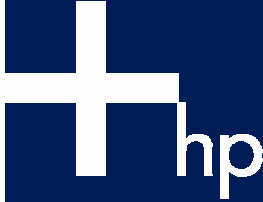
 invent

HP supported VPN


Providerunabhängige Internet VPNs als alternative WAN Infrastruktur

DECUS Symposium
21. April 2004

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

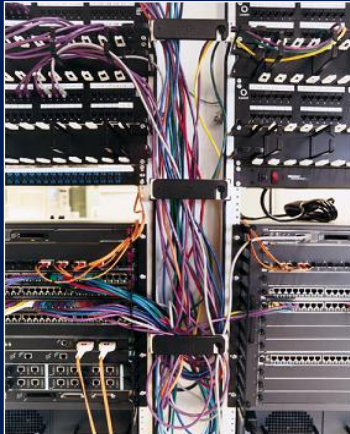


© 2004 Hewlett-Packard Development Company, L.P.
The information contained herein is subject to change without notice

 invent

Inhalt

- VPN – Definition
- Internet VPNs
 - VPN Typen
 - MPLS vs. IPsec VPN
- VPN – Topologien
 - Site-to Site
 - Combined
 - Dual WAN
- Policy Based Routing
- Firewall oder Router ?
- Anbindungsarten
- Security
 - Krypto-ALgorithmen/Analyse
 - Security Risiken
 - IPsec Ziele
 - Schlüsselaustausch/management
 - Pre shared secrets/Zertifikate
 - Certificate Authority (CA)
 - Paralleler Internetzugang
 - Redundanzszenario
- Geschwindigkeiten im VPN: Beispiel
- HP supported VPN
- Future Look




21. April 2004 Internet VPNs Copyright © HP Corporate presentation. All rights reserved 2

hp
invent

VPN Definition

VPN (Virtual Private Networks)

Unternehmensnetzwerke in denen die Daten über geschützte Unternehmensnetze (z. B. ATM, Frame Relay..) und teilweise mit entsprechenden Sicherheitsvorkehrungen (z.B. Tunneling) über öffentliche Netze, in erster Linie das Internet, transportiert werden.



21. April 2004 Internet VPNs Copyright © HP Corporate presentation. All rights reserved 3

hp
invent


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

Eine besondere Form des VPN:

- **Internal VPN**
Basiert auf dem eigenen Corporate Network
 - z.B. ein verschlüsseltes Overlay Netz für sensitive Daten (Manager VPN)

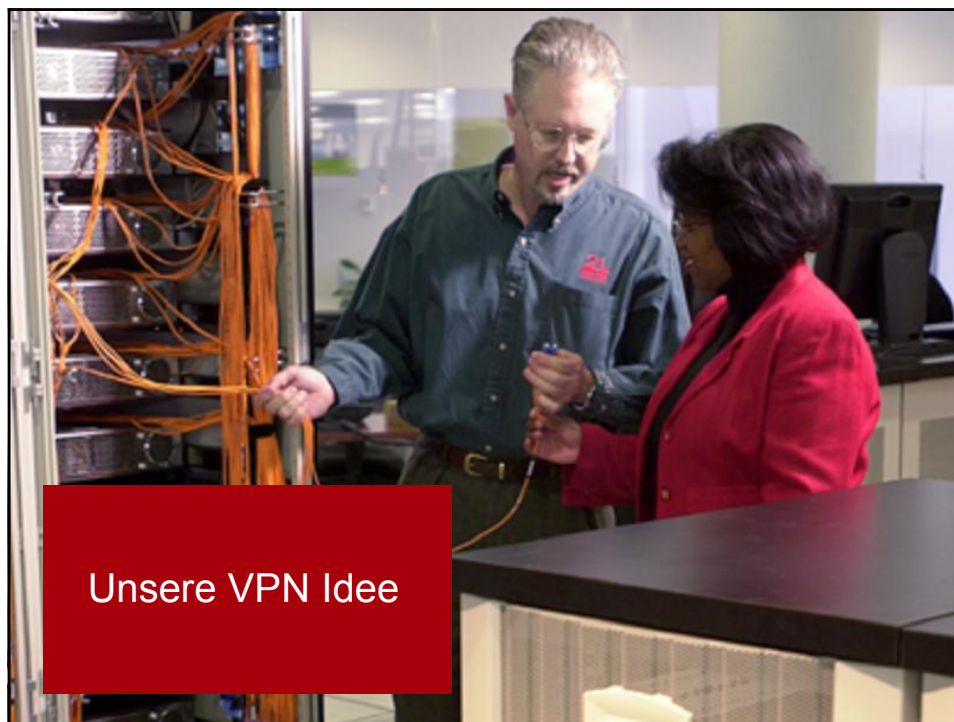
21. April 2004 Internet VPNs Copyright © HP Corporate presentation. All rights reserved 4

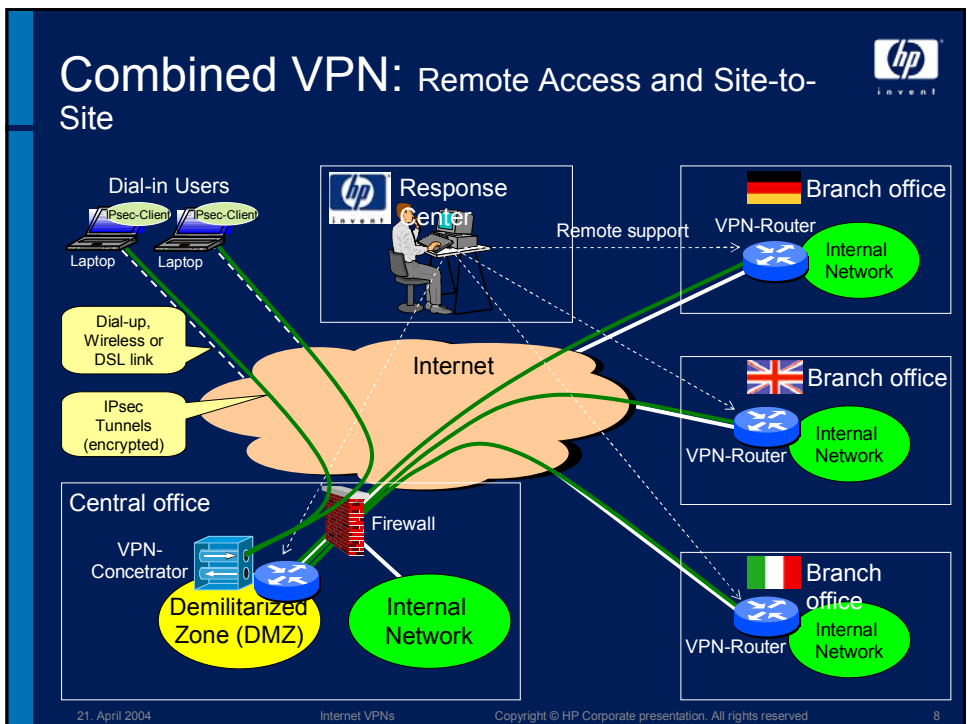
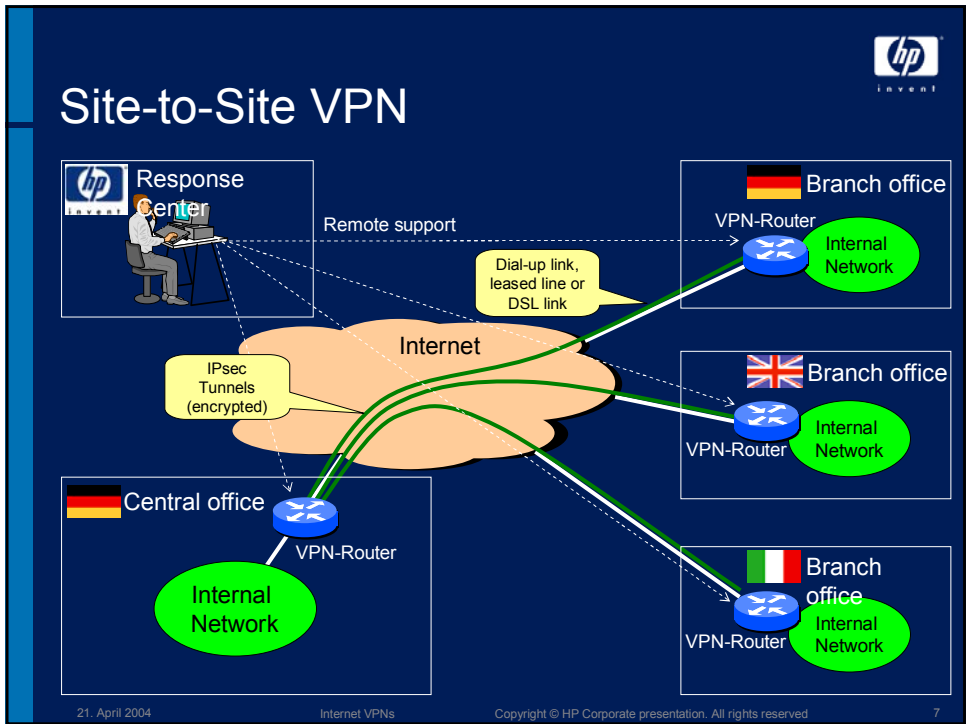


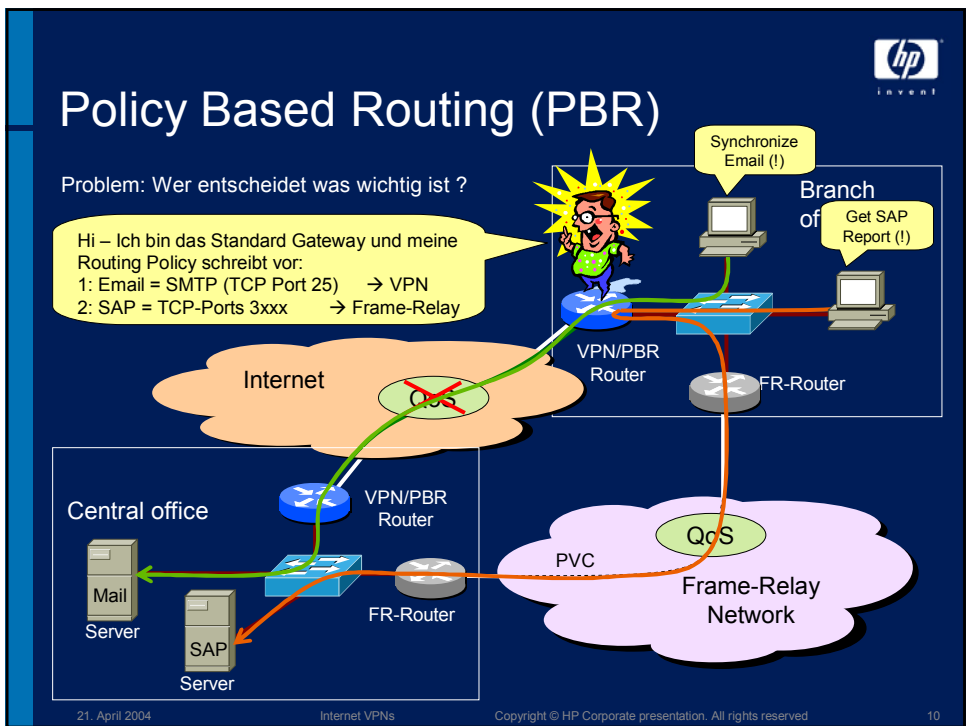
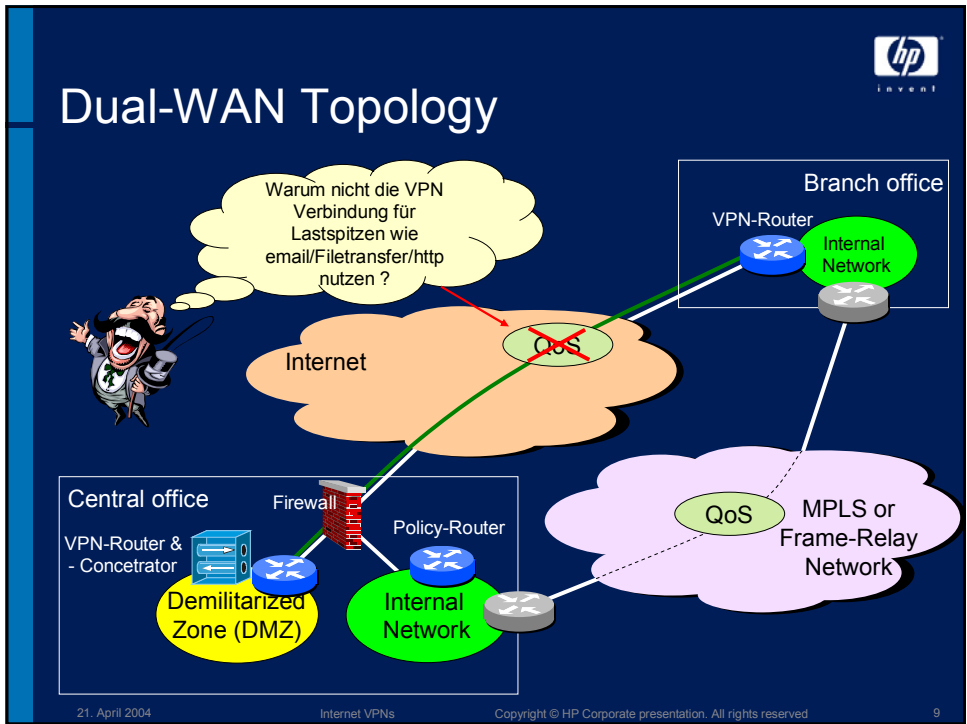
MPLS vs. Internet VPN

<h3>MPLS</h3> <p>Multi Protocol Label Switching</p> <ul style="list-style-type: none">• 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 welcher Priorität• MPLS gilt heute als Nachfolger vom klassischen Frame-Relay Netz• CoS = Classes of Service• Provider managed – also Kosten für Equipment, Access und Übertragung	<h3>IPsec VPN</h3> <p>Routing verschlüsselter IP Pakete</p> <ul style="list-style-type: none">• Public Internet• Verschlüsselte Datenübertragung – Daten werden "getunnelt" (RFC 2401, 2402 u. 2406)• 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• Weltweit verfügbar – Internet Access gibt's fast überall
--	---


21. April 2004 Internet VPNs Copyright © HP Corporate presentation. All rights reserved 5





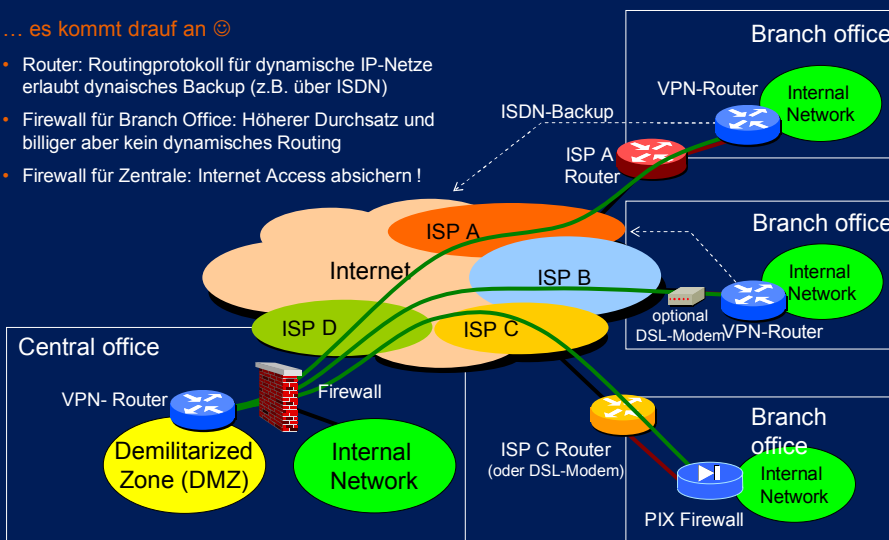


Firewall oder Router ?



... es kommt drauf an ☺

- Router: Routingprotokoll für dynamische IP-Netze erlaubt dynaisches Backup (z.B. über ISDN)
- Firewall für Branch Office: Höherer Durchsatz und billiger aber kein dynamisches Routing
- Firewall für Zentrale: Internet Access absichern !



21. April 2004 Internet VPNs Copyright © HP Corporate presentation. All rights reserved 11


Anbindungsarten



- Zentrale Anbindung ans Internet
 - **WICHTIG: Feste IP Adressen !**
 - Leased Line(s) bei COLT, Telekom, ...
 - SDSL
- Anbindung Außenstellen
 - **ADSL**
 - ISDN (Wählverbindung)
 - leased line
- Remote Access Clients
 - ADSL
 - ISDN
 - Wireless HotSpot
 - ... what you can get ☺



21. April 2004 Internet VPNs Copyright © HP Corporate presentation. All rights reserved 12




Internet Anbindungen

Beispiele für die Verwendung zur VPN Anbindung von Außenstellen
Stand 17. April 2004

Nr.	Typ	BW down kbit/s	BW up kbit/s	Fltrate möglich ?	Volumen geschätzt	Volumen inclusive	einmalig		monatlich	
							Bereitstellung* Telekom / ISP	Kosten flat	Kosten Volumen	
1	ADSL	1024	128	ja	5 GB	5 GB	86 €	49 €	27 €	
2	ADSL	3072	384	ja	> 20GB	>20GB	86 €	73 €	n/a	
3	ADSL	2048	192	ja	2 GB	2 GB	108 €	80 €	31 €	
4	ADSL	2048	384	ja	2 GB	2 GB	151 €	82 €	32 €	
5	ADSL	3072	256	ja	5 GB	5 GB	129 €	99 €	49 €	
6	ADSL	3072	512	ja	5 GB	5 GB	151 €	103 €	53 €	
7	SDSL	1024	1024	nein	10 GB	2 GB	349 €	n/a	211 €	
8	SDSL	2048	2048	nein	10 GB	5 GB	349 €	n/a	189 €	
9	ISDN(Dial-in)	128	128	nein	n/a	n/a	0 €	436 €	n/a	
10	ISDN(Dial-in)	256	256	nein	n/a	n/a	0 €	872 €	n/a	
11	Festverbindung	128	128	nein	5 GB	0 GB	0 €	n/a	394 €	
12	Festverbindung	2048	2048	nein	10 GB	0 GB	1.990 €	n/a	1.026 €	

21. April 2004 Internet VPNs Copyright © HP Corporate presentation. All rights reserved 13






Kryptografische Algorithmen

Symmetrisch = gleiche Schlüssel für Ver- und Entschlüsselung		Asymmetrisch = verschiedene Schlüssel für Ver- und Entschlüsselung	
Chiffre	Schlüssellänge	Chiffre	Schlüssellänge
Blowfish	1-448 Bit	Knapsack	?
DES	56 Bit	RSA	mind. 1024 Bit
IDEA	128	El Gamal	512-1024 Bit
RC4	1-2048 Bit	Symetrische Verfahren sind schneller und werden daher in IPsec zur Verschlüsselung eingesetzt. Diffie-Hellman: Verfahren zum initialen Schlüsselaustausch IKE: Autom. Schlüsselaustausch und Identitätsnachweis	
RC5	128-256 Bit		
Rijndael (= AES)	128-256 Bit		
Serpent	128-256 Bit		
Triple DES	168 Bit		
Twofish	128-256 Bit		

21. April 2004
Internet VPNs
Copyright © HP Corporate presentation. All rights reserved
15




Kryptoanalyse

Angreifer	Budget ¹⁾	56-Bit (DES) ¹⁾	168-Bit (3DES) ¹⁾	Rijndael = AES ²⁾
Standard User	400 \$	38 Jahre	No way.	No way.
Hacker	10.000 \$	556 Tage	10 ¹⁹ Jahre	No way
Geheimdienst	10 Mio. \$	21 Minuten	10 ¹⁷ Jahre ³⁾	10 ¹⁰ Jahre ⁴⁾

¹⁾ Quelle: Cisco Trainingsunterlagen / Stand 1996
²⁾ Quelle: Andrew S. Tanenbaum, Computernetzwerke 4.Auflage 2003
³⁾ Cisco geht von einer Verdoppelung der Rechenleistung alle 2 Jahre aus → Werte heute circa um den Faktor 32 kleiner. Geheimdienst bräuchte heute ca 10¹² Jahre beim 3DES
⁴⁾ Tanenbaum geht dabei von einen theoretischen Parallelrechner mit 1 Mrd Prozessoren aus – mit einer Leistung von einer Schlüsselauswertung in einer Sekunde – bei 3 x 10³⁸ möglichen Schlüsseln ... ein Haufen Arbeit ☺

21. April 2004
Internet VPNs
Copyright © HP Corporate presentation. All rights reserved
16



Security Risiken

Security Risiko	Beispiele	Verteidigung durch
Denial of Service (DoS, DDoS)	<ul style="list-style-type: none"> • TCP Synflood • Ping of Death • Smurf 	<ul style="list-style-type: none"> • Intrusion Detection (IDS) • Firewall / Access-Lists
Privacy Violation	<ul style="list-style-type: none"> • Datenmanipulation • Aktive Attacken (Replay) • Passive Attacken (Sniffing) 	<ul style="list-style-type: none"> • Encryption z.B. durch IPSec VPNs
Einbrüche	<ul style="list-style-type: none"> • Unberechtigter Zugriff • Identity Spoofing 	<ul style="list-style-type: none"> • Encryption z.B. durch IPSec VPNs • Strong Authentication (AAA, Certificates, Token)

• Firewall / Access-Lists

• Interne vs. Externe Angriffe = 80% / 20%

21. April 2004
Internet VPNs
Copyright © HP Corporate presentation. All rights reserved
17




IPSec Ziele

Ziel	Methode	IPSec Protokoll
Confidentiality (gegen Sniffing)	Encryption	ESP
Authentication (gegen aktive Attacken)	Symmetrisch: DES, 3DES, AES (Asymmetrisch: RSA) HMAC (Hashed message authentication code):	ESP (früher: AH)
Integrity (gegen aktive Attacken)	SHA (168Bit) oder MD5 (128Bit)	

- ESP: Encapsulating Security Payload (Layer 4), AH = Authentication Header
- Beide Tunnelendpunkte müssen im Besitz der **gleichen** Schlüssel sein
- Pro 3DES ESP Tunnel: 4 Schlüsselpaare (3 * DES + 1 * HMAC)
- Problem: Wie können Schlüssel sicher und dynamisch über ein „untrusted“ Medium wie das Internet ausgehandelt werden ?
→ Lösung: **IKE** als IPSec Key Management Protokoll

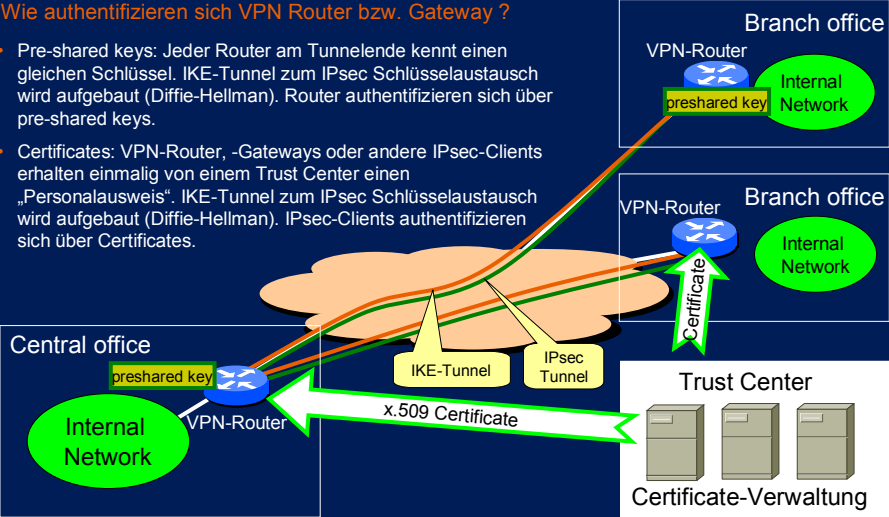
21. April 2004
Internet VPNs
Copyright © HP Corporate presentation. All rights reserved
18

Schlüsselaustausch




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.

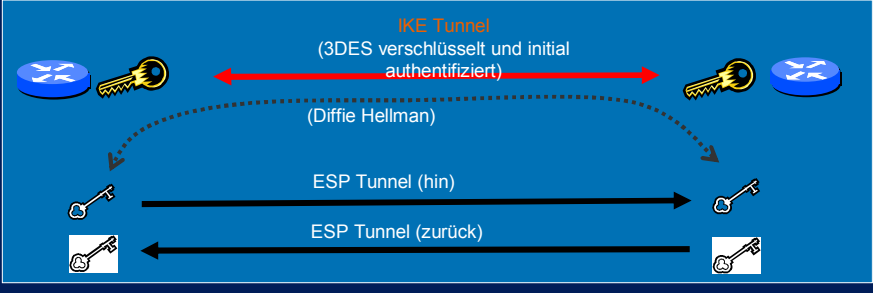


21. April 2004 Internet VPNs Copyright © HP Corporate presentation. All rights reserved 19

Schlüsselmanagement



- Beide Endpunkte benötigen je einen identischen Schlüssel für ESP Encryption (bzw. zwei für 3DES) und einen für die Authentifizierung (HMAC)
- Aushandlung symmetrischer Schlüssel mittels **Diffie Hellman** mit Hilfe des **IKE** (Internet Key Exchange) Protokolls
- Schlüssel haben nur beschränkte **Lebenszeit**
→ Regelmäßige Generierung neuer Schlüsselpaare
- IKE Tunnel verschlüsselt (DES/3DES) und Endpunkte authentifizieren sich mit:
 - **Preshared Secrets**
 - **Zertifikaten** (ausgestellt von einem Trusted Root z.B. Verisign CA)



21. April 2004 Internet VPNs Copyright © HP Corporate presentation. All rights reserved 20

Preshared Secrets vs. Zertifikate

Authentifizierung für IKE Tunnel Aushandlung notwendig, um Man-In-the-Middle Attacks auszuschließen

- **Preshared Secrets:** Auf beiden Tunnelendpunkten manuell konfigurierter Schlüssel
→ **pro Tunnel**
Problem: Für dynamische Tunnelendpunkte (z.B. ADSL) muss ein „Wildcard Preshared Secret“ angelegt werden !
- **Zertifikate:** Ein CA Server (d.h. ein gemeinsamer Trusted Root) stellt den Endpunkten „Ausweise“ nach IETF Standard x.509 aus
→ **pro Router**

Vorteil: Zertifikate können zentral verwaltet, erneuert oder zurückgezogen werden. Manuelle Konfiguration auf Routern minimal. Fully meshed VPN realisierbar.

Eigener CA Server (W2k Server) vs.

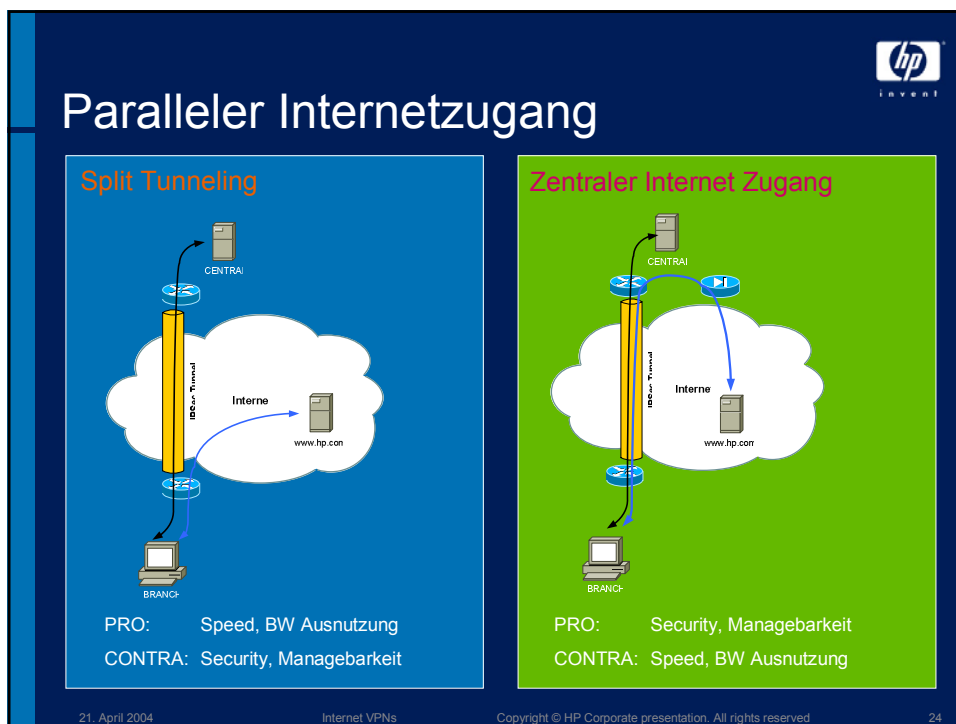
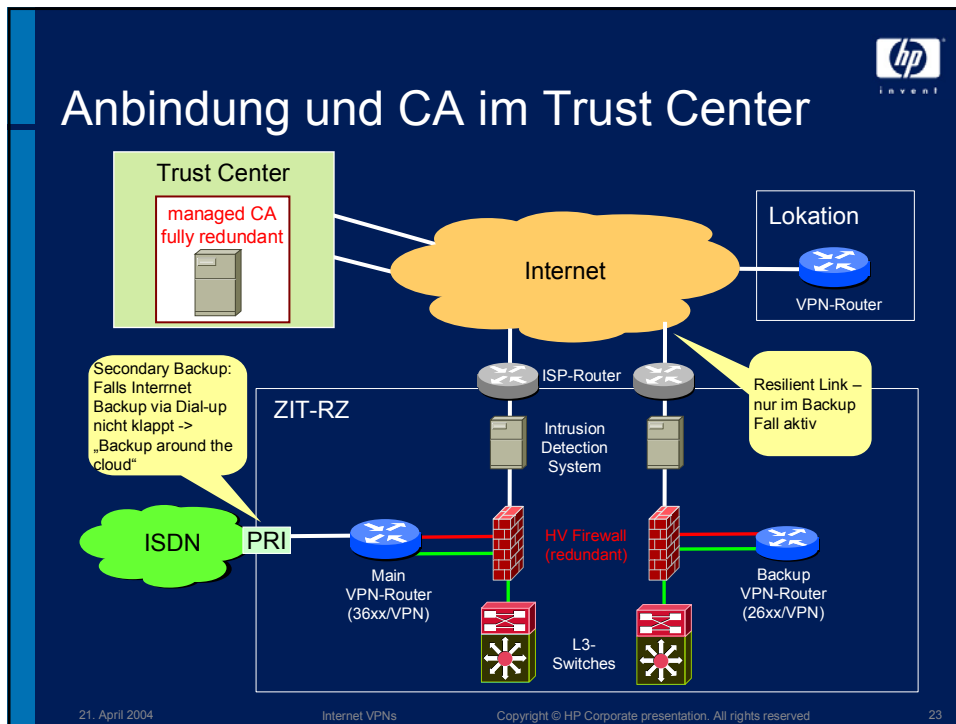
Copyright © HP Corporate presentation. All rights reserved. 21

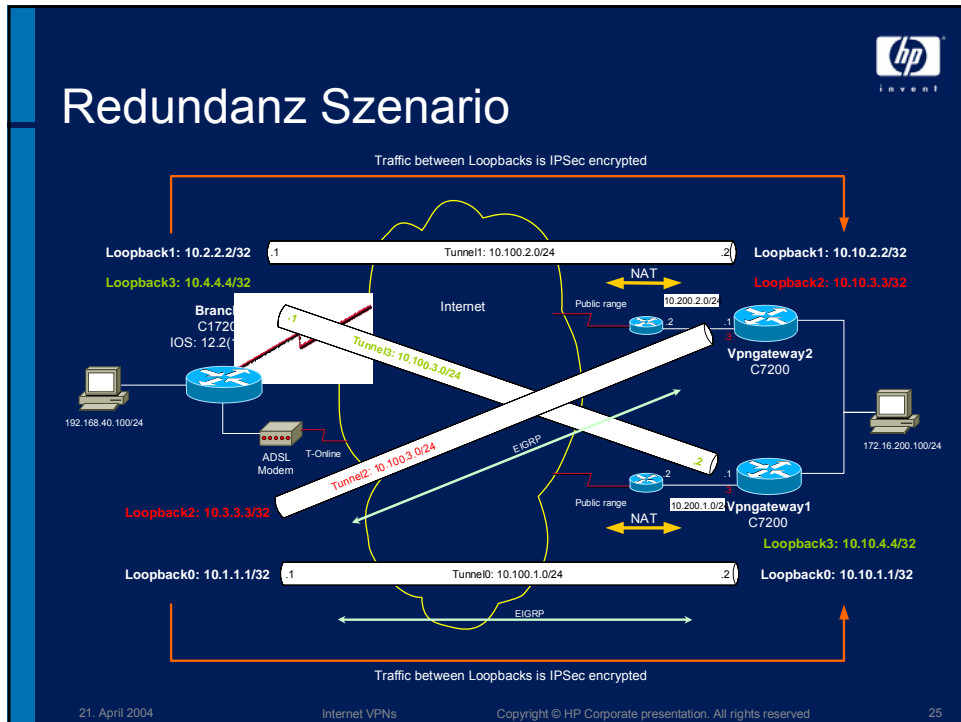
Anbindung und self managed CA

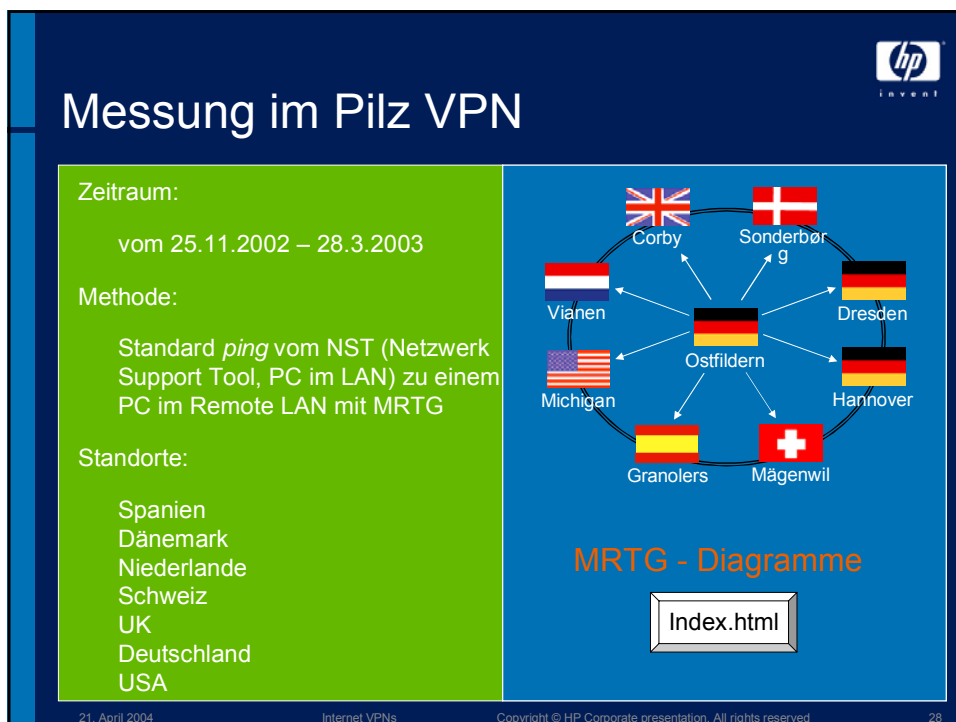
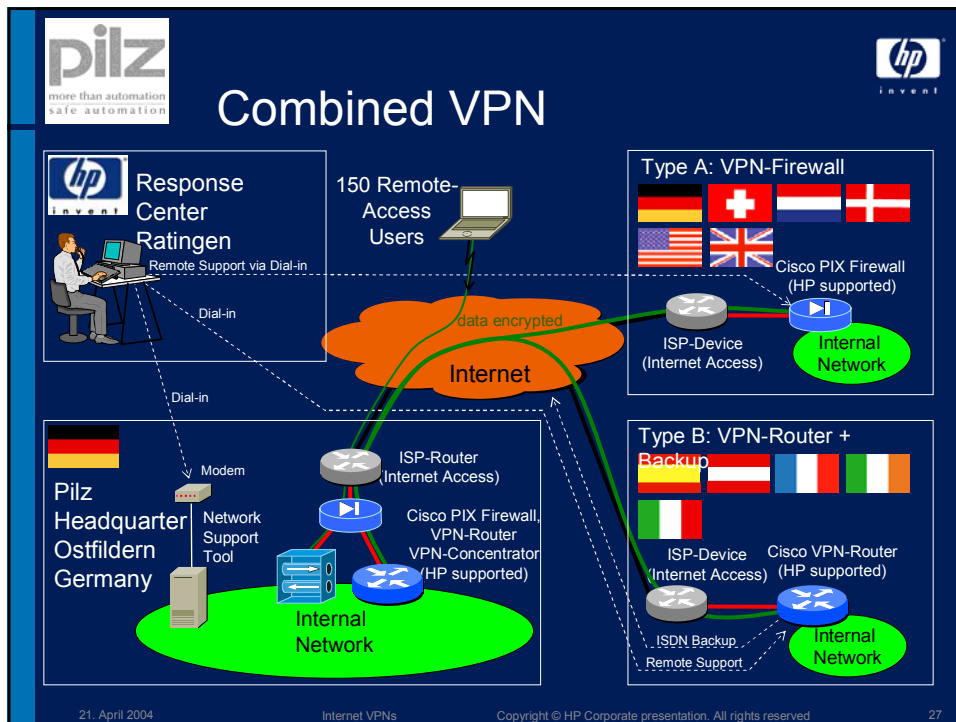
Secondary Backup: Falls Internet Backup via Dial-up nicht klappt -> „Backup around the cloud“


ISDN PRI

Copyright © HP Corporate presentation. All rights reserved. 22









Messung im Pilz VPN








Zusatzinfo's:

- Langzeitmessung mit MRTG 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

Wochendurchschnitt
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

21. April 2004 Internet VPNs Copyright © HP Corporate presentation. All rights reserved 29






HP supported VPN: Positionierung

Fully outsourced VPN:	HP supported VPN:	Self made VPN:
<ul style="list-style-type: none"> • Provider managed 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 	<ul style="list-style-type: none"> • HP erbringt reaktive Support- und 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. 	<ul style="list-style-type: none"> • Kunde realisiert VPN selbst • Kunde möchte VPN-Equipment günstigst, evtl. durch Einsatz von PC-basierenden Lösungen • Kleine Firmen sind nicht überzeugt, einen Second oder Third level Support zu benötigen. • Lösung für Kunden die entweder genügend KnoHow im Hause haben oder die längere Ausfallzeiten hinnehmen.

21. April 2004
Internet VPNs
Copyright © HP Corporate presentation. All rights reserved
31



Netzwerk Lifecycle

NSG Projekt- und Qualitymanagement				
Netzwerk Integrations Services		Netzwerk Managed Services	Netzwerk Support	
Planung	Design	Migration & Integration	Betrieb & Erweiterung	Support
Netzwerk Projekt Management	Installation	Outtasking/Betrieb	Netzwerk Account Betreuung	
Beratung	Infrastruktur	Beschaffung	LAN	Integrierter Lösungssupport
Assessment	Management	Konfiguration & Distribution	WAN	Netzwerk Lösungssupport
	Security	Installation & Abnahme	Security	Netzwerk Verfügbarkeitsupport
			Web Infrastruktur	Netzwerk HW & SW Support
NSG Leistungen			MS	NSG

21. April 2004
Internet VPNs
Copyright © HP Corporate presentation. All rights reserved
32



Future look

what we are going to do...

- WAN Traffic Management (Traffic Shaping)
 - Ein- UND ausgehender traffic (Layer 7) wird steuerbar
 - Optionale Kompression pro Applikation
 - Tipp Download Vortrag 2H04 ☺
- Radware
 - Loadsharing in der Zentrale – über zwei ISPs ohne BGP ☺

21. April 2004

Internet VPNs

Copyright © HP Corporate presentation. All rights reserved

33

