Forschungszentrum Jülich
in der Helmholtz-Gemeinschaft

Vortrag 2G01

L2TP over IPSEC

Remote Access VPN

Werner Anrath
Forschungszentrum Jülich
Zentralinstitut für Angewandte Mathematik

IT Symposium 2004 in Bonn
21.04.2004

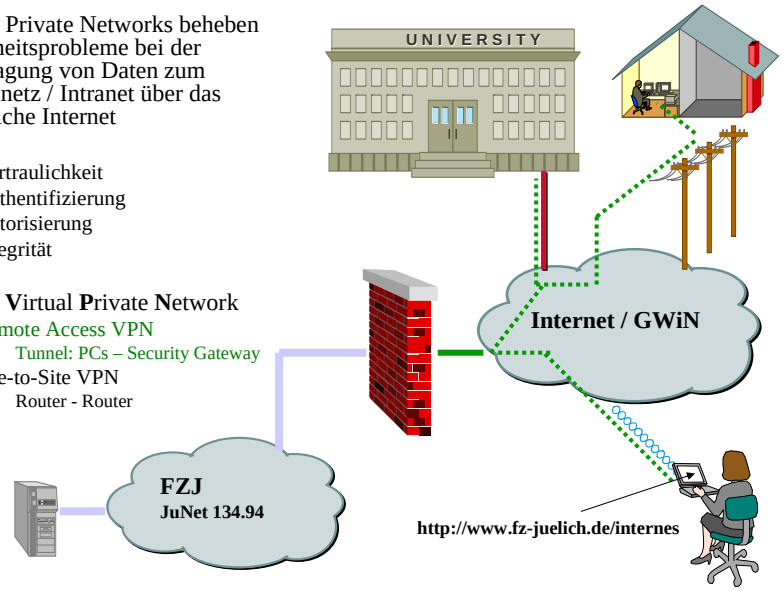
Forschungszentrum Jülich
in der Helmholtz-Gemeinschaft

Inhalt

Forschungszentrum Jülich
in der Helmholtz-Gemeinschaft

Definition – Virtual Private Networks

- Virtual Private Networks beheben Sicherheitsprobleme bei der Übertragung von Daten zum Firmennetz / Intranet über das öffentliche Internet
  - Vertraulichkeit
  - Authentifizierung
  - Autorisierung
  - Integrität
- VPN = **V**irtual **P**rivate **N**etwork
  - Remote Access VPN
    - Tunnel: PCs – Security Gateway
  - Site-to-Site VPN
    - Router - Router

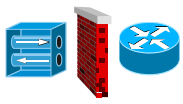


Werner Anrath - Zentralinstitut für Angewandte Mathematik 3

Forschungszentrum Jülich
in der Helmholtz-Gemeinschaft

Überblick - VPN Protokolle

OSI-Layer:	Protokolle:	Plattformen:	Geräte:
Application	ssh (scp, sftp), https, s/mime	*UNIX,Windows*	
Presentation			
Session			
Transport	Secure socket layer (TCP)	*UNIX, Windows*	
Network	~~PPTP~~, L2PT, **IPSEC**	*UNIX, Windows 2000/XP*	
Data Link	~~MPPE~~, ~~WEP~~	*LINUX-, Windows-PPP*	
Physical			



WEP = Wired Equivalent Privacy
MPPE = Microsoft Point-to-Point Encryption
PPTP = Point to Point Tunneling Prototocol
L2TP = Layer 2 Tunneling Protocol (over IPSEC)
IPSEC = Internet Protocol Security

Werner Anrath - Zentralinstitut für Angewandte Mathematik 4

Forschungszentrum Jülich
in der Helmholtz-Gemeinschaft

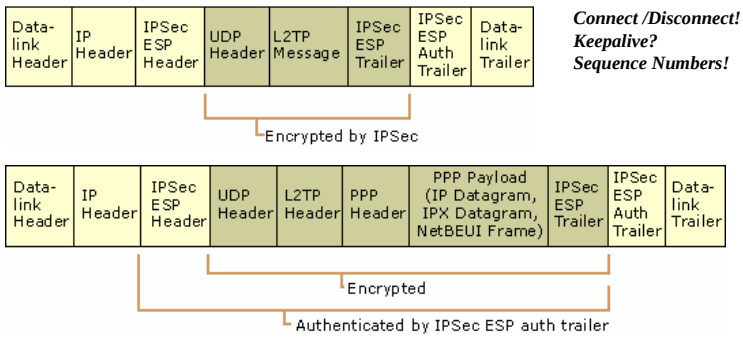
VPN-Betrieb im Forschungszentrum

- CISCO VPN Client im Produktionsbetrieb seit Oktober 2001
  - IPSEC-Lösung mit proprietären Erweiterungen:
    - xauth, mode-config, keepalive .....
  - primäre VPN-Technik im Forschungszentrum
    - Windows, LINUX und MacOS
  - Einschränkungen:
    - Installation der Cisco-Client Software nötig
- Erweiterung VPN-Angebot im Frühjahr 2003
  - L2TP over IPSEC
  - RFC-Standard
  - favorisierte Protokoll-Suite von Microsoft
  - komfortable Unterstützung in Windows XP
- Hardware-Unterstützung /Tunnelendpunkte
  - CISCO PIX
  - CISCO VPN 3030 Concentrator
  - April 2004: > insgesamt 450 VPN-Anwender

Forschungszentrum Jülich
in der Helmholtz-Gemeinschaft

L2TP over IPSEC Bausteine - L2TP Vorstellung -

- L2PT = Layer 2 Tunneling Protocol
- Weiterentwicklung von PPTP und L2F (Layer 2 Forwarding, CISCO)
- PPP Frames werden in IP/UDP-Rahmen übertragen
- RFC 2661 (L2TP) und RFC 3193 (L2TP over IPSEC)
  - Kontroll-Pakete und Daten-Pakete verwenden UDP Port 1701
  - IPSEC wird zum Verschlüsseln der Payload Information verwendet



Connect /Disconnect!
Keepalive?
Sequence Numbers!

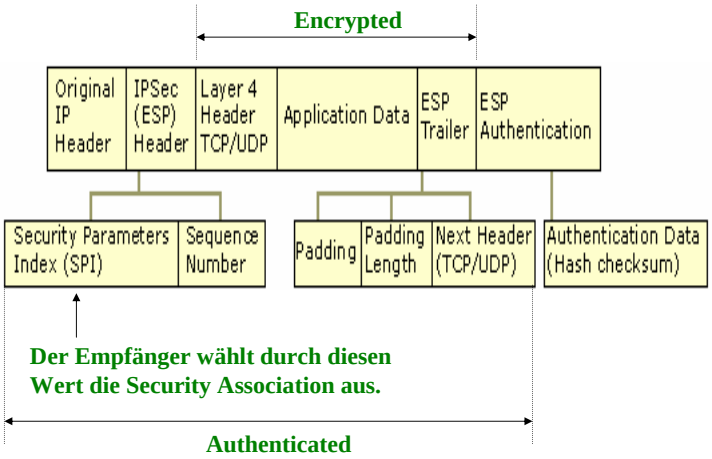
Forschungszentrum Jülich
in der Helmholtz-Gemeinschaft

L2TP over IPSEC Bausteine - IPSEC Technik -

- **IPSEC** = Internet Protocol Security
  - RFC 2401-2412, RFC 2451
- unterstützt in IPv6 (required) und IPv4 (optional)
  - Linux, Windows 2000 /XP
  - CISCO VPN Lösungen
    - Cisco VPN Client
    - Cisco IOS, PIX-Firewall, VPN 3000 Concentrator Serie
- IPSEC-Protokolle
  - Datentransfer, Transport- oder Tunnel-Modus
  - AH = Authentication Header (Protocol Number 51), RFC 2402
  - **ESP = Encapsulating Security Payload (Protocol Number 50),** RFC 2406
- **IKE = Internet Key Exchange** (UDP PORT 500), RFC 2409
  - Kontrollverbindung
  - SA = Security Association, diese ist eine unidirektionale Verbindung zwischen zwei IPSEC Systemen
    - Verschlüsselungsalgorithmen, Lebensdauer, Transport- oder Tunnel-Modus
    - IKE SA + Receive SA + Send SA

Forschungszentrum Jülich
in der Helmholtz-Gemeinschaft

L2TP over IPSEC Bausteine - IPSEC ESP Header -

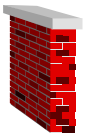


L2TP over IPSEC Bausteine - IPSEC und IKE -

Forschungszentrum Jülich
in der Helmholtz-Gemeinschaft

Main Mode SA Request - Preshared Key - Initiert wegen Crypto ACL

Initiator



Responder

Isakmp Hdr, SA Proposals (DES, SHA, . . .)

Isakmp Hdr, selected SA Proposal

Isakmp Hdr, public DH-Information, Nonce-i

Isakmp Hdr, public DH-Information, Nonce-r

ISAKMP Phase 1
Oakley Main Mode

MAIN MODE

*** = Verschlüsselt!**

Isakmp Hdr*, ID-i, Hash-i

Isakmp Hdr*, ID-r, Hash-r

IKE SA
INBOUND/OUTBOUND verfügbar

IKE SA
INBOUND/OUTBOUND verfügbar

Quick Mode SA Request – Initiert wegen Crypto ACL

QUICK MODE

Isakmp Hdr*, Hash, SA Proposals, Nonce-i, [,KE] [,IDci, IDcr]

Isakmp Hdr*, Hash, selected SA, Nonce-r, [,KE] [,IDci, IDcr]

Isakmp Hdr*, Hash

IPSEC SA
INBOUND/OUTBOUND verfügbar

IPSEC SA
INBOUND/OUTBOUND verfügbar

Werner Anrath - Zentralinstitut für Angewandte Mathematik

9

L2TP over IPSEC Bausteine - PPP -

Forschungszentrum Jülich
in der Helmholtz-Gemeinschaft

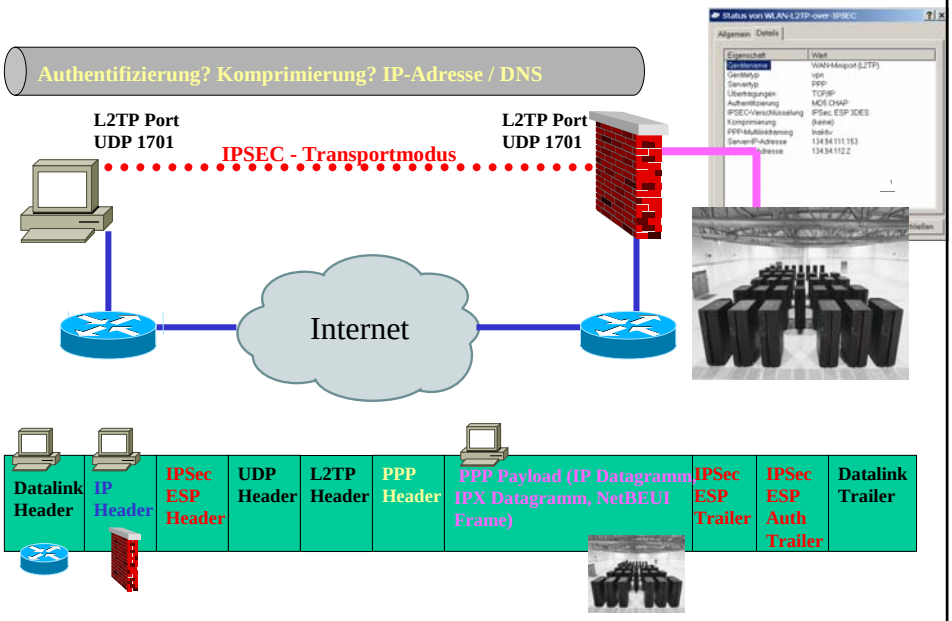
- Point-to-Point Protocol
  - Multiprotocol Data Encapsulation (IP, IPX,...)
  - PPP Link Control Protocol (LCP)
  - PPP Network Layer Negotiation (NCP – Network Control Protocol)
- LCP
  - Callback Option
  - Multilink Option
  - Authentication Protocol (PAP, CHAP, MS-CHAP .....)
  - Compression
- NCP
  - IPCP (Internet Protocol Control Protocol)
    - IP Address
    - DNS / WINS
    - IP Compression Protocol
- Vorteil: diese Mechanismen können je nach Bedarf im Remote Access VPN eingesetzt werden

Werner Anrath - Zentralinstitut für Angewandte Mathematik

10

L2TP over IPSEC Bausteine - Funktion -

Forschungszentrum Jülich
in der Helmholtz-Gemeinschaft



PIX-Firewall und L2TP over IPSEC

Forschungszentrum Jülich
in der Helmholtz-Gemeinschaft

```
crypto ipsec transform-set vpn-set-1 esp-3des esp-md5-hmac
crypto ipsec transform-set vpn-set-2 esp-3des esp-sha-hmac
.....
crypto ipsec transform-set l2tp-set1 esp-3des esp-md5-hmac
crypto ipsec transform-set l2tp-set1 mode transport
crypto ipsec transform-set l2tp-set2 esp-3des esp-sha-hmac
crypto ipsec transform-set l2tp-set2 mode transport

crypto dynamic-map vpn3000-clients 20 set transform-set vpn-set-1 vpn-set-2 vpn-set-3 vpn-set-4
crypto dynamic-map l2tp-clients 3 set transform-set l2tp-set1 l2tp-set2
.......
crypto map partner-map 20 ipsec-isakmp dynamic vpn3000-clients
crypto map partner-map 21 ipsec-isakmp dynamic l2tp-clients
crypto map partner-map client authentication fzjauth
crypto map partner-map interface outside
crypto map partner-map interface inside
crypto map partner-map interface ras
crypto map partner-map interface wlan

isakmp enable outside
isakmp enable inside
isakmp enable ras
isakmp enable wlan
......
isakmp key ********** address 0.0.0.0 netmask 0.0.0.0 no-xauth no-config-mode
```

```
vpdn group l2tp accept dialin l2tp
vpdn group l2tp ppp authentication chap
vpdn group l2tp client configuration address local vpn-pool
vpdn group l2tp client configuration dns 134.94.80.2
.....
vpdn group l2tp client configuration wins 134.94.80.84
vpdn group l2tp client authentication aaa fzjauth
vpdn group l2tp l2tp tunnel hello 30
vpdn enable outside
vpdn enable ras
vpdn enable wlan
```

Forschungszentrum Jülich
in der Helmholtz-Gemeinschaft

Windows XP und L2TP over IPSEC

Start-Button -> Systemsteuerung -> Netzwerkverbindungen
Assistent für neue Verbindungen öffnen
Auswahl ‚Verbindung mit dem Netzwerk am Arbeitsplatz herstellen' markieren
Auswahl ‚VPN-Verbindung' markieren
Name für die Verbindung eingeben, z.B. L2TP-IPSEC-FZJ
Auswahl ‚keine Verbindung automatisch wählen'
VPN-Server eintragen: wingate.zam.kfa-juelich.de

Das neue Verbindungs-ICON kann jetzt geöffnet werden, danach ‚Eigenschaften' öffnen

Registerkarte ‚Sicherheit' auswählen

‚IPSEC-Einstellungen' bearbeiten und den
‚vorinstallierten Schlüssel' (pre-shared key) eintragen

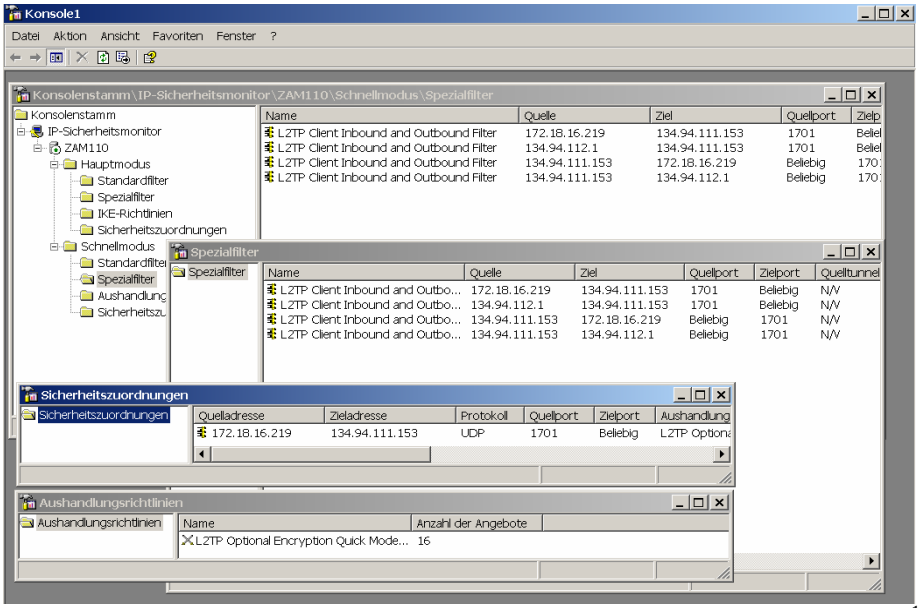
die Registerkarte ‚Sicherheit' öffnen und ‚Datenverschlüsselung ist erforderlich' deaktivieren

(Hinweis: die L2TP RC4 Verschlüsselung wird dadurch deaktiviert)

Werner Anrath - Zentralinstitut für Angewandte Mathematik 13

Forschungszentrum Jülich
in der Helmholtz-Gemeinschaft

Windows XP und L2TP over IPSEC



Werner Anrath - Zentralinstitut für Angewandte Mathematik 14

Forschungszentrum Jülich
in der Helmholtz-Gemeinschaft

Fazit: Gute Ergänzung zur Cisco VPN-Lösung ohne Deployment Overhead!

	Cisco VPN Client	MS L2TP over IPSEC
Geräteauthentifizierung	IPSEC	IPSEC
Benutzerauthentifizierung	IKE-xauth	CHAP
Kompression	optional	optional
einheitliches 'Look and Feel' – Windows Plattform	ja (9x / Me / 2000 / XP)	nein
NDIS / NDIS-WAN	ja / ja (9x / Me / 2000 / XP)	ja / ja (2000 /XP)
LINUX / MacOS	ja / ja	nein /nein
integrierte Betriebssystem-Software	nein	2000 / XP
einfache Konfiguration	ja (9x / Me / 2000 / XP)	XP

Forschungszentrum Jülich
in der Helmholtz-Gemeinschaft

Vielen Dank für Ihre Aufmerksamkeit!