

VPN – Der sichere Zugang zum Unternehmen

**Netzwerk
Kommunikationssysteme
GmbH**

Agenda

- Einleitung: VPN allgemein
- VPN-Szenarien
- Funktionsweise von VPN
- Die Protokolle
- VPN in der Praxis
- Fazit

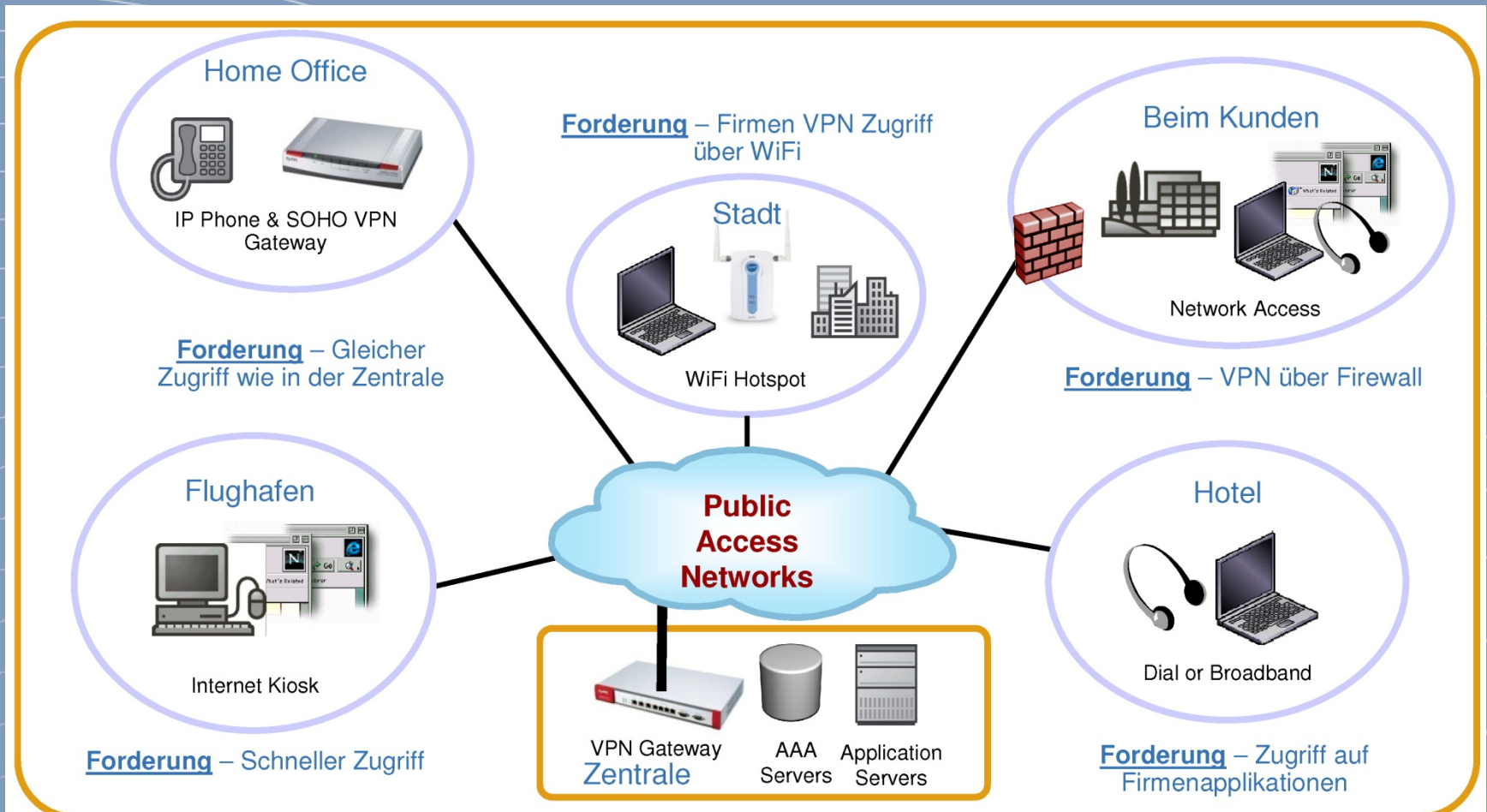
Einleitung: VPN allgemein

Allgemeine VPN Definition

- Ein Virtuelles Privates Netz ist die Nachbildung eines privaten Netzes unter Nutzung einer öffentlichen verteilten Netzinfrastruktur, ...
... wobei auch entsprechende Forderungen an Verfügbarkeit, Leistungsfähigkeit und Sicherheit zu erfüllen sind.

= Sicherer Transport von Daten

Remote Access – Heute



Was ist ein VPN noch...

- Bei aller Technikbegeisterung: Ein VPN (**Virtual Private Network** - dt.: **virtuelles privates Netz**) dient dem...

..... **Geldsparen!**

- Keine Nutzung teurer Modemstrecken oder angemieteter Kanäle
- Einsatz der VPN-Technik: Internet als ein "Trägermedium"

VPN

zur Erfüllung wichtiger Schutzziele im Unternehmen

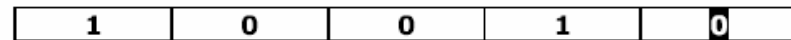
- Authentizität (Echtheit)
- Integrität (Unversehrtheit)
- Vertraulichkeit (Confidentiality)

Schutzziel: Authentizität

- Ziel: Ist der Kommunikationspartner wirklich derjenige, den man annimmt bzw. kommen die Daten vom dem Richtigen ?
- Benutzername-Passwort-Verfahren
- One-Key-Verfahren am Beispiel von Pin und Tan
- Public-Key-Verfahren

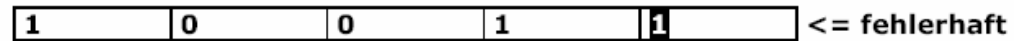
Schutzziel: Datenintegrität

- Ziel: Verhinderung, dass die zu übermittelnden Daten auf ihrem Weg manipuliert werden können



Gerade Parität, dh. Anzahl der „1sen“ ist gerade.

- Prüfsumme



- Hash-Funktion / MD5 (Message Digest Algorithm 5)

| |
|--|
| VPN ist ein Computernetz, das zum Transport privater Daten ein öffentliches Netz nutzt |
| 15530156c421fdb0726ab3fa26a5ecbd |

Eine kleine Änderung der Nachricht erzeugt einen komplett anderen Hash.

| |
|--|
| VPN ist ein Computernetz, das zum Transport privater Daten kein öffentliches Netz nutzt |
| a16294ba5f0fa4153d8c448516478651 |

Schutzziel: Vertraulichkeit

- Vorgehensweise um die Vertraulichkeit zu wahren:
- - Der Sender (Client) verschlüsselt seine Daten bei der Übertragung mit einem Schlüssel (einem public key) und diese verschlüsselten Daten werden dann übertragen.
- - Daraufhin empfängt der Empfänger (Server) die verschlüsselten Daten und benutzt zur Entschlüsselung den entsprechenden, schon zuvor erhaltenden Schlüssel.

Schutzziel: Vertraulichkeit

- **Brute-Force-Verfahren**

- --- Ein einfaches Szenario der Durchführung:
 1. Client(A) verschlüsselt seine Nachricht mit Client(B)'s public Key – ein private key, der die Nachricht als Client(A)'s angibt.
 2. Client(A) sendet nun seine, mit dem public key verschlüsselte Nachricht an Client(B)
 3. Client(B) entschlüsselt nun diese Nachricht mit Client(A)'s public key – ebenfalls ein private key.
 4. Client(B) weiß nun, dass die Nachricht nur von Client(A) stammen kann, da der Sender fest angegeben wird.
 5. Die Nachricht kann nur von Client(B) entschlüsselt werden, da sein public key geheim ist.

- **Datenvertraulichkeit**

- ---- Eines der ältesten Probleme im Netzwerk ist der unautorisierte Zugriff auf unverschlüsselte Dateien, die somit für jedermann im Klartext und somit lesbar und kopierbar vorliegen kann – dies gilt natürlich zu verhindern.

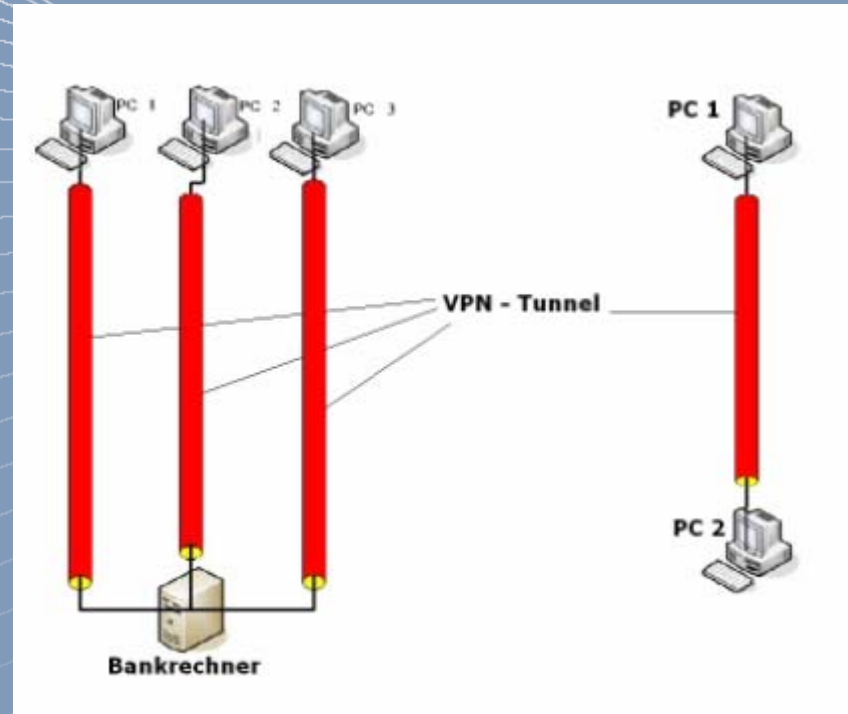
Zur Beachtung

- Kommunikation in öffentlichen Netzwerken ist unsicher.
- Mögliche Angriffe sind:
 - Spoofing
 - Sesion Hijacking
 - Replay-Angriffe
 - Verkehrsanalyse
 - Sniffing
 - Man in the Middle

VPN – Szenarien

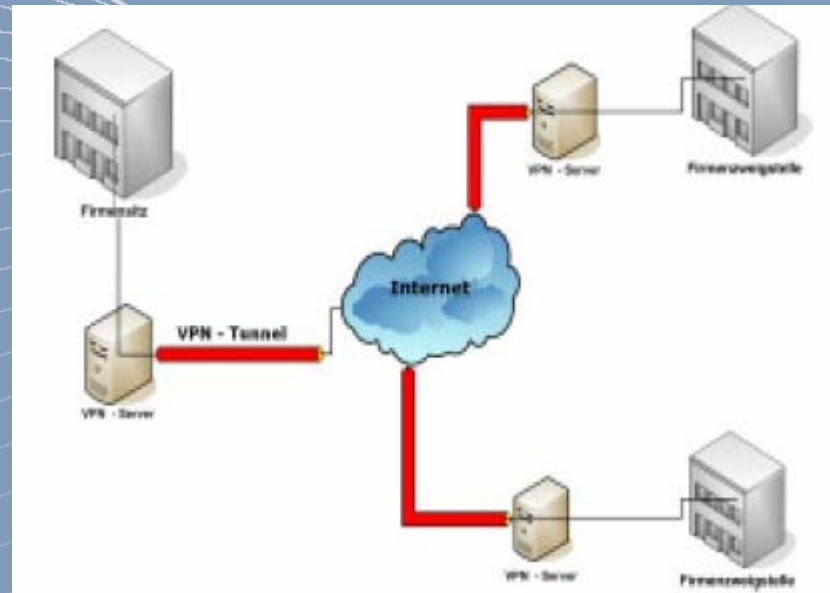
VPN-Szenarien

- End-to-End VPNs



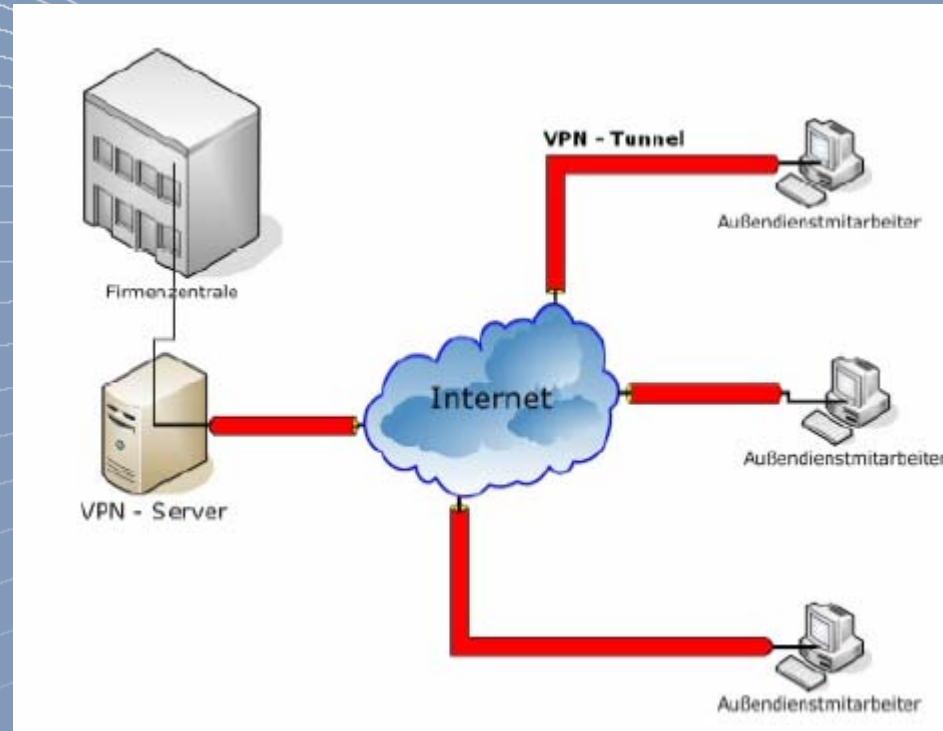
VPN-Szenarien

- Site-to-Site-VPNs



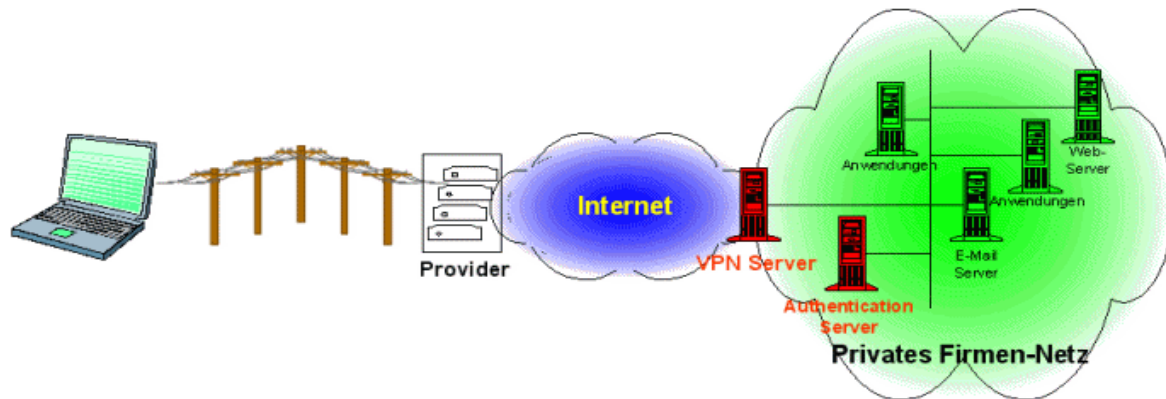
VPN-Szenarien

- End-to-Site-VPNs

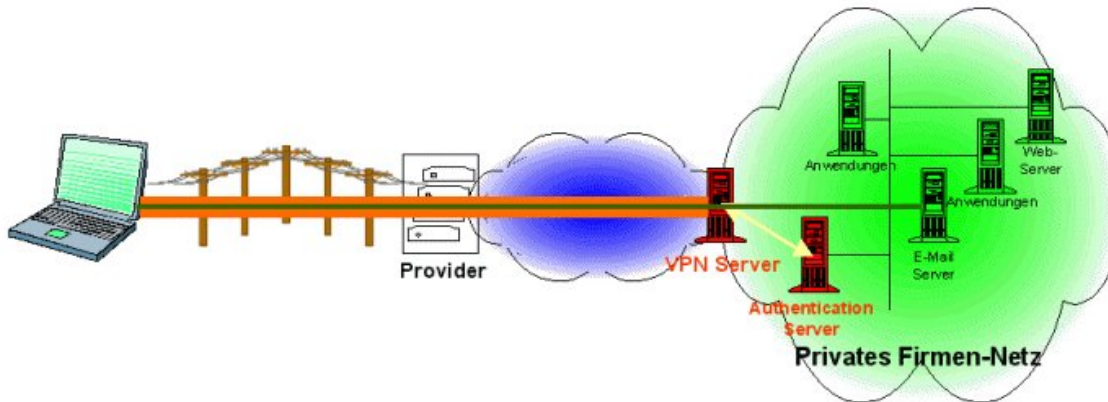


Funtionsweise von VPN

Funktionsweise VPN



Funktionsweise VPN



1. Verbindung zum Internet über beliebigen Provider wird aufgebaut
2. Verbindung zwischen VPN-Client (Notebook) und VPN-Server wird hergestellt
3. Authentisierungsüberprüfung beim VPN-Server
4. Sichere Datenverbindung (IPsec-Tunnel) wird etabliert
5. Eine gesicherte Verbindung zu einem beliebigen Rechner im Firmen-Netz ist möglich



Die Protokolle

VPN-Protokolle

- **PPTP** Point-to-Point Tunneling Protocol
- **L2TP** Layer 2 Tunneling Protocol
- **IPSec** IP-Security
- **L2Sec** Layer 2 Security
- **SSL** Secure Sockets Layer
- **SSH** Secure Shell

Point to Point Tunneling Protocol

PPTP

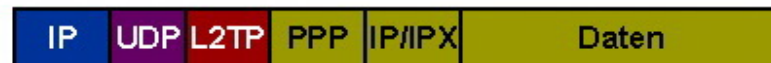
- PPTP (Point to Point Tunneling Protocol) wird von allen Microsoft-Systemen ab Windows 95 unterstützt und gilt deshalb als Industriestandard.
- PPTP nutzt GRE (Generic Route Encapsulation, IP Type 47) für die Daten- und TCP (Port 1723) für die separate Steuersession.
- Optional kann MPPE (Microsoft Point-to-Point Encryption) mit PPTP verwendet werden, d.h. RC4-Verschlüsselung auf PPP-Ebene mit 40 oder 128 Bit.
- Paket-Integritätsprüfung wie z.B. in IPSec ist in PPTP nicht implementiert.
- PPTP wurde in RFC 2637 beschrieben, ist aber bisher nicht standardisiert.



Layer 2 Tunneling Protocol

L2TP

- Im Gegensatz zu L2F und PPTP ist L2TP (Layer 2 Tunneling Protocol) ein standardisiertes Tunneling Protokoll (RFC 2661).
- Es wird gerne als Synthese aus L2F und PPTP bezeichnet. Die Authentisierung basiert auf L2F, während das Format der Control Messages stark an PPTP angelehnt ist.
- L2TP nutzt UDP (Port 1701) als Transportdienst. Steuer- und Datenpakete werden über einen eigenen Message-Header unterschieden.
- L2TP enthält keine Datenverschlüsselung und keine Paketintegritätsprüfung. Das Standardisierungsgremium empfiehlt den Einsatz von L2TP zusammen mit IPsec im Transportmodus.



Ipsec

- IPsec-Protokoll ist ein "Ableger" der IPv6-Arbeitsgruppe
- Standard, der den Aufbau von sicheren IP-Verbindungen (z.B. VPN-Verbindungen) ermöglicht

Ipssec

- IPSec beinhaltet vier wichtige Sicherheitsfunktionen:
 - Verschlüsselung - als Schutz gegen unbefugtes Mitlesen
 - Authentisierung der Nachricht - zum Beweis der Unverfälschtheit einer Nachricht (Paketintegrität)
 - Authentisierung des Absenders - zur unzweifelhaften Zuordnung eines Senders/ Empfängers (Paketauthentizität)
 - Verwaltung von Schlüsseln

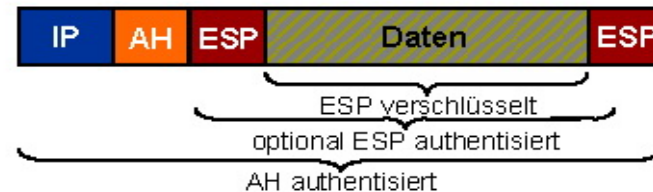
Ipsec Architektur

- Die zentralen Funktionen in der IPsec-Architektur sind:
- das **AH-Protokoll** (Authentication Header),
- das **ESP-Protokoll** (Encapsulating Security Payload)
- und die Schlüsselmanagement (Key Management); **IKE** (Internet Key Exchange)

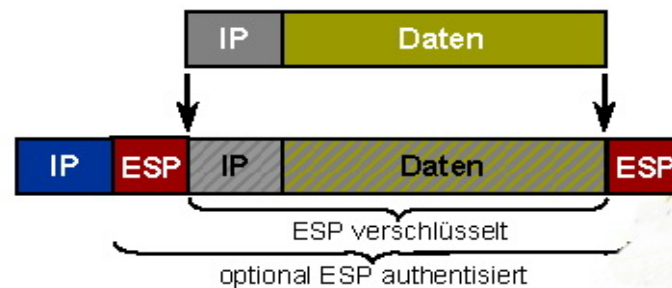
IPSec Funktionsmodell

IPSec Funktionsmodelle

Transport Mode



Tunnel Mode



Vergleich der Protokolle auf Schicht 2 und 3

| Eigenschaft | PPTP | L2TP | IPSec | L2Sec |
|---|-------------|-------------|--------------|--------------|
| Nutzer-Authentifizierung | Ja | Ja | Nein | Ja |
| NAT-Support | Ja | Ja | Nein | Ja |
| Multiprotokollfähigkeit | Ja | Ja | Nein | Ja |
| Dynamische Zuweisung von Tunnel IP-Adressen | Ja | Ja | N/A | Ja |
| Verschlüsselung | begrenzt | Nein | Ja | Ja |
| Authentifizierung von Paketen | Nein | Nein | Ja | Ja |

SSL

(secure sockets layer)

- Im OSI-Modell ist SSL oberhalb der Transportschicht (z.B. TCP) und unter Anwendungsprotokollen wie HTTP oder SMTP angesiedelt.
- SSL arbeitet transparent, so dass es leicht eingesetzt werden kann, um Protokollen ohne eigene Sicherheitsmechanismen abgesicherte Verbindungen zur Verfügung zu stellen.
- Zudem ist es erweiterbar, um Flexibilität und Zukunftssicherheit bei den verwendeten Verschlüsselungstechniken zu gewährleisten.

SSL-Funktionsweise

SSL Funktionsweise

Das SSL-Protokoll besteht aus zwei Schichten (layers): Zu Grunde liegt in der untersten Ebene das SSL Record Protocol, das zur Kapselung verschiedener höherer Protokolle (higher level protocols) dient. Ein Beispiel dafür ist das SSL Handshake Protocol zur Authentifizierung von Client und Server und der Vereinbarung des verwendeten Verschlüsselungsverfahrens, oder das HTTP zur Übertragung von Webseiten.

Der Vorteil des SSL-Protokolls ist die Möglichkeit, jedes höhere Protokoll auf Basis des SSL Protokolls zu implementieren. Damit ist eine Unabhängigkeit von Applikationen und Systemen gewährleistet.

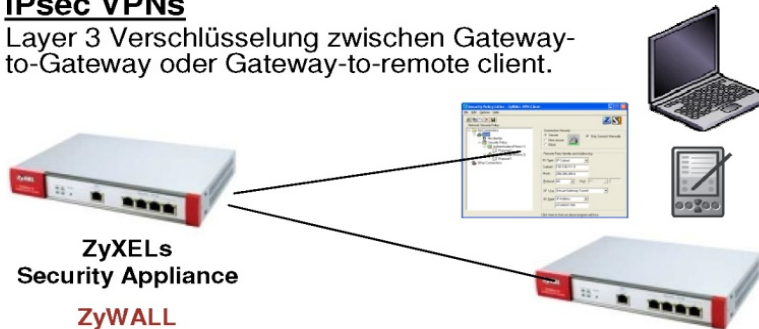
Entscheidung im Tunnel IPSec oder SSL

- IPSec auf Netzwerkebene:
- ---kein Übertragungsverkehr Ende-zu-Ende
- ---Keine Verschlüsselung vom Zugreifer bis zur Zielapplikation
- SSL-VPN (secure-socket-layer)
- --- Tunnel über HTTP hinaus
- --- keine Clientsoftware (Installation, Administration, Konfiguration)
- --- dynamisch JAVA-Applet, Active-X
- --- Applikationen müssen WEB-fähig sein

Sicherer Remote Access: ZyXELs IPsec and SSL VPN technology

IPsec VPNs

Layer 3 Verschlüsselung zwischen Gateway-to-Gateway oder Gateway-to-remote client.



ZyXELs
Security Appliance
ZyWALL

ZyXELs
Security Appliance
ZyWALL SSL

SSL VPNs

Application layer Verschlüsselung zwischen Gateway und Web Browser. Keine spezielle Clientsoftware – auch als "clientless" bekannt



IPsec VPN Client

- Installierter Client beim User
- Jede IP Applikation kann genutzt werden (eg. eMail, client/server, VoIP)
- IPsec VPNs bieten echte network-level remote connection

SSL – Browser-based

- Ermöglicht jedem, mit einem Browser ausgestatteten Gerät, das Netzwerk sicher zu erreichen
- Nutzt einen Java und Active X Client, dieser kann mit einem kompatiblen Browser genutzt werden
- Viele Applikationen (eg. eMail, client/server, web apps)
- Kompromisse gegenüber network-level VPN connection

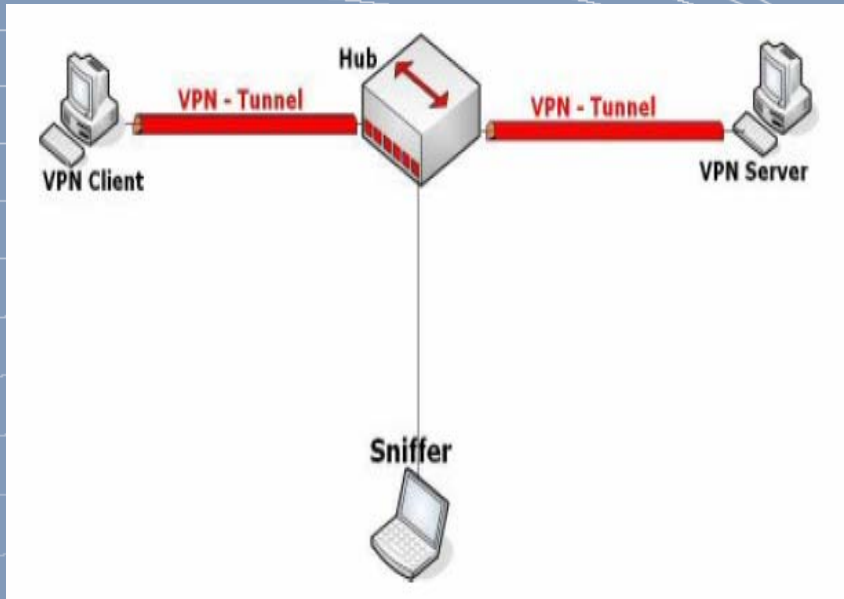
IPSec vs. SSL

IPSec vs. SSL

- **Vorteile von SSL/TLS**
 - Einfache Nutzung
 - Breite Verfügbarkeit in Web-Browsern
(keine spezielle Client-Software erforderlich)
- **Vorteile von IPSec**
 - Hohes Sicherheitsniveau (z.B. bidirektionale Authentisierung, oft stärkere Verschlüsselungsverfahren, unterschiedliche Schlüssel für Verschlüsselung und Integritätsprüfung)
 - Anwendungsunabhängigkeit
 - Endgeräte-unabhängiger Einsatz (z.B. Vermieten von Netzkapazität, Outsourcing von Geräte- und Netzmanagement)
- **Probleme, die beiden Lösungen gemeinsam sind**
 - Verzögerungen durch Verschlüsselung (heute kein Thema mehr)
 - Oft noch fehlender QoS-Support im Providernetz

VPN in der Praxis

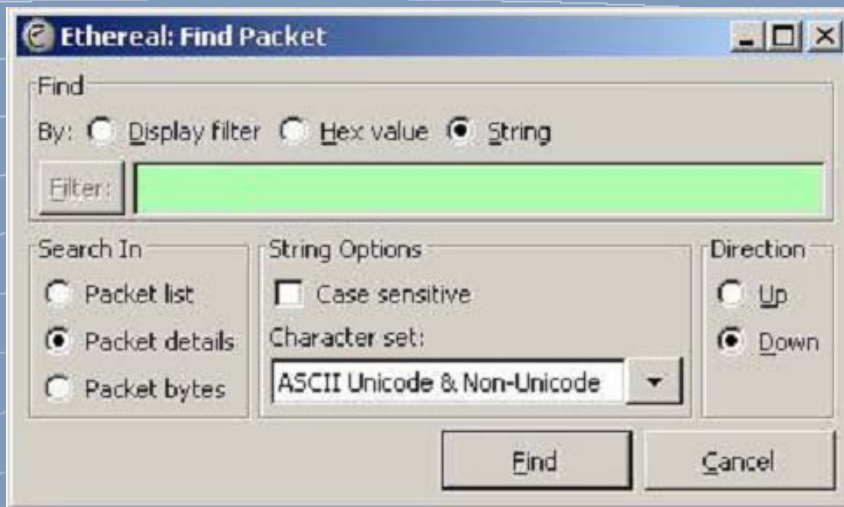
Beispiel Lösungsansätze



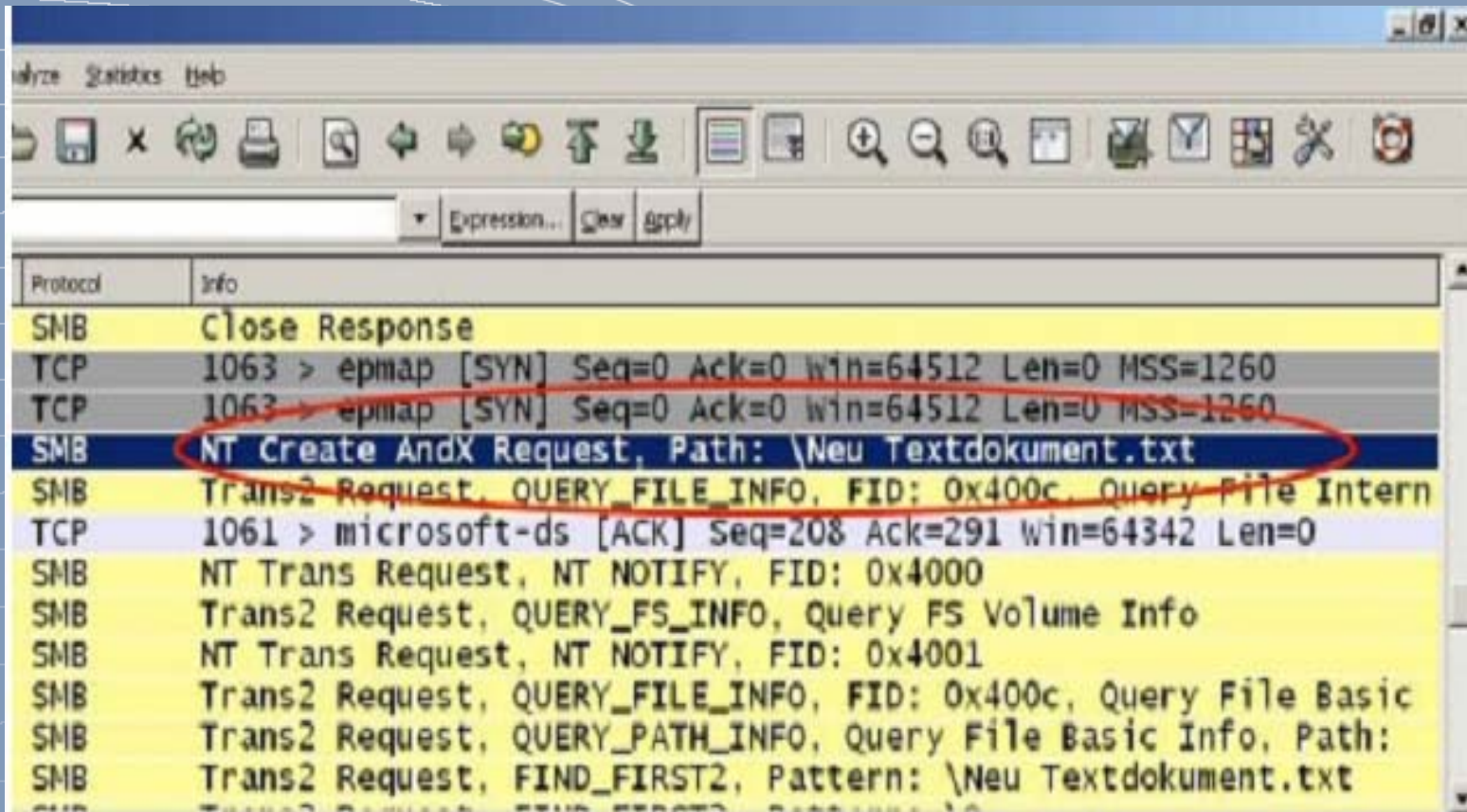
- VPN-Client + VPN Server
- Über den HUB „mitschniffen“ Protokollanalysator Ethereal
- Information im Tunnel lesbar?

1. Test ohne VPN

- Ethereal Suchfunktion nach den Befehlen für die Dateiverwaltung suchen: Create, Rename, Write



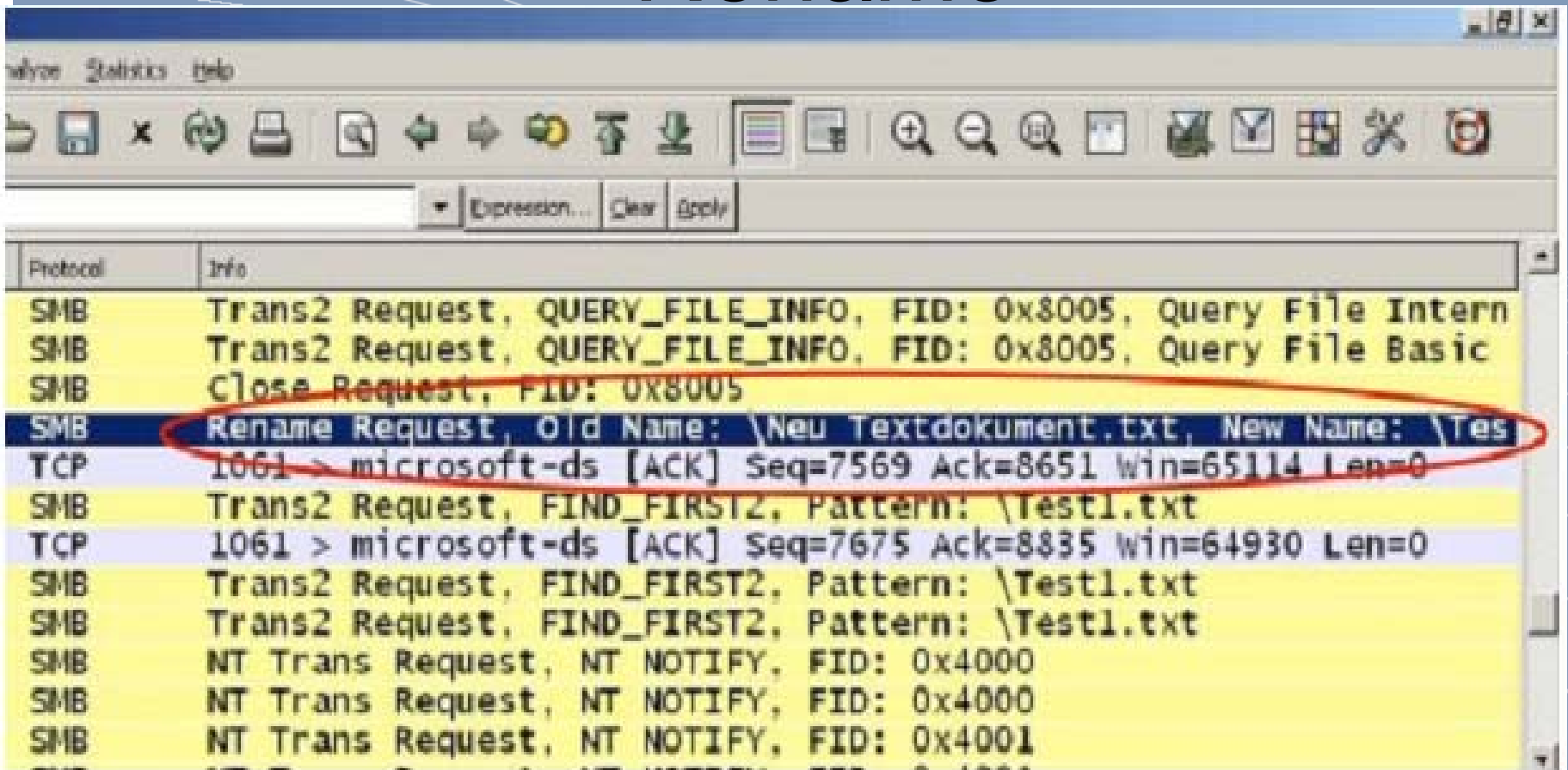
1. Test ohne VPN Create



The screenshot shows a network traffic analysis window with a menu bar (Analyse, Statistics, Help) and a toolbar. Below the toolbar is a search bar with 'Expression...' and 'Clear' buttons. The main area is a table with two columns: 'Protocol' and 'Info'. The table contains the following entries:

| Protocol | Info |
|----------|---|
| SMB | Close Response |
| TCP | 1063 > epmap [SYN] Seq=0 Ack=0 Win=64512 Len=0 MSS=1260 |
| TCP | 1063 > epmap [SYN] Seq=0 Ack=0 Win=64512 Len=0 MSS=1260 |
| SMB | NT Create AndX Request, Path: \Neu Textdokument.txt |
| SMB | Trans2 Request, QUERY_FILE_INFO, FID: 0x400c, Query File Intern |
| TCP | 1061 > microsoft-ds [ACK] Seq=208 Ack=291 Win=64342 Len=0 |
| SMB | NT Trans Request, NT NOTIFY, FID: 0x4000 |
| SMB | Trans2 Request, QUERY_FS_INFO, Query FS Volume Info |
| SMB | NT Trans Request, NT NOTIFY, FID: 0x4001 |
| SMB | Trans2 Request, QUERY_FILE_INFO, FID: 0x400c, Query File Basic |
| SMB | Trans2 Request, QUERY_PATH_INFO, Query File Basic Info, Path: |
| SMB | Trans2 Request, FIND_FIRST2, Pattern: \Neu Textdokument.txt |

1. Test ohne VPN Rename



The image shows a Wireshark network traffic capture window. The main pane displays a list of network packets. The 'SMB' protocol is highlighted in yellow. A red circle highlights the 'Rename Request' packet, which shows the old name '\Neu Textdokument.txt' and the new name '\Tes'. Below it, a 'Find First2' packet is also highlighted, showing the pattern '\Test1.txt'. The interface includes a toolbar with various icons and a search bar at the top.

| Protocol | Info |
|----------|---|
| SMB | Trans2 Request, QUERY_FILE_INFO, FID: 0x8005, Query File Intern |
| SMB | Trans2 Request, QUERY_FILE_INFO, FID: 0x8005, Query File Basic |
| SMB | Close Request, FID: 0x8005 |
| SMB | Rename Request, Old Name: \Neu Textdokument.txt, New Name: \Tes |
| TCP | 1061 > microsoft-ds [ACK] Seq=7569 Ack=8651 Win=65114 Len=0 |
| SMB | Trans2 Request, FIND_FIRST2, Pattern: \Test1.txt |
| TCP | 1061 > microsoft-ds [ACK] Seq=7675 Ack=8835 Win=64930 Len=0 |
| SMB | Trans2 Request, FIND_FIRST2, Pattern: \Test1.txt |
| SMB | Trans2 Request, FIND_FIRST2, Pattern: \Test1.txt |
| SMB | NT Trans Request, NT NOTIFY, FID: 0x4000 |
| SMB | NT Trans Request, NT NOTIFY, FID: 0x4000 |
| SMB | NT Trans Request, NT NOTIFY, FID: 0x4001 |

1. Test ohne VPN Write

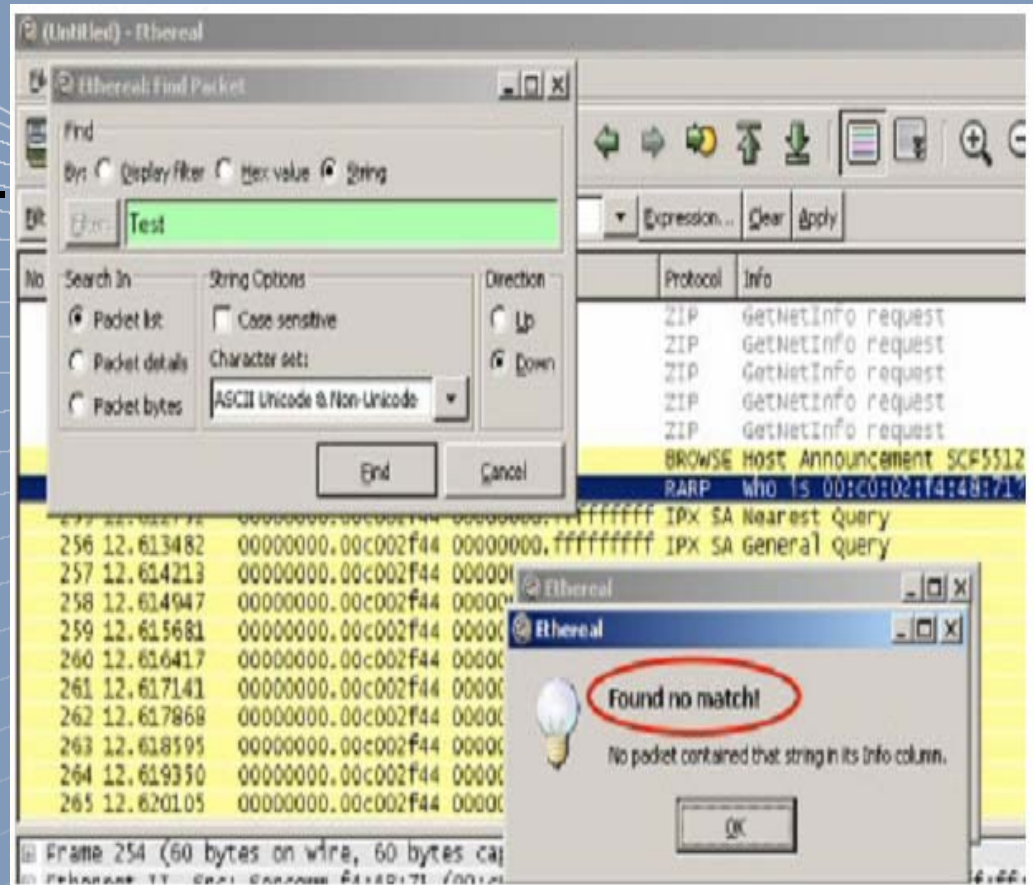
The screenshot shows a network analysis tool window with a toolbar and a packet list. The selected packet is an SMB Write AndX Request. The hex dump and ASCII view of the data are shown below the packet list. A red circle highlights the text 'st ein T estlauf ohne VPN' in the ASCII view.

| Protocol | Info |
|----------|---|
| TCP | 1061 > microsoft-ds [ACK] Seq=13219 Ack=15024 Win=64286 Len=0 |
| SMB | Trans2 Request, QUERY_PATH_INFO, Query File Basic Info, Path: \ |
| SMB | NT Trans Request, NT NOTIFY, FID: 0x4000 |
| SMB | Write AndX Request, FID: 0x800a, 30 bytes at offset 0 |

| Hex | ASCII |
|-------------------------------------|-------------------|
| 01 00 00 0e e0 89 05 c2 ad 58 30 18 |T...AP. |
| 00 00 00 00 00 5e ff 53 4d 42 2f 00 |^SMB/. |
| 07 e8 00 00 00 00 00 00 00 00 00 00 | |
| ff fe 01 08 a3 0f 0e ff 00 de de 0a | |
| 00 ff ff ff ff 00 00 00 00 00 00 1e | |
| 00 00 00 1f 00 ee 44 69 65 73 20 69 | ..@..... ..Dies 1 |
| 69 6e 20 54 65 73 74 6c 61 75 66 20 | st ein T estlauf |
| 20 56 50 4e | ohne VPN |

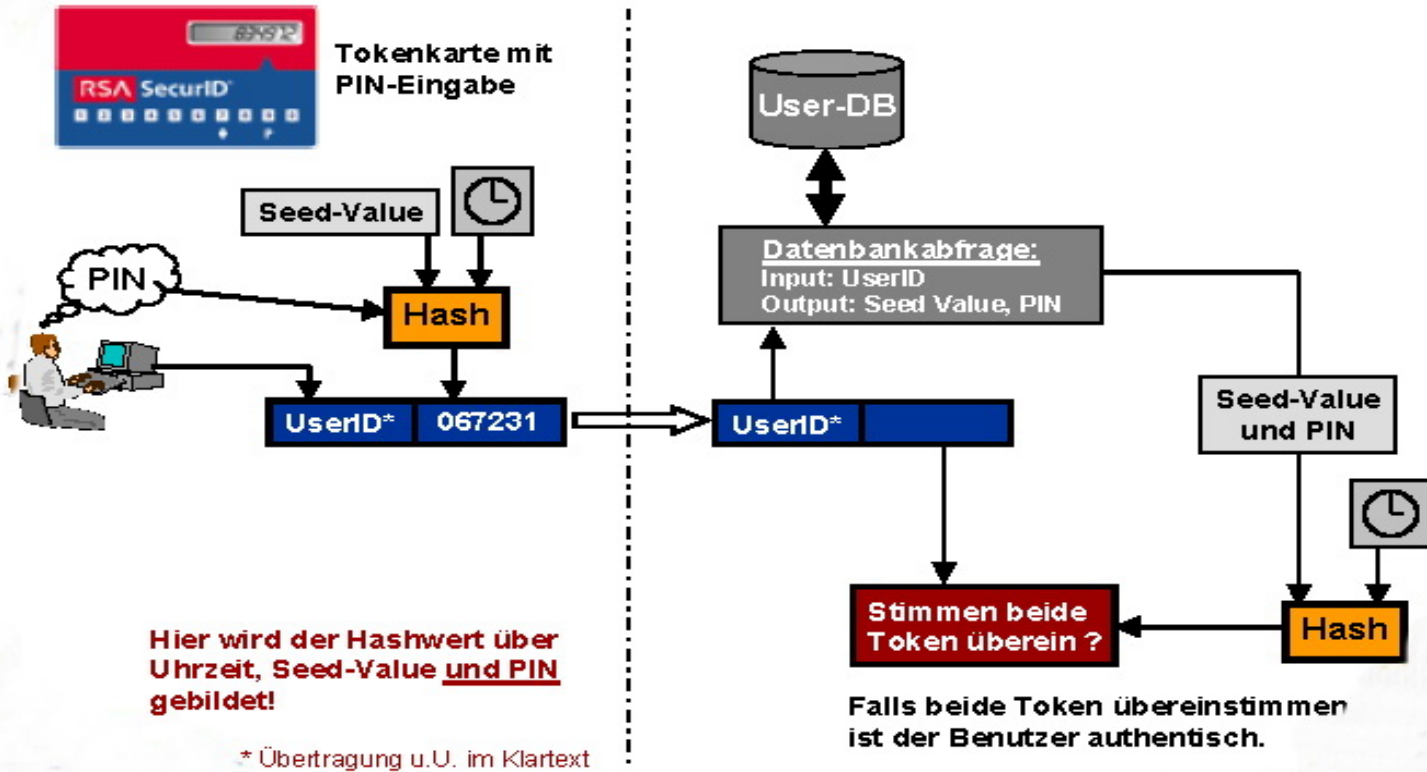
2. Test mit VPN

- Versucht man nun mit aufgebauter VPN-Verbindung nach diesen Befehlen zu suchen...
- Nachricht „Foundnomatch!“



One Time Token (1)

One Time Token / SecurID (1)



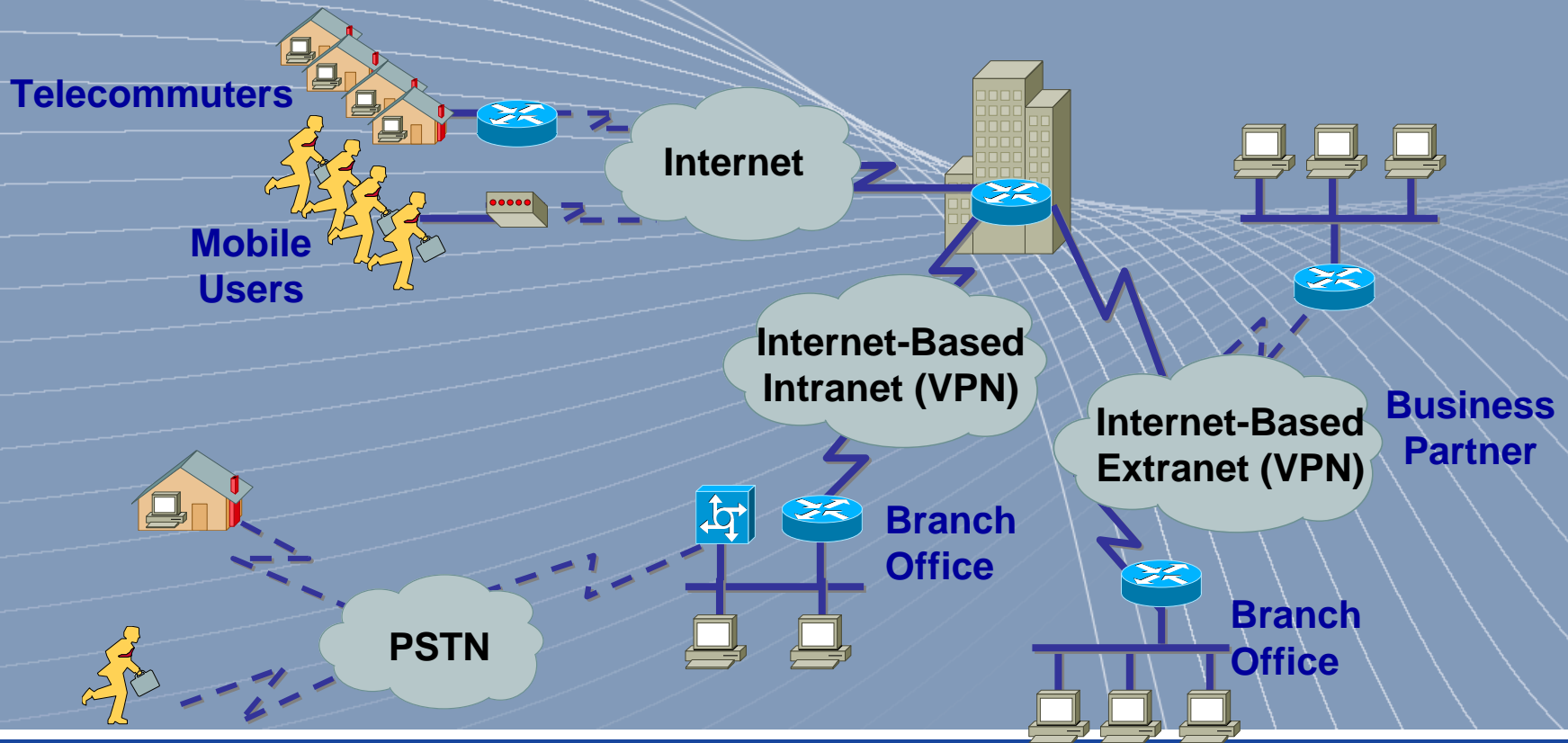
Fazit

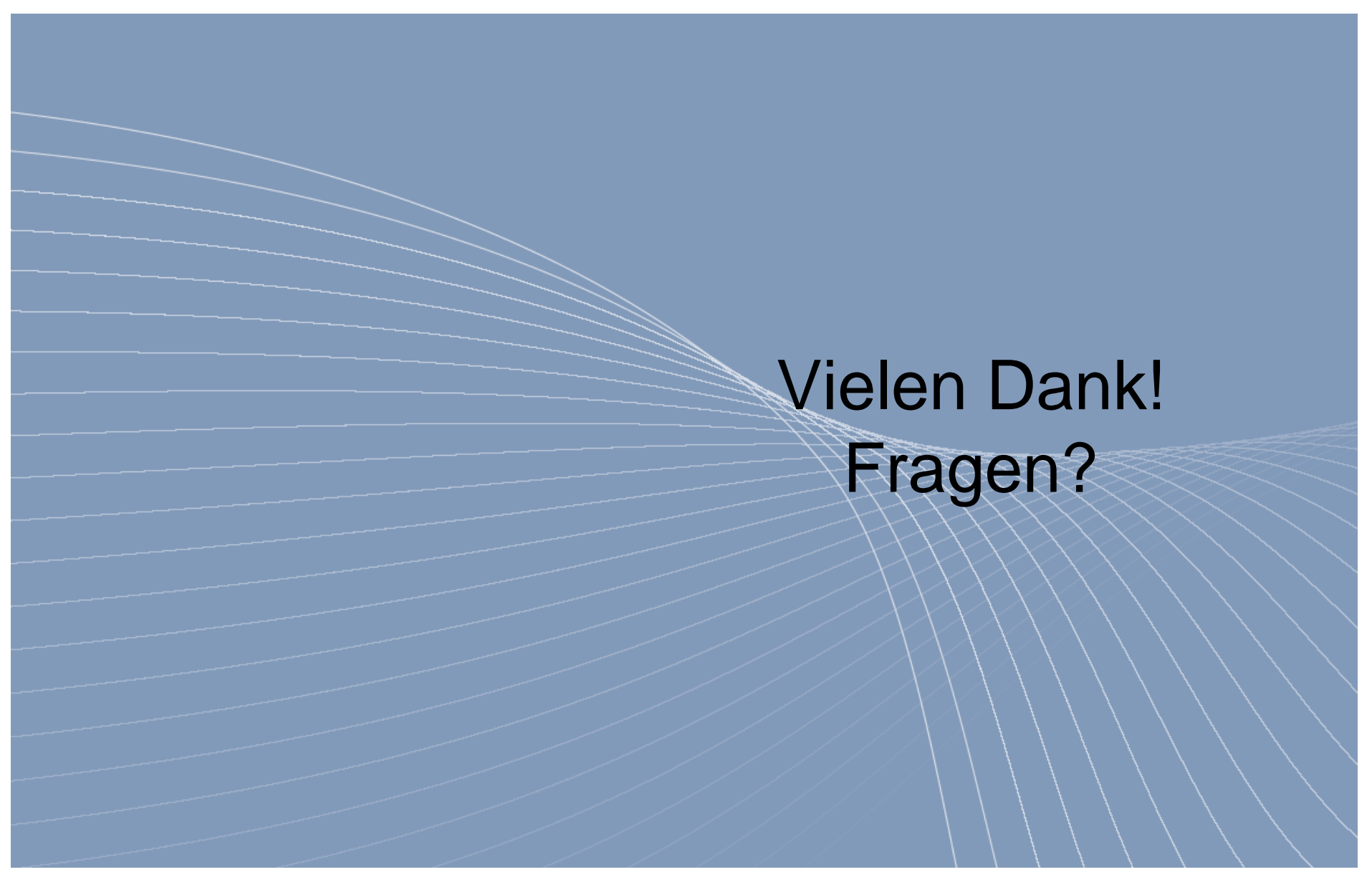
- VPN-Verbindungen bieten ein sehr hohes Maß an Sicherheit
- die beste Alternative zu einer physikalischen Festverbindung – besonders aus wirtschaftlicher Sicht
- Besondere Eignung der Protokolle L2Sec und IPsec over L2TP
- Hoher Konfigurationsaufwand bei IPsec over L2TP
- Investition in ein entsprechendes System.

- stets über die neuesten Entwicklungen informieren, denn ein Protokoll bzw. eine Verschlüsselung ist nicht auf ewig sicher.
- !!! VPN wird immer noch relativ selten verwendet.

Netzwerke von morgen

Offenes Netzwerk





Vielen Dank!
Fragen?