

Remote Desktop Gateway

Was ist ein Remote Desktop Gateway?

- Remote Desktop Gateway (RD-Gateway) ist ein Rollendienst auf Windows-Servern, der Remotebenutzern das Herstellen einer Verbindung mit internen Netzwerkressourcen des Unternehmens über das Internet mithilfe einer verschlüsselten Verbindung ermöglicht, ohne dass dabei eine VPN-Verbindung konfiguriert werden muss.
- Netzwerkressourcen können Remotedesktopsitzungs-Server, Remotedesktopsitzungen-Server mit RemoteApp-Programmen oder Computer mit aktiviertem Remotedesktop sein.
- RD-Gateway verwendet das Remotedesktopprotokoll (RDP) über HTTPS zur Herstellung einer sicheren, verschlüsselten Verbindung zwischen Remotebenutzern im Internet und den internen Netzwerkressourcen.

Remote Desktop Gateway

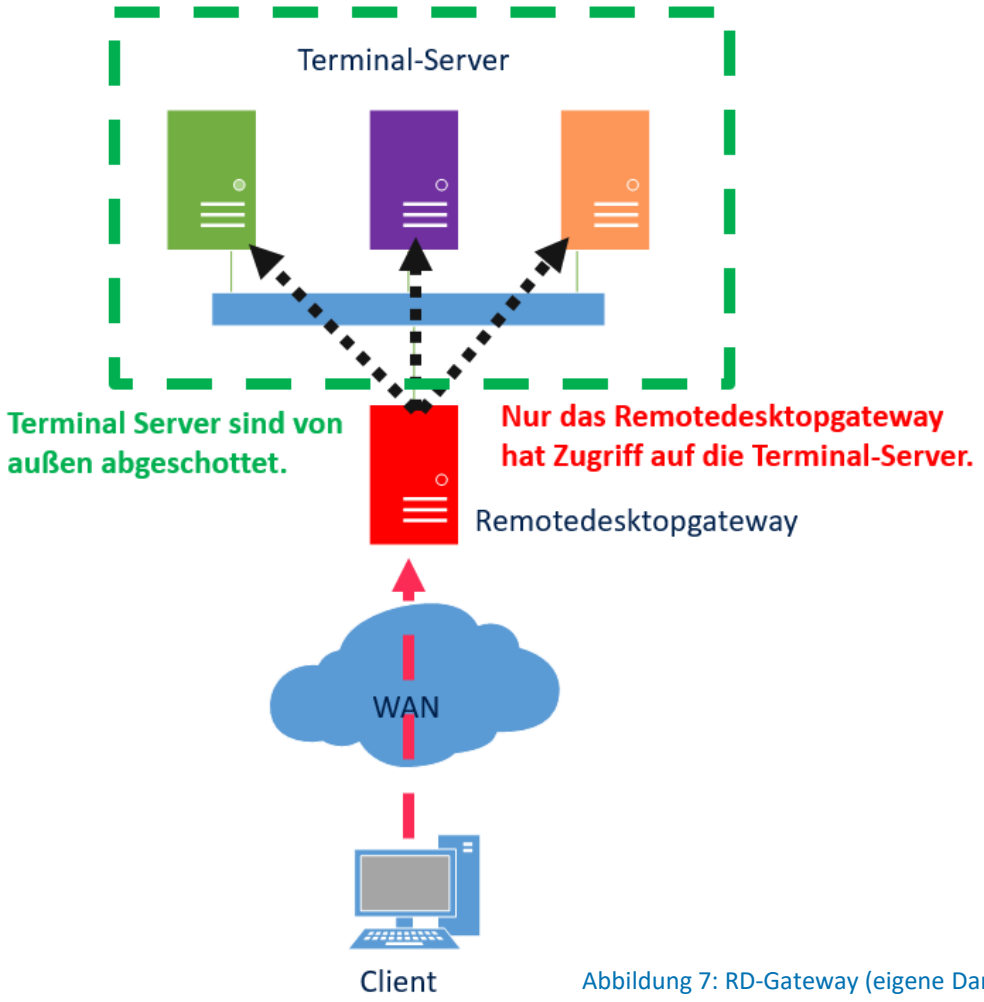

Abbildung 7: RD-Gateway (eigene Darstellung)

Quellen

Buchquelle

Kersken, Sascha (2017): IT-Handbuch für Fachinformatiker. Der Ausbildungsbegleiter. 8. Auflage, revidierte Ausgabe. Bonn: Rheinwerk Verlag; Rheinwerk Computing.

Schreiner, Rüdiger (2014): Computernetzwerke. Von den Grundlagen zur Funktion und Anwendung. 5., erw. Aufl. München: Hanser.

Was ist ein VPN (Virtual Private Network)? (2016). In: *1&1 IONOS SE*, 13.05.2016. Online verfügbar unter https://www.ionos.de/digitalguide/server/knowhow/was-ist-ein-vpn-virtual-private-network/, zuletzt geprüft am 18.05.2021.

Schnabel, Patrick (2013): Netzwerktechnik-Fibel. Grundlagen Netzwerktechnik ; Übertragungstechnik ; TCP/IP ; Anwendungen und Dienste ; Netzwerk-Sicherheit. 3. Aufl. Ludwigsburg.

Schreiner, Rüdiger (2014): Computernetzwerke. Von den Grundlagen zur Funktion und Anwendung. 5., erw. Aufl. München: Hanser.

VIELEN DANK!