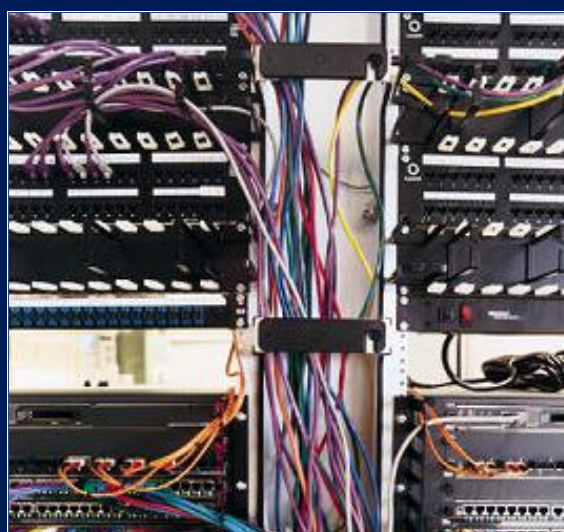
Providerunabhängige Internet VPNs als alternative WAN Infrastruktur

8. April 2003

Engelbert Epple
Senior Technical Consultant
HP Network Solutions Group
engelbert.epple@hp.com

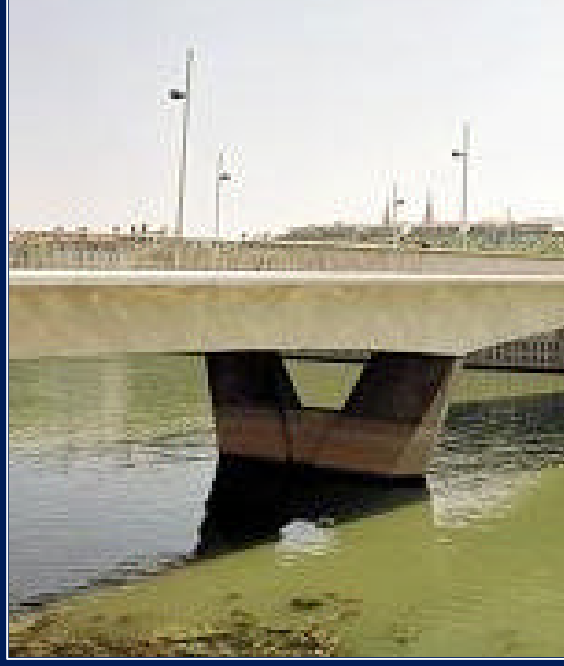
nhalt

- VPN – Definition
- Internet VPNs
  - VPN Typen
  - MPLS vs. IPsec VPN
- VPN – Topologien
  - Site-to Site
  - Combined
  - Dual WAN
- Policy Based Routing
- Firewall oder Router ?
- Security: Schlüsselmanagement



VPN (Virtual Private Networks)

nternehmensnetzwerke in denen die aten über geschützte nternehmensnetze (z. B. ATM, Frame elay..) und teilweise mit entsprechenden icherheitsvorkehrungen (z.B. Tunneling) ber öffentliche Netze, in erster Linie das nternet, transportiert werden.



VPN - Typen

Remote Access VPN

Remote dial in (dial-in, dial-up) der Mitarbeiter auf das Corporate Network

- In erster Linie der Zugang direkt von einem Endsystem (Notebook)

Site-to-Site VPN

Anbindung von festen Lokationen (Branch Office VPN)

- z.B. Verbindungen von Niederlassungen zur Firmenzentrale

Extranet

Verbindungen von Partnerfirmen zum eigenen Corporate Network

- Möglichkeit für Geschäftspartner, auf dedizierte Daten in eigenen Netz zuzugreifen oder z.B. um Fernwartung durchzuführen

Multi Protocol Label Switching

Provider network

"Markiert" einen Datenstrom und ordnet diesen einem VPN zu

Switching statt Routing

Anhand eines Labels entscheiden WAN-Switches wohin Daten geschickt werden und mit welches Priorität

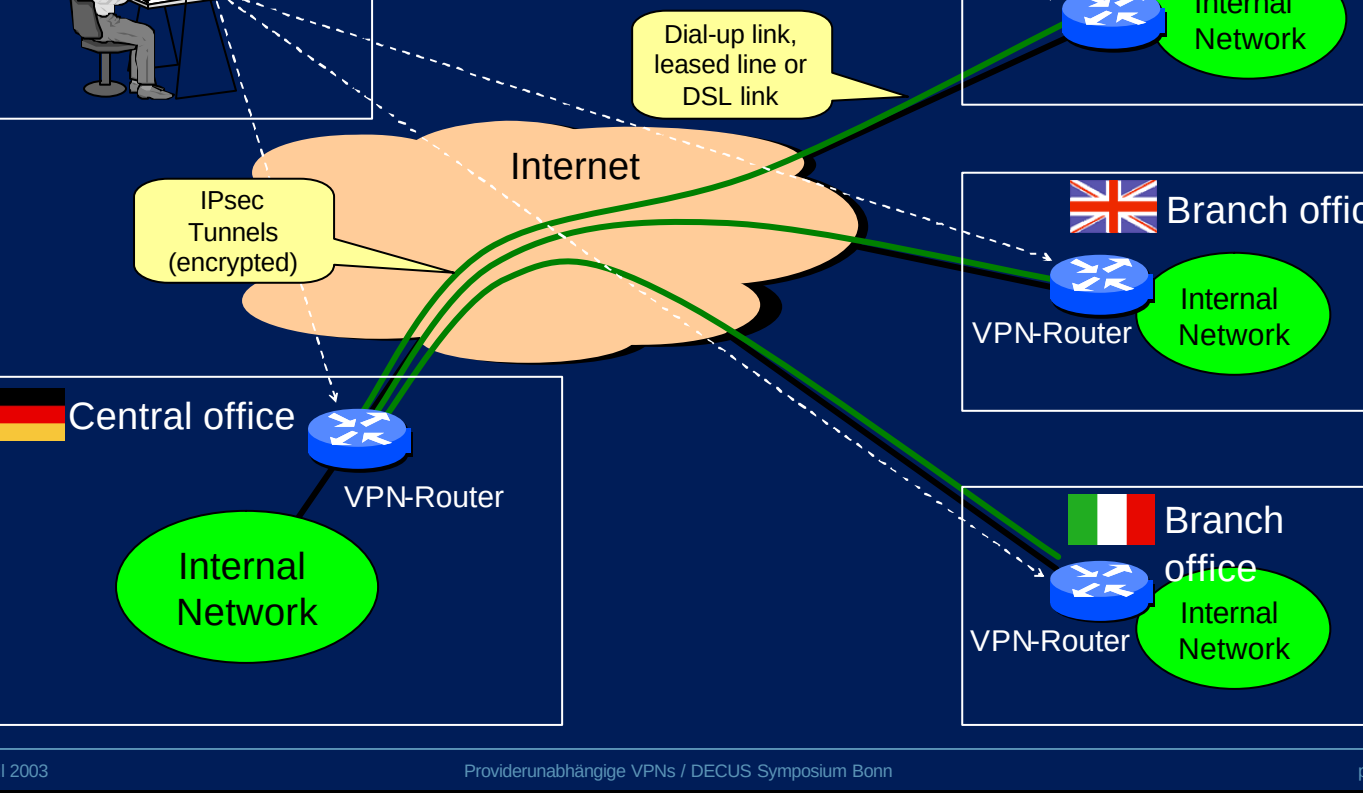
MPLS gilt heute als Nachfolger vom klassischen Frame-Relay Netz

CoS = Classes of Service

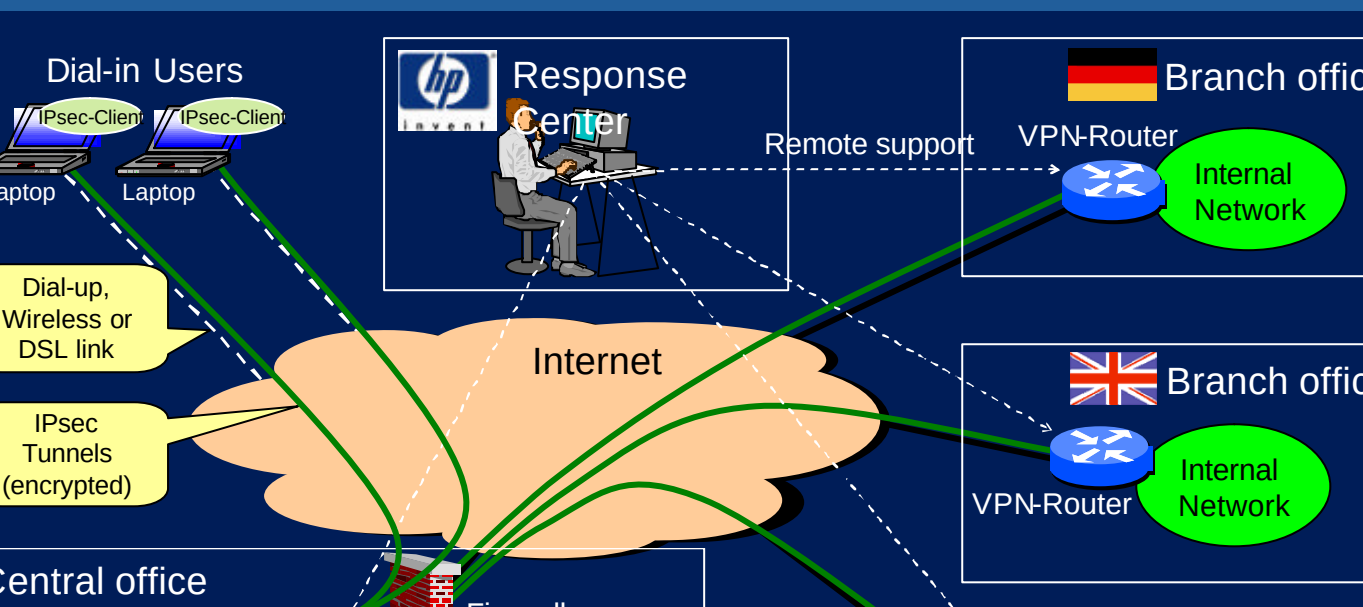
Provider managed – also Kosten für Equipment, Access und Übertragung

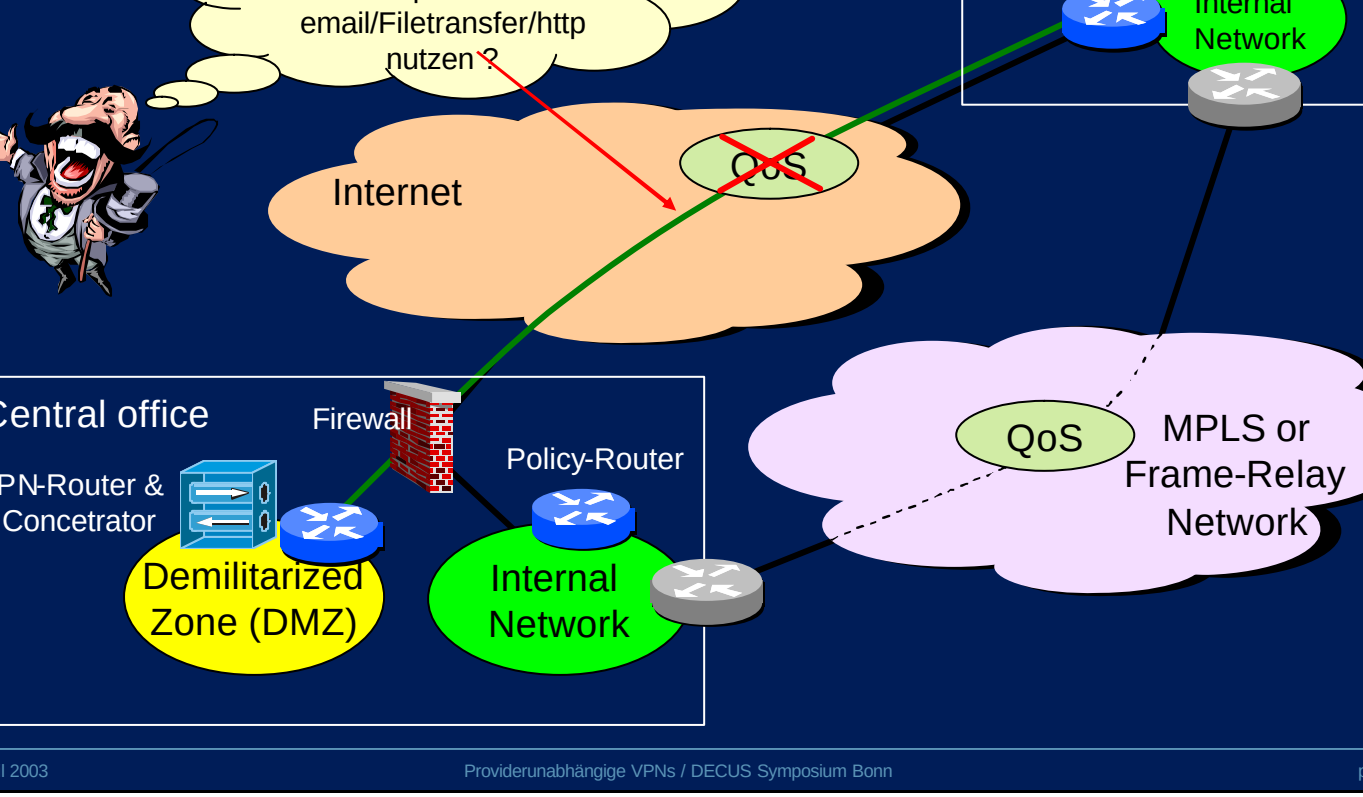
IPsec – Verschlüsselungsstandard

- Public Internet
- Verschlüsselte Datenübertragung – Daten werden "getunnelt"
- Verschlüsselung erfolgt mit Hilfe von VPN-Gateways/Router oder z.B. auf Firewall-Systemen
- IPsec-VPNs gelten heute als flexible Möglichkeit, kostengünstig Site-to-Site oder Remote Access-VPNs zu realisieren
- Keine durchgehenden CoS – aber Priorisierung auf Endsystem möglich
- Providerunabhängig
- Welteweit verfügbar – Internet Access gibt's fast überall

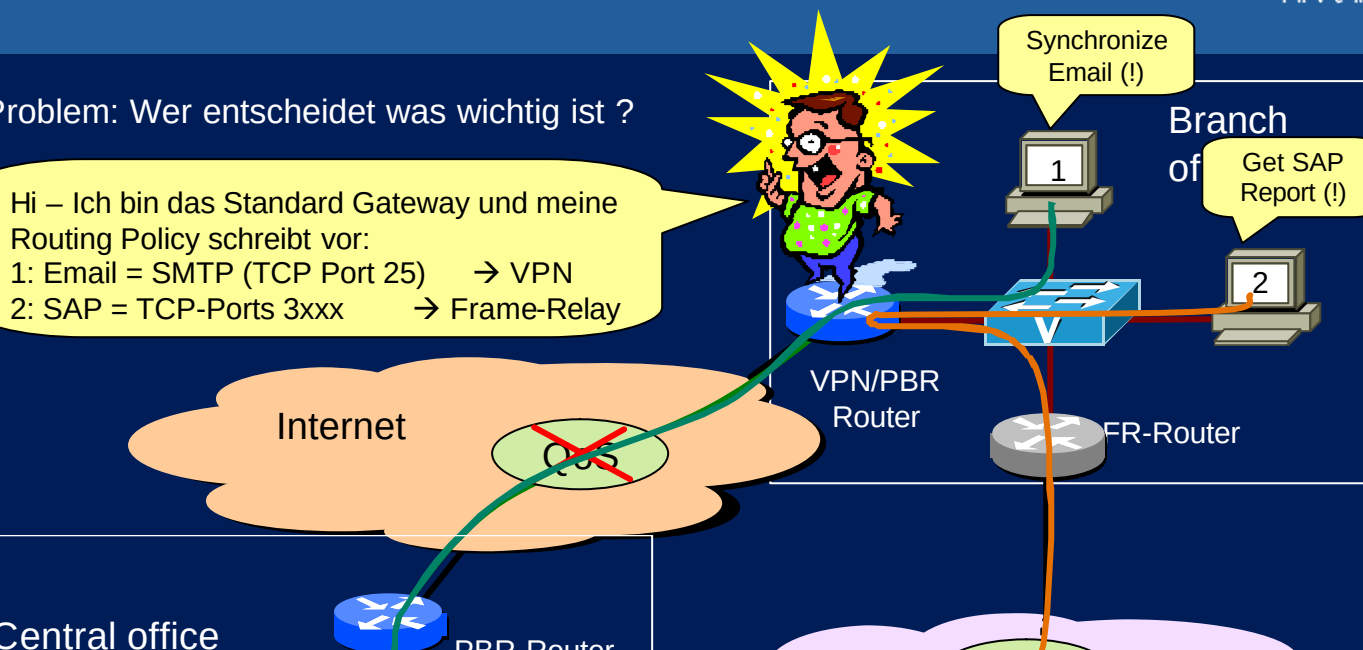


Combined VPN: Remote Access and Site-to-Site



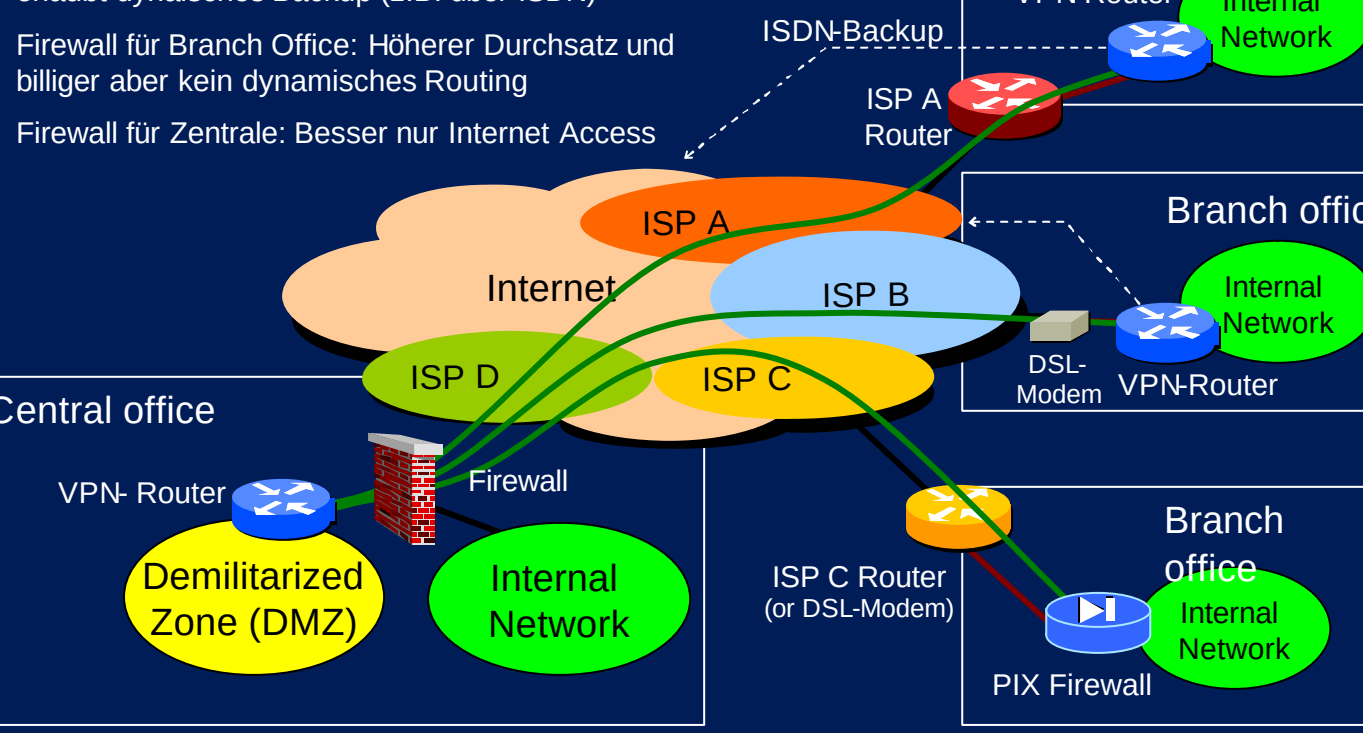


olicy Based Routing (PBR)



Firewall für Branch Office: Höherer Durchsatz und billiger aber kein dynamisches Routing

Firewall für Zentrale: Besser nur Internet Access



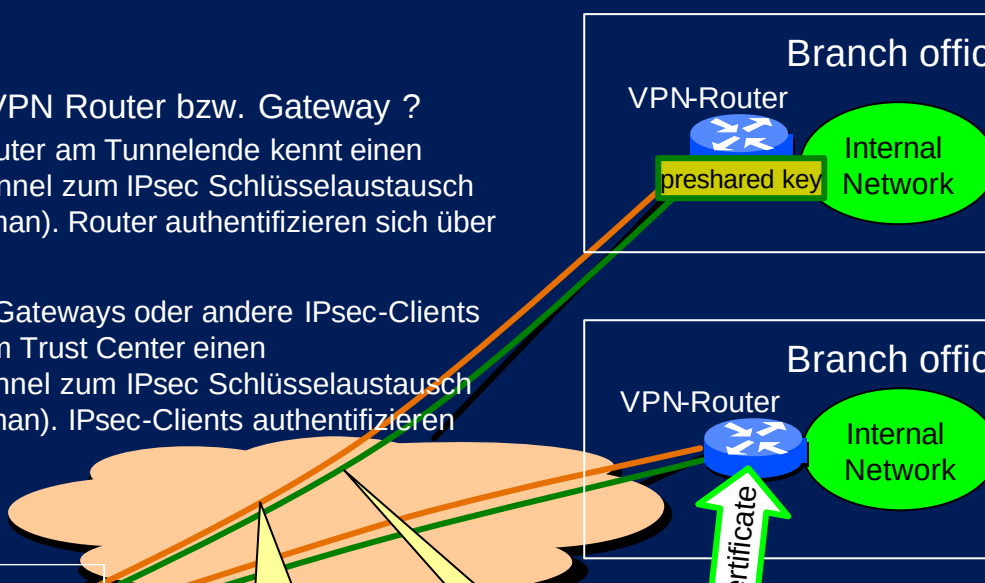
Security: Schlüsselaustausch

Problem:

Wie authentifizieren sich VPN Router bzw. Gateway ?

Pre-shared keys: Jeder Router am Tunnelende kennt einen gleichen Schlüssel. IKE-Tunnel zum IPsec Schlüsselaustausch wird aufgebaut (Diffie-Hellman). Router authentifizieren sich über pre-shared keys.

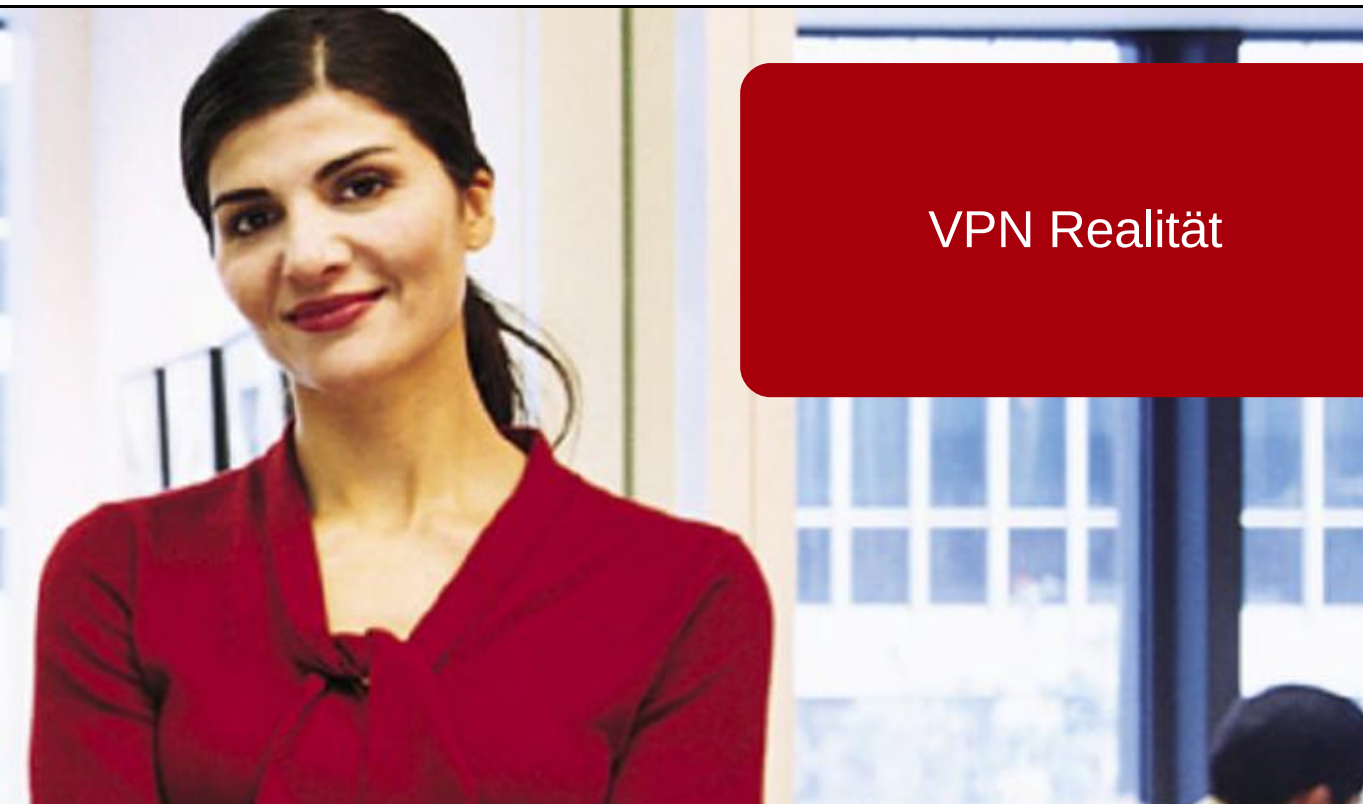
Certificates: VPN-Router, -Gateways oder andere IPsec-Clients erhalten einmalig von einem Trust Center einen „Personalausweis“. IKE-Tunnel zum IPsec Schlüsselaustausch wird aufgebaut (Diffie-Hellman). IPsec-Clients authentifizieren sich über Certificates.

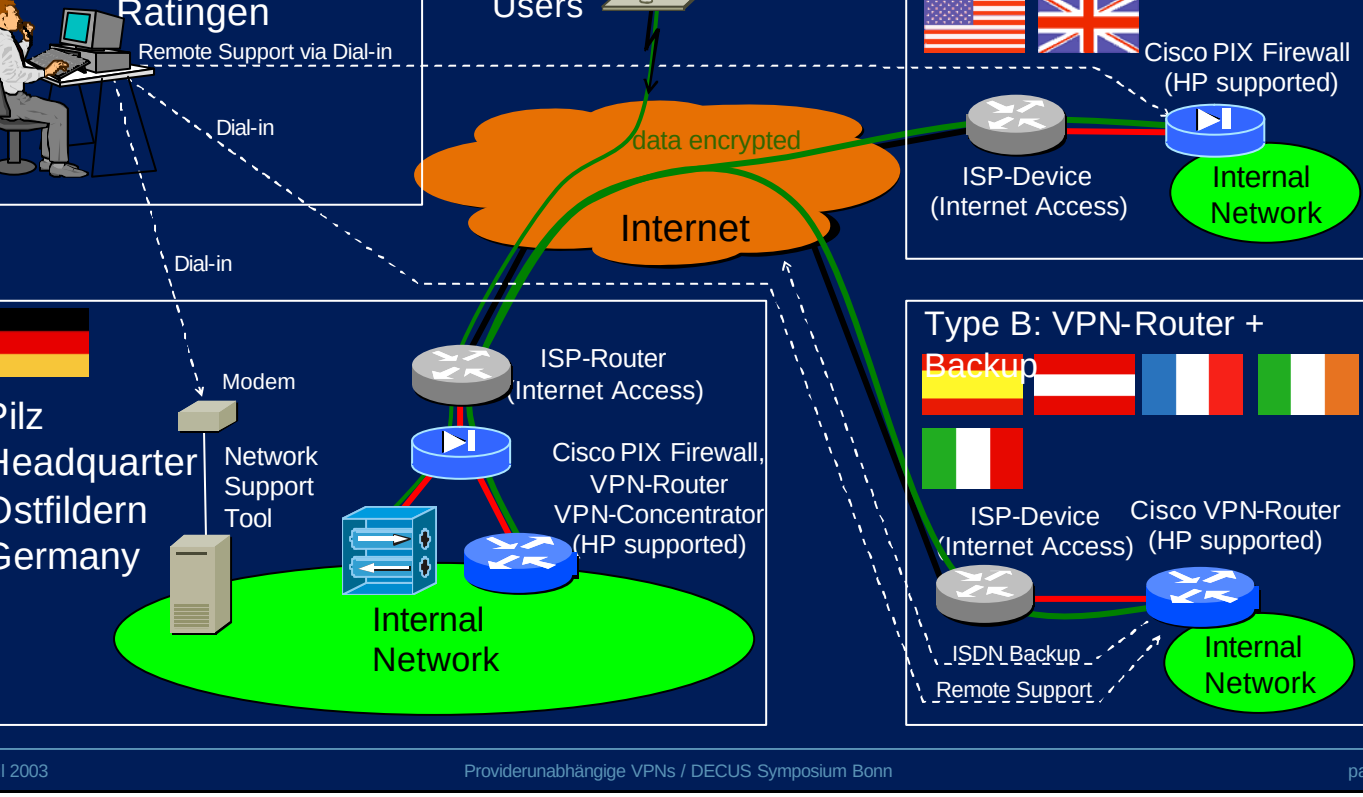


Standard User	400 $	5 Stunden	38 Jahre	No way.
Hacker	10.000 $	12 Minuten	556 Tage	10^{19} Jahre
Geheimdienst	10 Mio. $	20 msec.	21 Minuten	10^{17} Jahre

Quelle: Cisco / Stand 1996

Bei einer angenommen Verdoppelung der Rechenleistung innerhalb von 2 Jahren, sind die angegeben Werte heute (2002) maximal um den Faktor 16 kleiner geworden





Messung im Pilz VPN

Zeitraum:

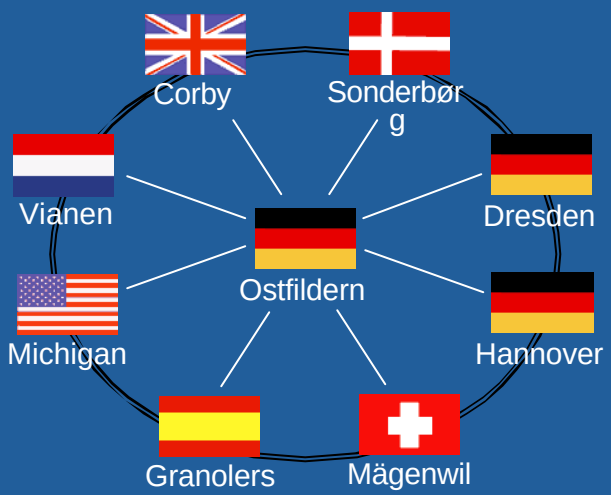
vom 25.11.2002 – 28.3.2003

Methode:

Standard *ping* vom NST (Netzwerk Support Tool, PC im LAN) zu einem PC im Remote LAN mit MRTG

Standorte:

Spanien



Langzeitmessung mit IVPN läuft permanent

- Leichter Zugriff in fast Echtzeit per Browser
- Ping auf belasteten Leitung ist nur beschränkt repräsentativ

Meine Interpretation:

- Auch ohne QoS – gute Ergebnisse
- Spanien: Internet & VPN auf einer Zuleitung – trotzdem geht‘s ☺
- Tipp: separater Zugang für VPN

21.3. – 28.3.2003


150 - 230 ms


71 – 86 ms

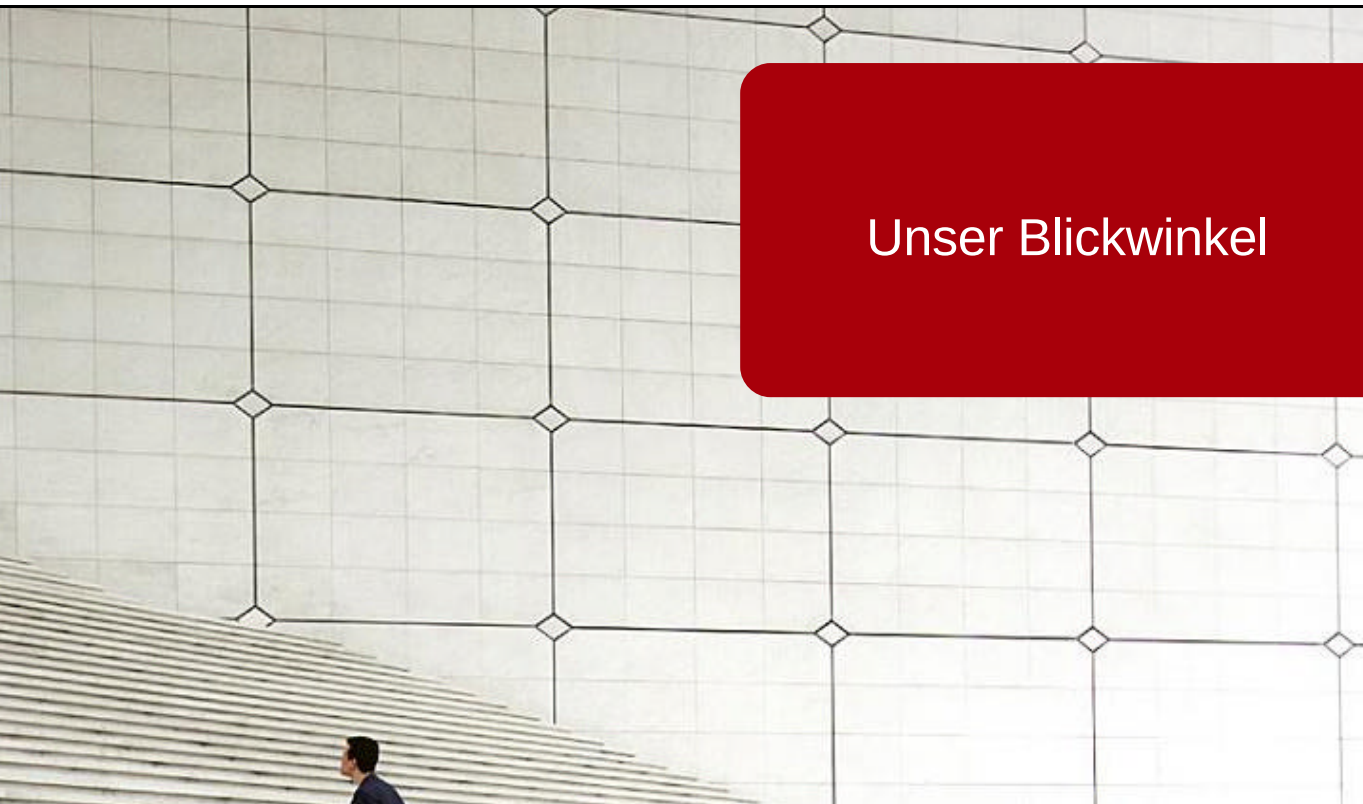

54 – 81 ms


30 – 72 ms


48 – 73 ms


60 – 106 ms


113 – 129 ms



Unser Blickwinkel

VPN-Router proaktiv

Kunde erwartet Single Point of contact für eine Komplettlösung inklusive Internet-Zuleitungen.

Kunde erwartet eine Rechnung

Kunde hat bereits ein Provider-managed WAN (Frame-Relay) und benötigt zusätzliche VPN Services.

Lösung für Kunden, die „All-in-one“ Preise akzeptieren

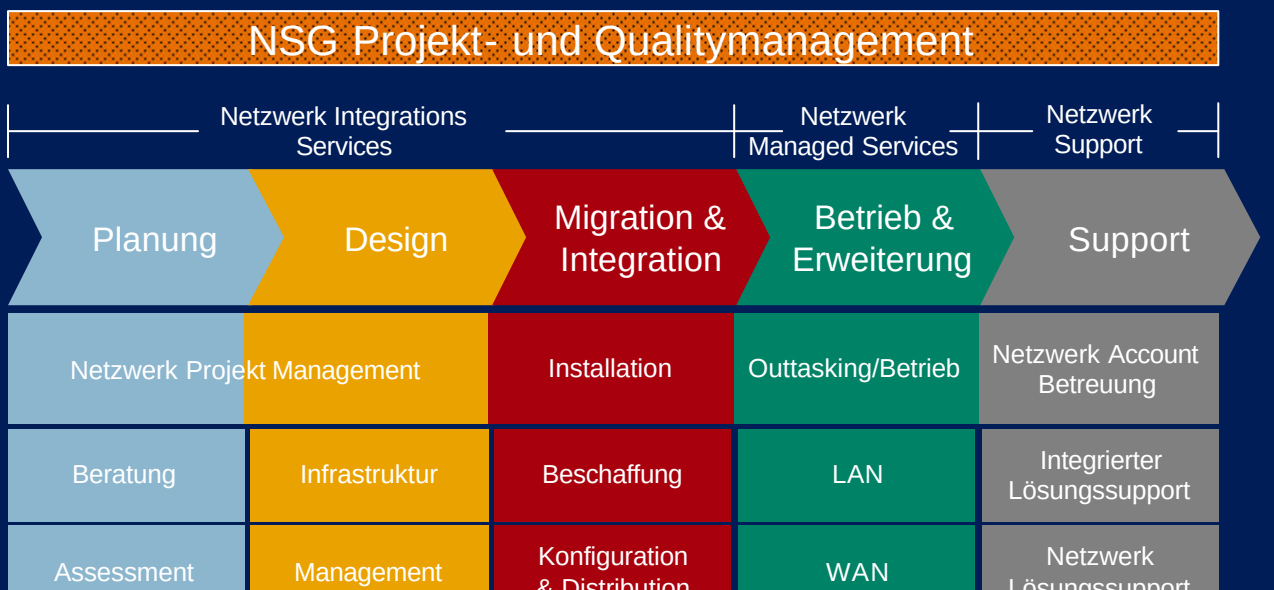
Service- Dienstleistungen für das VPN Equipment

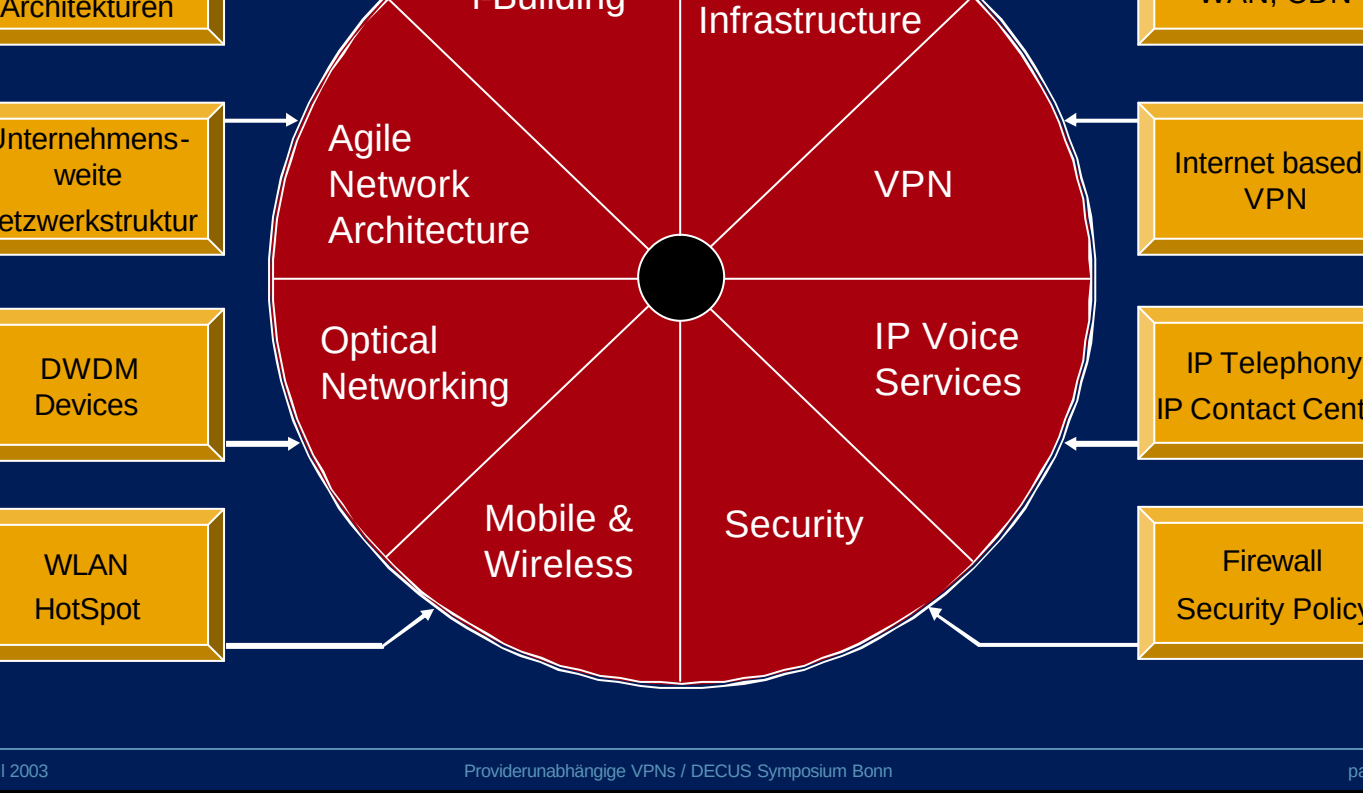
- Kunde mietet günstige Internet Zugänge selbst an
- Kunde möchte VPN Equipment kaufen anstatt mieten (Reduzierung monatlicher Kosten)
- Kunde möchte Hilfe wenn’s “brennt” und technischen Support bei Providerfragen
- Kunde akzeptiert verschiedene Rechnungen von ISPs und HP
- Kunde möchte seine Router unter eigener Verantwortung halten und benötigt High Level Support und HW-Service
- Lösung für Kunden, die keinen Full-Service bezahlen wollen.

selbst

- Kunde möchte VPN Equipment günstigs evtl. durch Einsatz vo PC-basierenden Lösungen
- Kleine Firmen sin nicht überzeugt, eine Second oder Third leve Support zu benötigen.
- Lösung für Kunden di entweder genügen KnoHow im Haus haben oder die länger Ausfallzeiten hinnehmen.

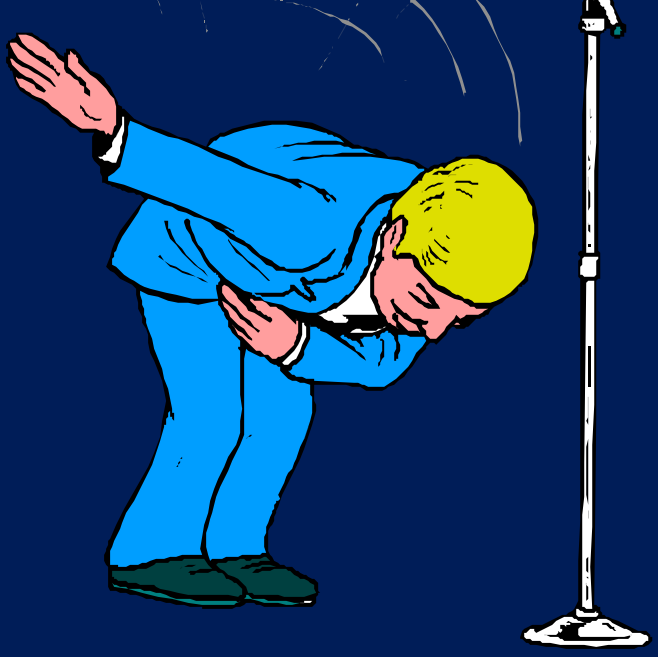
Netzwerk Lifecycle





Uberblick HP Netzwerk Services

- **Consulting**
  - Netzwerkplanung, Konzeptentwicklung
  - Security Consulting, PKI
  - Netzwerktrends, künftige Entwicklungen
- **Assessments**
  - Netzwerk Ist-Aufnahmen & Dokumentation
  - Analysen, Empfehlungen & Design-Ansätze
  - Entscheidungsvorbereitung &
- **Cisco AS inside**
  - Kombination aus HP NAS & Cisco Service
  - Dedizierter Ansprechpartner bei Cisco
  - Cisco: SW Strategie, Performance, NW Design
- **Monitoring**
  - Network Monitoring = NAS „plus“
  - Remote Netzwerk Überwachung
  - Detailliertes Reporting
- **NAS**
  - Network Availability Support = NCS „Plus“
  - Dedizierte Ansprechpartner im Supportcenter



invent