Virtual **P**rivate **N**etwork

Unter einem Virtual Private Network (VPN) versteht man eine durch geeignete Verschlüsselungs- und Authentifizierungs-mechanismen geschützte Verbindung zwischen 2 Rechnern (VPN-Client und VPN-Gateway) durch das Internet hindurch.

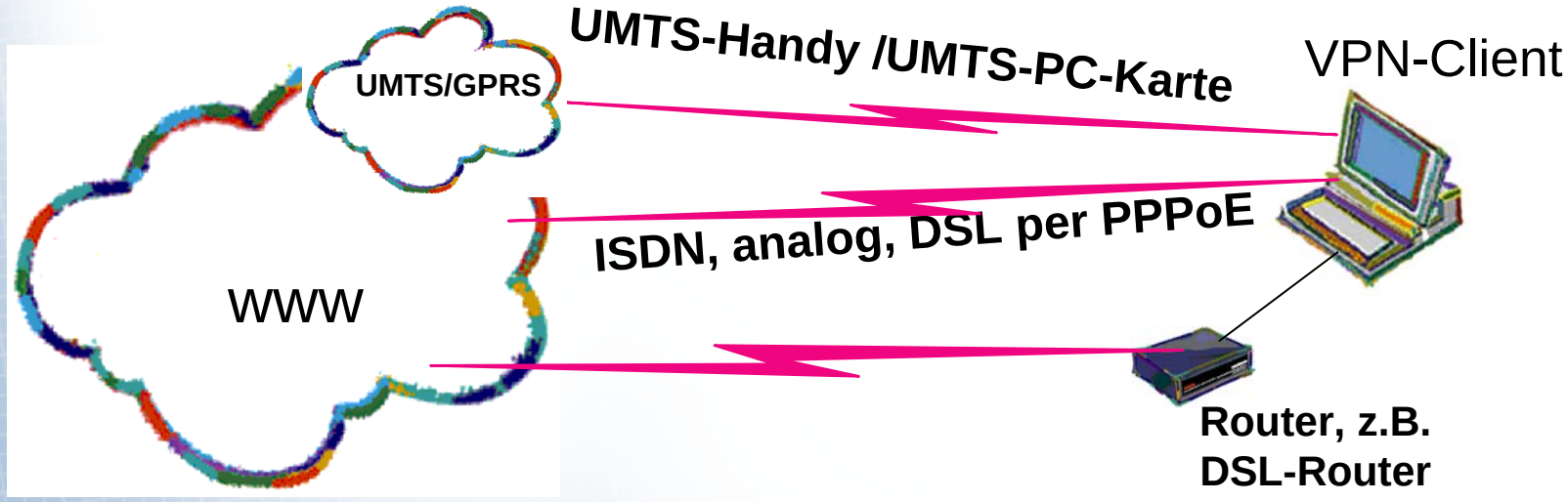
Man spricht auch von einem VPN-Tunnel

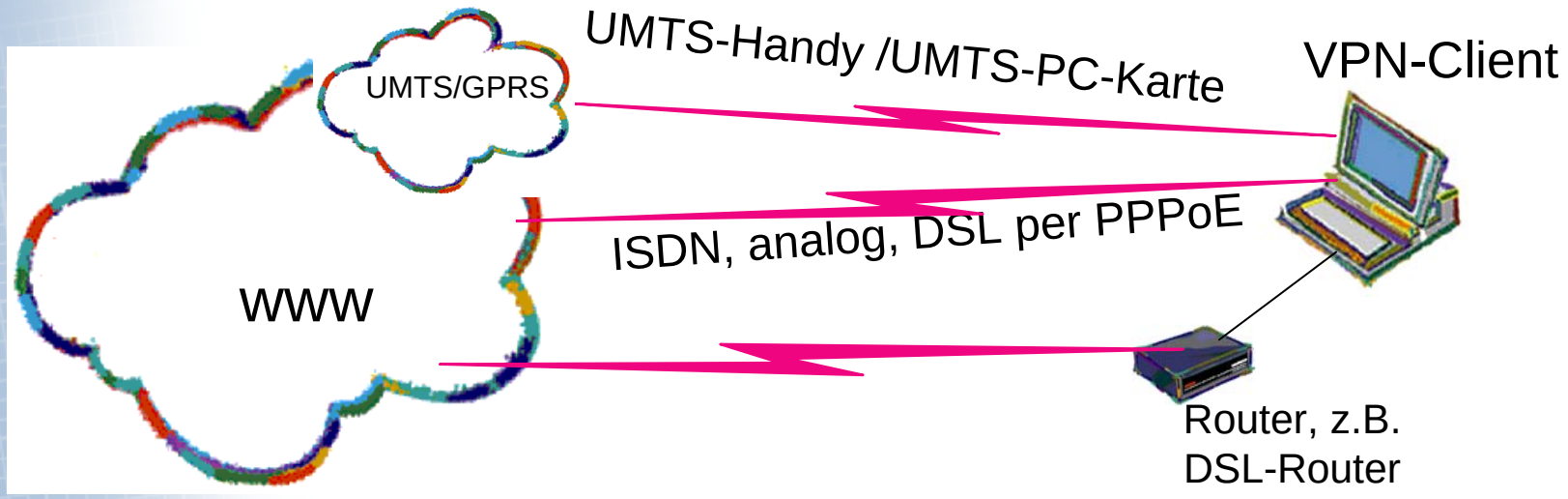
Aufbau des VPN-Tunnels

Der Aufbau eines VPN-Tunnels vollzieht sich aus Sicht des VPN-Clients immer in 2 Schritten:

1. Schritt: Verbindung mit dem Internet herstellen

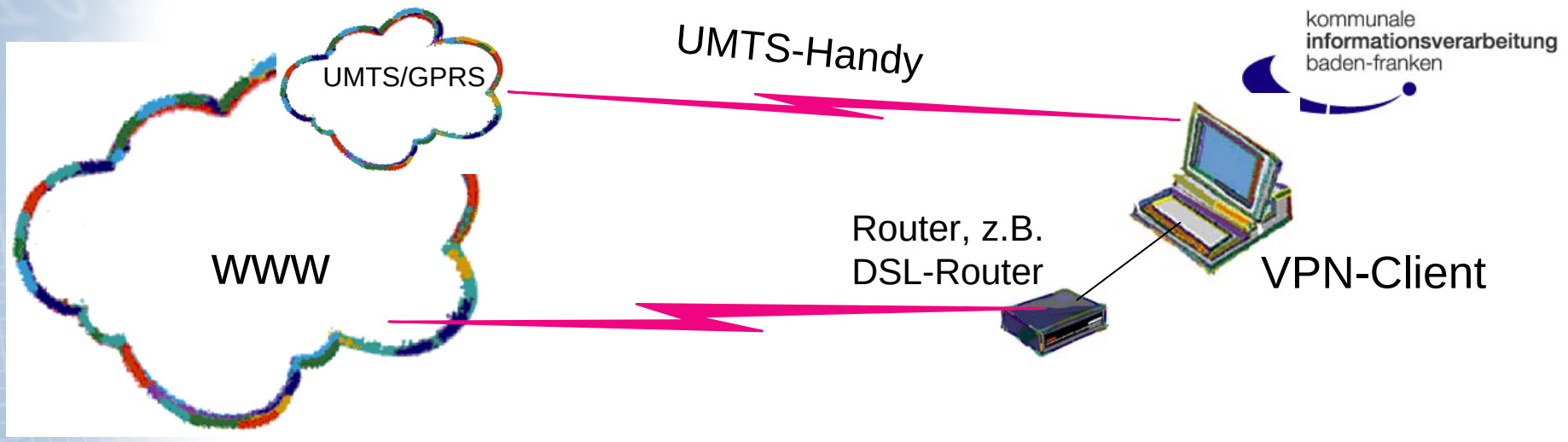
Zunächst muss eine Verbindung mit dem Internet hergestellt werden (z.B. Einwahl per ISDN, analog, UMTS/GPRS) oder es ist schon eine Internet-verbindung vorhanden (Z.B. vorhandene DSL-Router-Verbindung)





Wenn möglich, erfolgt die Einwahl ins Internet durch die VPN-Client-Software:

Wird die Verbindung angefordert, schaltet sich automatisch die VPN-Firewall ein:



Bei Internet-Verbindungen über einen DSL-Router oder über UMTS-Handy-Software erfolgt die Internet-Einwahl nicht über die VPN-Client-Software. Deshalb ist bei dieser Zielwahl (_Internet-GW (z.B. PC am DSL-Router) die VPN-Firewall auch ohne Tunnelverbindung aktiv:

Bei eingeschalteter VPN-Firewall sind Sie auch vor Ihrem eigenen LAN geschützt! Beispiel: W-Lan im Hotel

Sollte es notwendig sein, dass Server in Ihrem LAN, z.B. Softwareverteilungs-server, auf Ihren Client-PC zugreifen müssen, können Sie die Firewall ausschalten. Wählen Sie dazu einfach eine andere Zielwahl aus.

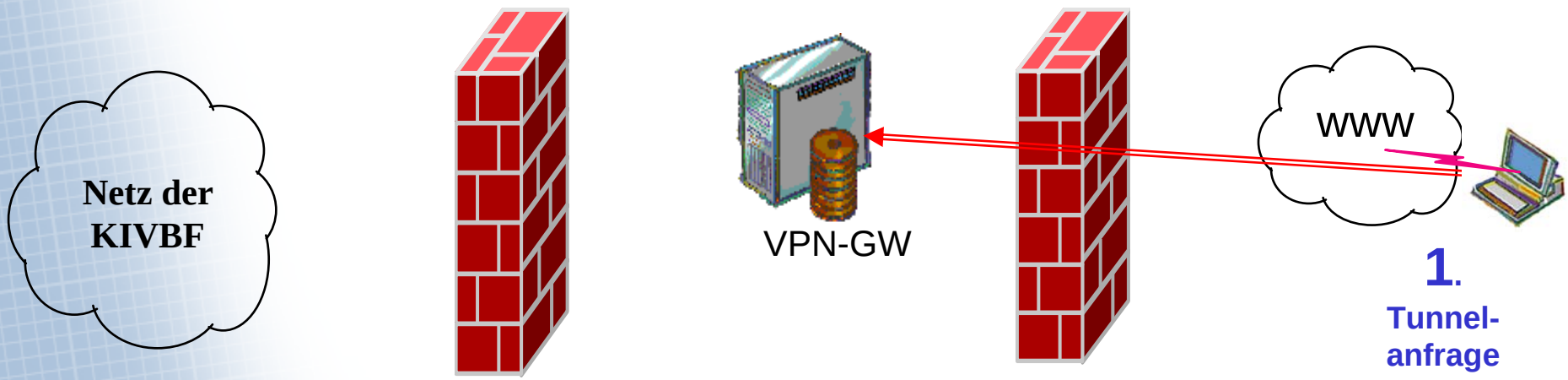
Allerdings hat Ihr PC dann auch nur noch den Schutz, den Sie selbst eingerichtet haben.

Für die Verbindungsart UMTS/GPRS ist zu beachten, dass diese Dienste nicht flächendeckend verfügbar sind. Ob diese Dienste an Ihrem Standort verfügbar sind, können Sie unter folgenden Links feststellen:

http://www.t-mobile.de/funkversorgung/inland
http://eis03sn1.eplus-online.de/evportal/portal/umts?cocoon-portal-event=0
http://www.vodafone.de/hilfe-support/netz-uebertragung-netzabdeckung/108099.html
http://o2umts-fut.arsmedium-ag.de/extra/umts_netzabdeckung_business_neu.asp

Für die Verbindungsarten ISDN, analog und DSL könnten auch KIVBF-eigene Internet-Einwahl-Accounts bereitgestellt werden. Mit diesen kann man sich über den Internet-Einwahl-Backbone der Telekom ins Internet verbinden. Die KIVBF-Accounts werden von der Telekom bereits bei der Einwahl ins Internet dahingehend geschützt, dass sie nur mit KIVBF-eigenen Servern im Internet kommunizieren dürfen.

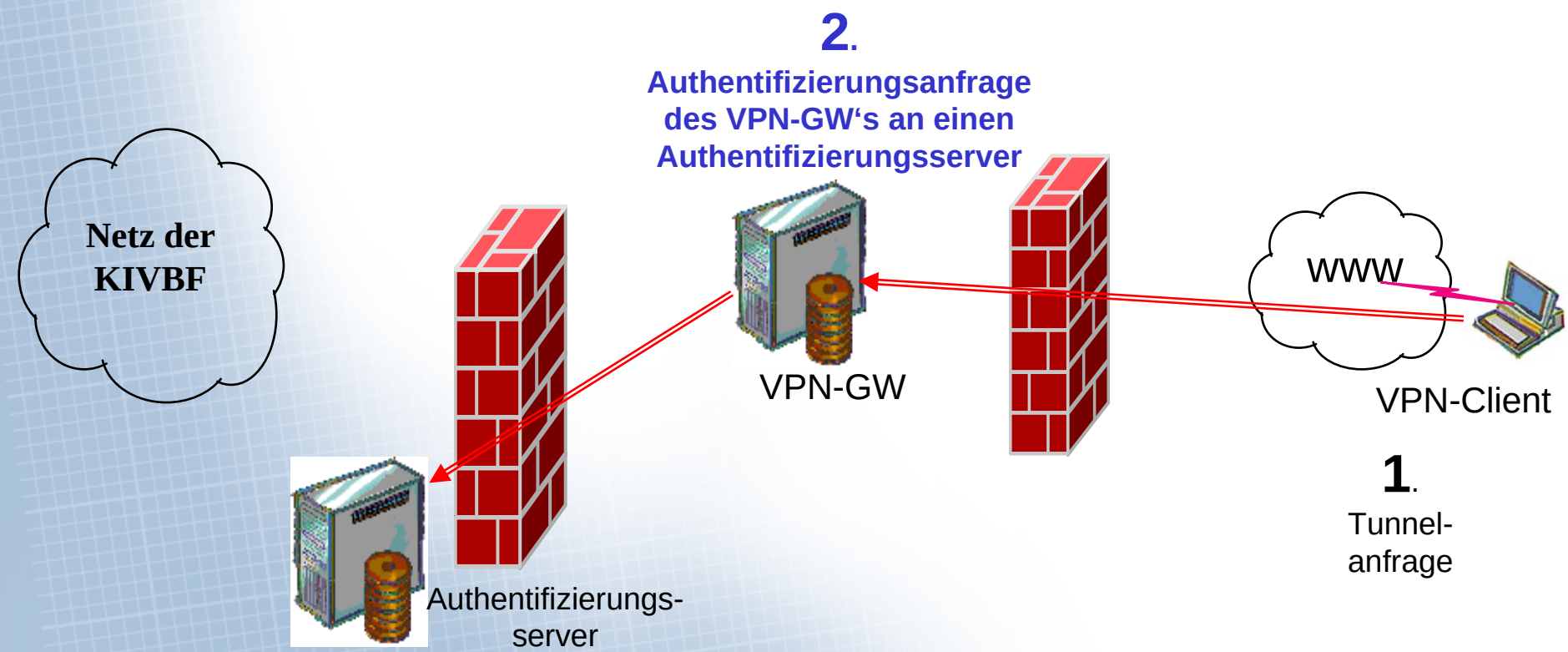
2. Schritt: Ist die Internet-Verbindung verfügbar, kann eine Tunnel-anfrage an das VPN-Gateway gesendet werden



Das VPN-Gateway muss für Tunnelanfragen der VPN-Clients aus dem Internet erreichbar sein. Auf der äußeren Firewall der KIVBF ist deshalb festgelegt, dass Anfragen für VPN-Tunnels an diesen Server durchgelassen werden. Alle anderen Dienstanfragen für diesen Server werden von der Firewall abgewiesen.

Kommt eine Tunnelanfrage beim VPN-GW an, sendet dieses eine Authentifizierungsanfrage an einen Authentifizierungsserver. Auf der inneren Firewall ist festgelegt, dass nur die VPN-GW‘s solche Authentifizierungsanfragen senden dürfen. Alle anderen Dienstanfragen an den Authentifizierungsserver werden abgewiesen. Ebenso alle anderen Dienstanfragen der VPN-GW‘s oder anderer Rechner.

Der Authentifizierungsserver steht alleine in einem eigenen Firewall-Segment.



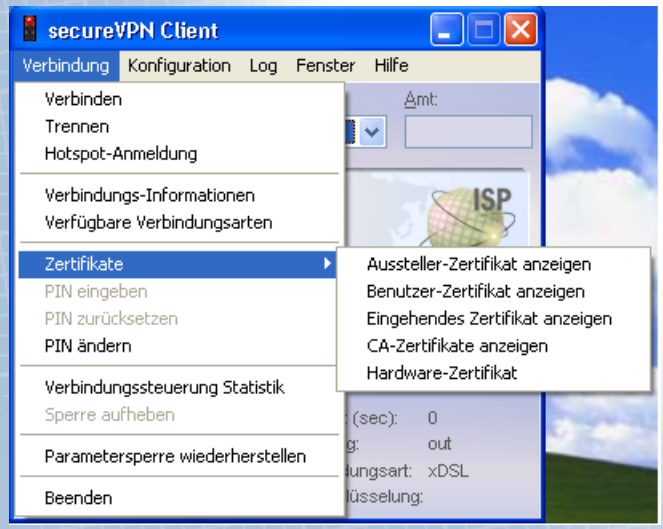
Authentifizierungsbedingungen

Im Zuge der Authentifizierungsanfrage findet eine „starke Authentifizierung“ statt. Diese beruht immer auf 2 Komponenten:

1. **Wissen einer PIN**
2. **Besitz einer Hardware**

Die VPN-Clienten der KIVBF benutzen im Normalfall zur Authentifizierung ein Software-User-Zertifikat, auf das nur zugegriffen werden kann, wenn zuvor die richtige PIN eingegeben wurde.

Die PC-Hardware von der die Tunnelanfrage kommt, wird mit Hilfe eines Hardware-Zertifikates im Hintergrund verifiziert.

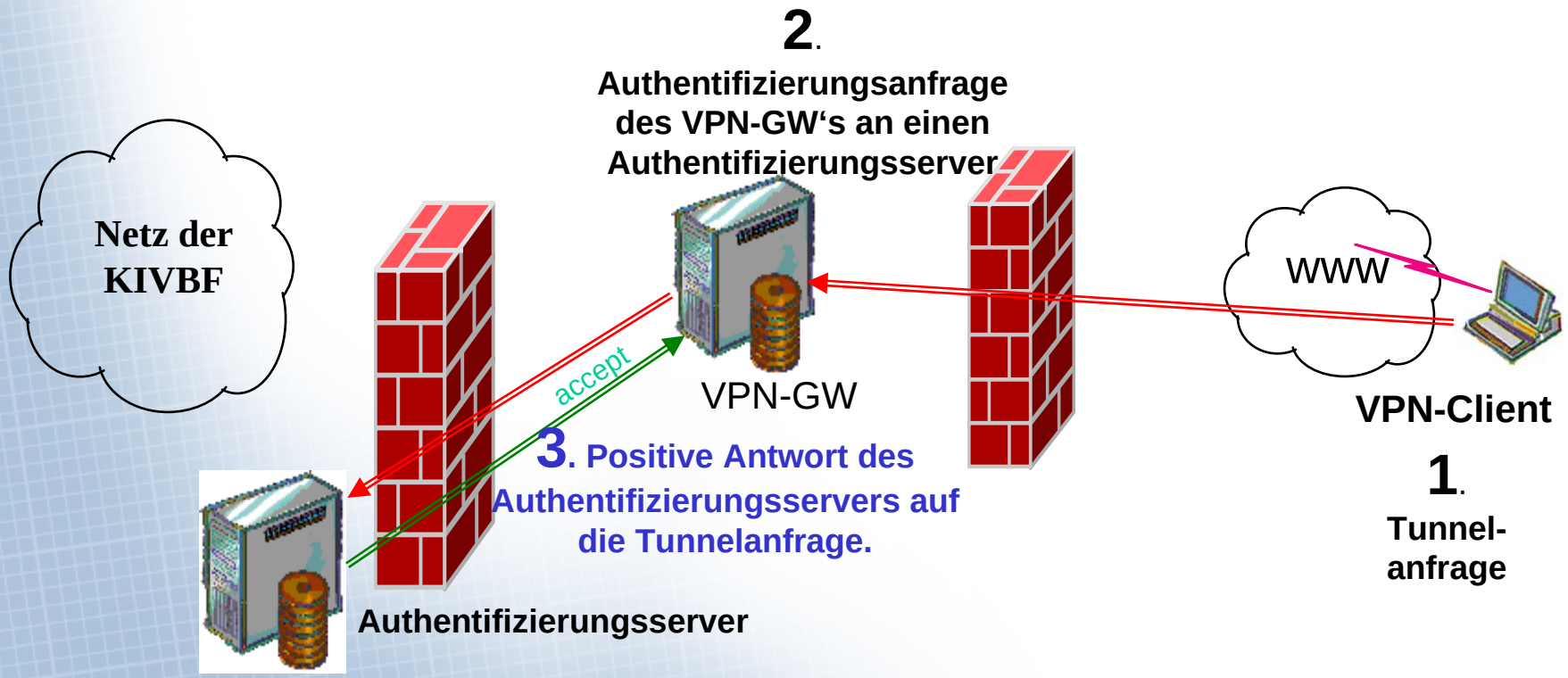


VPN-Clienten, die unter einem **Windows-CE-Betriebssystem (PDA‘s ect.)** arbeiten, unterstützen **keine Hardware-Zertifikate**. Deshalb wird hier wenn möglich die Seriennummer des Gerätes abgefragt und mit der im Authentifizierungsserver für diesen PC hinterlegten verglichen.

Alternativ könnte bei **CE-Betriebssystemen** die Authentifizierung auch mit Hilfe von **Einmal-Passwort-Chipkarten** gemacht werden. Dies ist aber umständlicher und wird deshalb wenn möglich vermieden.

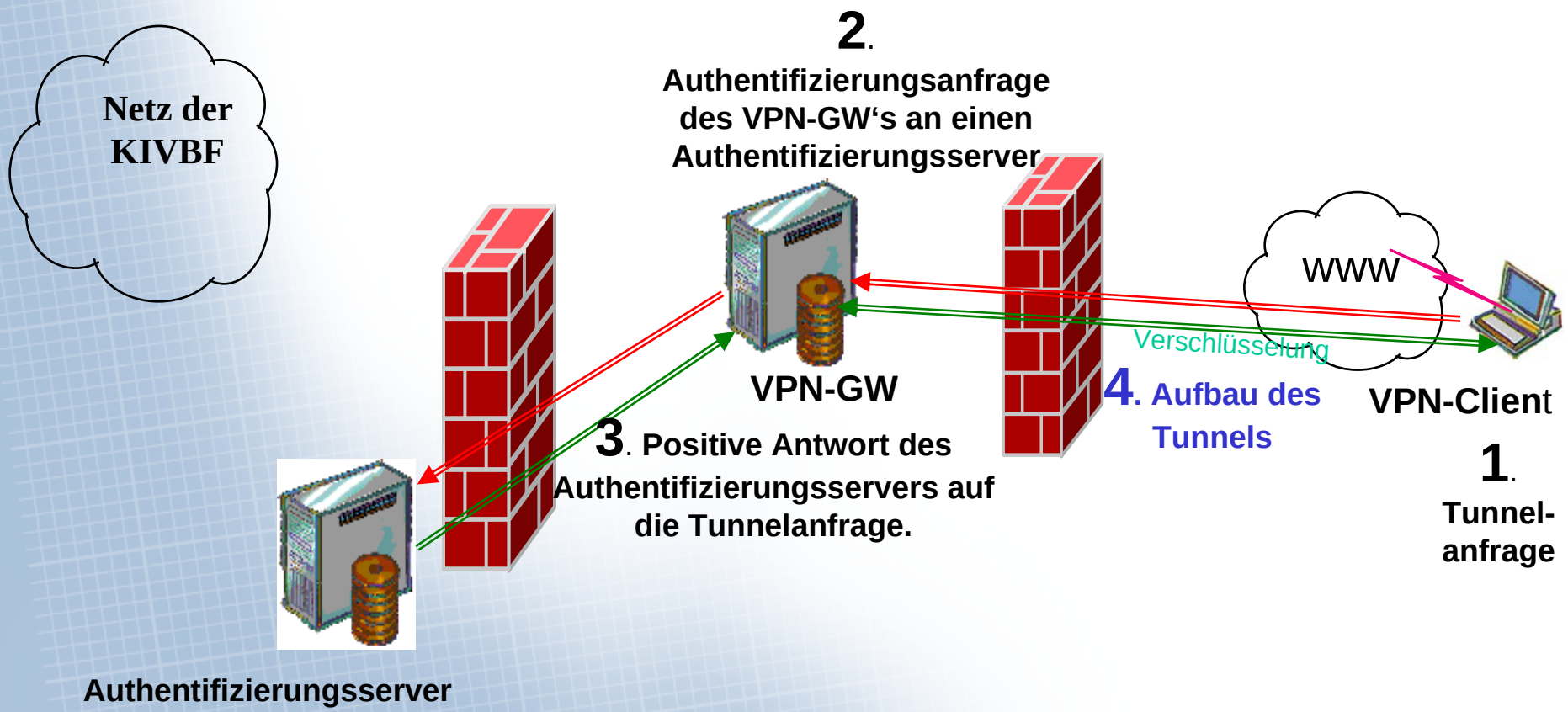
Waren die gesendeten Authentifizierungsdaten gültig, sendet der Authentifizierungsserver ein sogenanntes „accept“, verbunden mit den für diesen Clienten festgelegten Tunnel-Parametern:

- **Feste IP-Adresse des Clienten, mit der er im VPN-Tunnel und im KIVBF-Netz arbeitet.**
- **Verschlüsselungsmethode**
- **Kommpressionsparameter etc.**



Bekommt das VPN-GW das „accept“ des Authentifizierungsservers auf die Tunnelanfrage zurück, baut es den Tunnel zum VPN-Clienten mit den vom Authentifizierungsserver mitgeteilten Tunnelparametern auf.

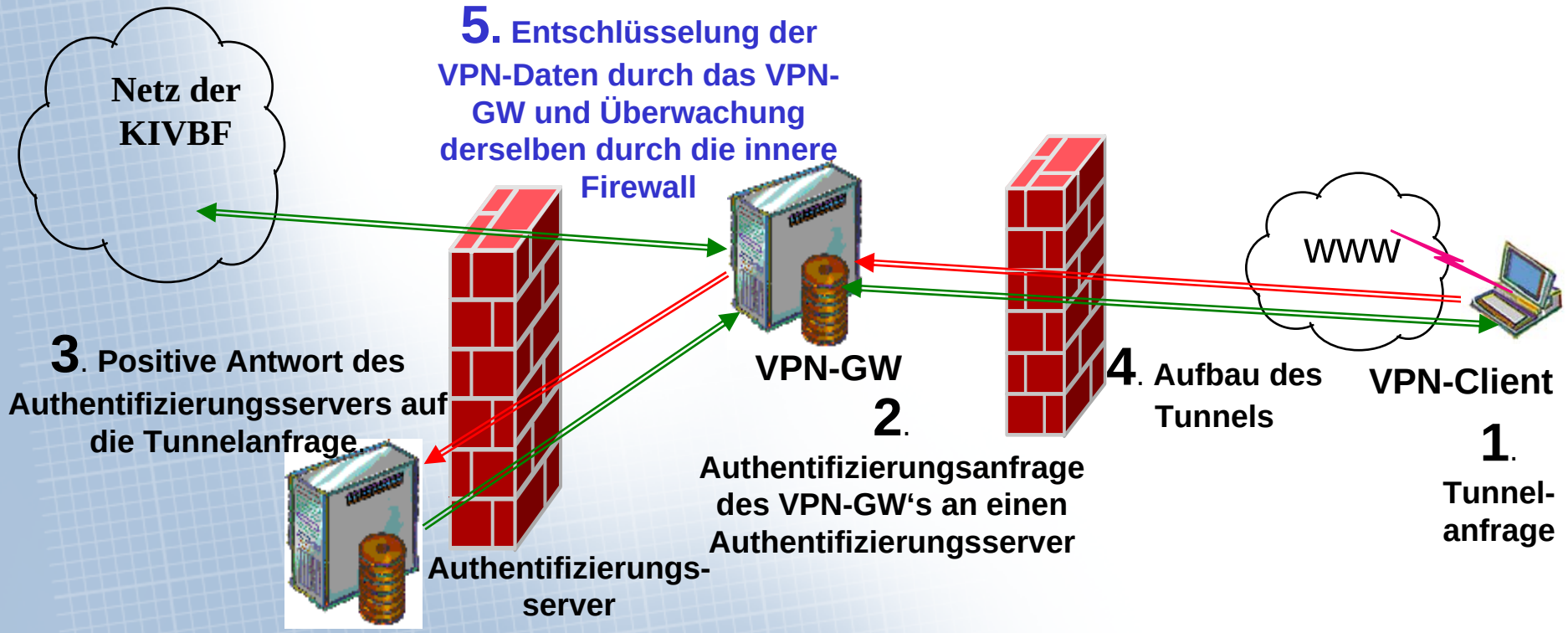
Zwischen den Tunnelendpunkten „VPN-GW“ und „VPN-Client“ wird nun aller Datenverkehr verschlüsselt.



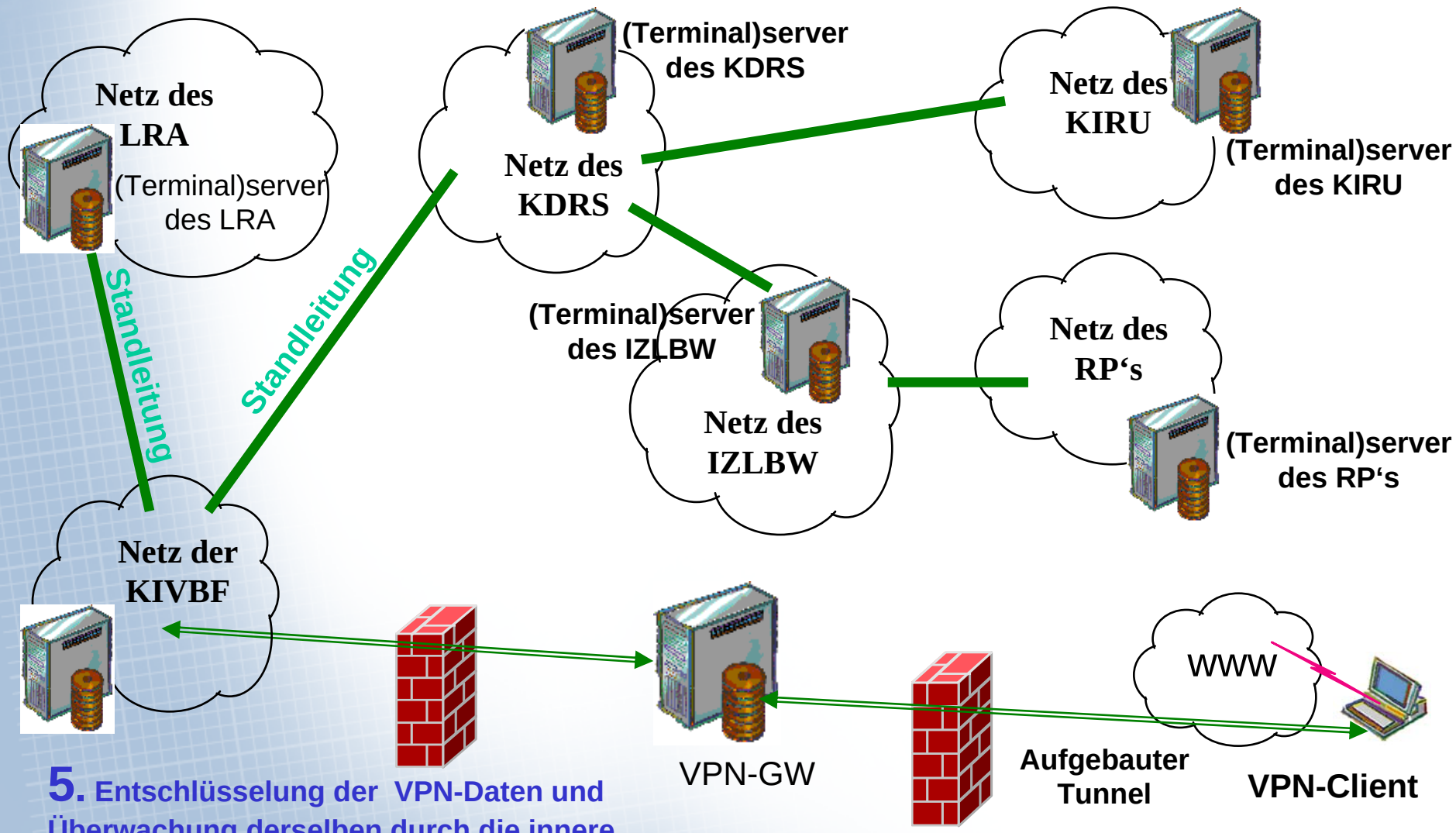
Ankommender VPN-Datenverkehr wird am VPN-GW entschlüsselt und versucht in das Netz der KIVBF weiterzuleiten. Auf der inneren Firewall ist hinterlegt, welcher VPN-Client welche Server mit welchem Dienst kontaktieren darf. Nur Datenpakete, die diesen Freigaben entsprechen werden durchgelassen.

So könnte z.B. hinterlegt sein, dass Ihr VPN-Client nur Ihren Terminalserver mit dem Dienst „Remote Desktop“ kontaktieren darf.

Alle anderen Datenpakete würden von der Firewall verworfen werden.



Ist der VPN-Tunnel aufgebaut, können wir den VPN-Client mit jedem Server verbinden, der aus dem Netz der KIVBF erreichbar ist.



5. Entschlüsselung der VPN-Daten und Überwachung derselben durch die innere Firewall. Z.B nur Terminalserverdienst zu einem bestimmten Terminalserver

Derzeit hat die KIVBF rund 750 VPN-Clienten in der beschriebenen Weise bereits angebunden.

Darunter sind z.B. etliche Forstrevierleiter, die über Ihren VPN-Tunnel Ihre forstlichen Anwendungen beim IZLBW betreiben: entweder durch Direktaufruf der Anwendung beim IZLBW oder über eine entsprechende Terminalserveranwendung, die bei Ihrem zuständigen LRA läuft.

Die KIVBF setzt als VPN-Clienten den „Secure VPN Enterprise Client“ der Fa. NCP in Nürnberg ein.

Der secureVPN-Client der Fa. NCP läuft unter folgenden Betriebssystemen:

- **Windows 2000 / XP / Vista**
- **Windows CE (PDA‘s ect.)**
- **Linux**