Forschungszentrum Jülich
in der Helmholtz-Gemeinschaft

IPSEC VPNs
Theorie und Praxis

-Vortrag 1E06-

Werner Anrath
Forschungszentrum Jülich
Zentralinstitut für Angewandte Mathematik
(Stand 29/03/2005)

IT Symposium 2005 in Düsseldorf
05.04.2005

Forschungszentrum Jülich
in der Helmholtz-Gemeinschaft

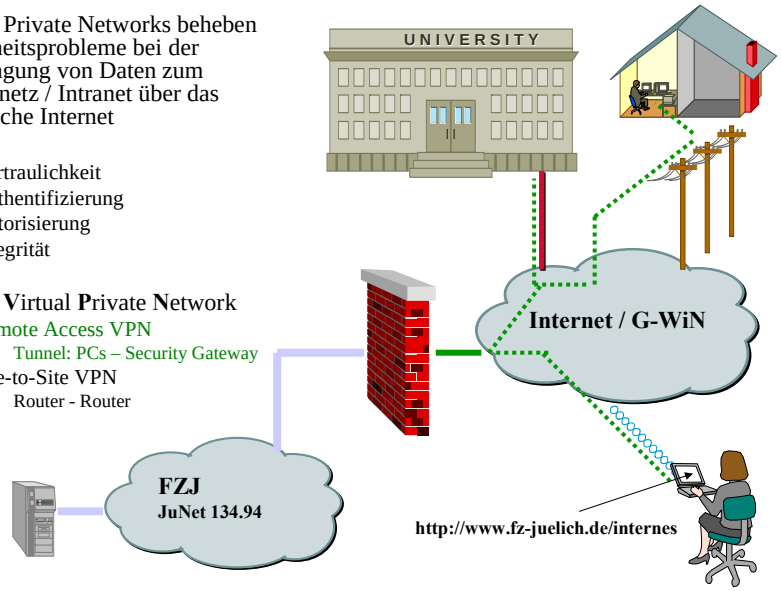
Inhalt

- Definition VPN und Überblick
- IPSEC Encapsulating Security Payload (ESP)
- Internet Key Exchange (IKE)
- Cisco VPN Komponenten (Software und Hardware)
- Erfahrungen
- IPSEC NAT/PAT Diskussion
- L2TP-over-IPSEC
- Konfiguration und Topologie im FZJ

Forschungszentrum Jülich
in der Helmholtz-Gemeinschaft

Definition – **V**irtual **P**rivate **N**etworks

- 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

Umfeld im FZJ / ZAM

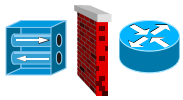
- Anforderung: Zugriff auf (interne) Netzdienste von außen
- zunehmende Anzahl Mitarbeiter mit Flatrate (DSL) / ISP-Zugang
  - Zugriff auf Dienste/Server im Intranet werden gefordert (z.B. Mail-Relay)
  - Mitarbeiter zeitlich befristet bei Kooperationspartnern, Hochschulen ..
    - LAN / WLAN
  - Tagungen
  - Forderung nach Verschlüsselung der Direkteinwahl
  - Außenstellen der Projektträger
  - Wartungszugänge (SAP, ...)
- Re-Design Firewall-Konzept (2001)
  - nur Dienste mit Verschlüsselung von extern nach intern
- Reduzierung und Vereinfachung der Direkteinwahl
- Benutzerverwaltung DB-gesteuert im ZAM-Dispatch

Werner Anrath - Zentralinstitut für Angewandte Mathematik 4

Forschungszentrum Jülich
in der Helmholtz-Gemeinschaft

VPN Protokolle - Überblick

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 Protocol
L2TP	=	Layer 2 Tunneling Protocol (over IPSEC)
IPSEC	**=**	**Internet Protocol Security**

Werner Anrath - Zentralinstitut für Angewandte Mathematik 5

Forschungszentrum Jülich
in der Helmholtz-Gemeinschaft

VPN Protokolle - PPTP

- PPTP = Point to Point Tunneling Protocol
- PPP Frames werden in IP Rahmen eingepackt und übertragen
- RFC 2637
  - Kontrollverbindung: TCP Port 1723
  - IP/GRE Tunnel zum Datenaustausch
  - MPPE = Microsoft Point to Point Encryption
  - PIX-Firewall: fixup protocol pptp 1723
    - Zugriff für Gäste nach außen / Remote VPN-Server initiiert GRE-Tunnel

Data-link Header	IP	TCP	PPTP Control Message	Data-link Trailer

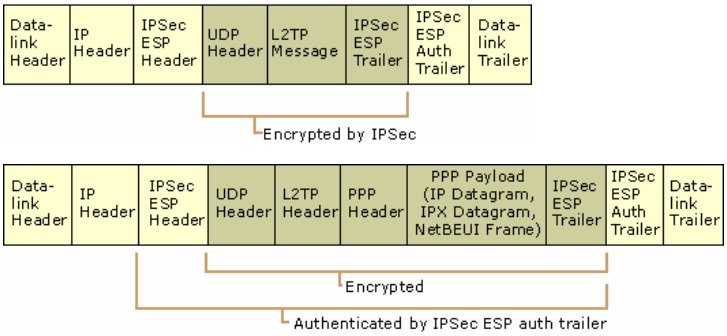
Data-link Header	IP Header	GRE Header	PPP Header	Encrypted PPP Payload (IP Datagram, IPX Datagram, NetBEUI Frame)	Data-link Trailer

Werner Anrath - Zentralinstitut für Angewandte Mathematik 6

Forschungszentrum Jülich
in der Helmholtz-Gemeinschaft

VPN Protokolle - L2TP

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



Werner Anrath - Zentralinstitut für Angewandte Mathematik 7

Forschungszentrum Jülich
in der Helmholtz-Gemeinschaft

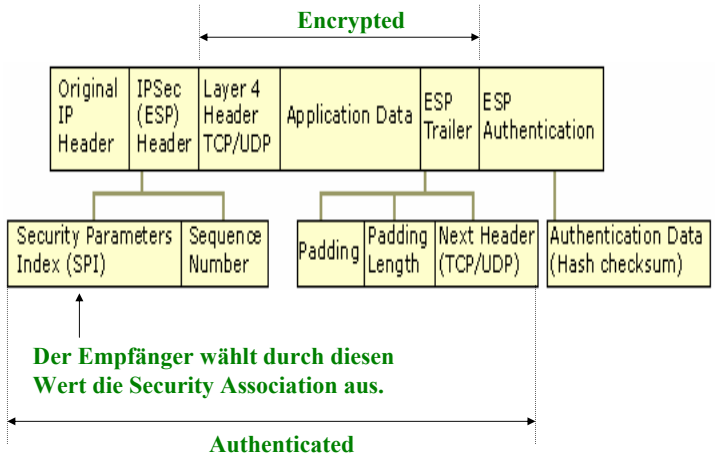
VPN Protokolle - IPSEC Überblick

- **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
    - Cat 6K VPN Service Module
- 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

Werner Anrath - Zentralinstitut für Angewandte Mathematik 8

Forschungszentrum Jülich
in der Helmholtz-Gemeinschaft

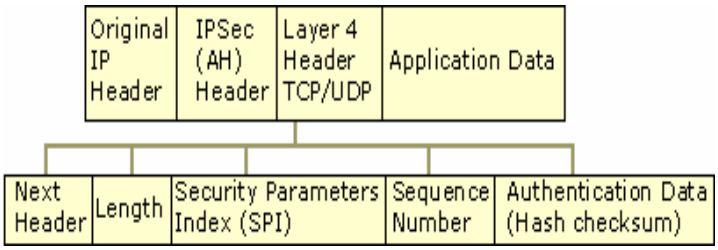
IPSEC ESP - Header Aufbau



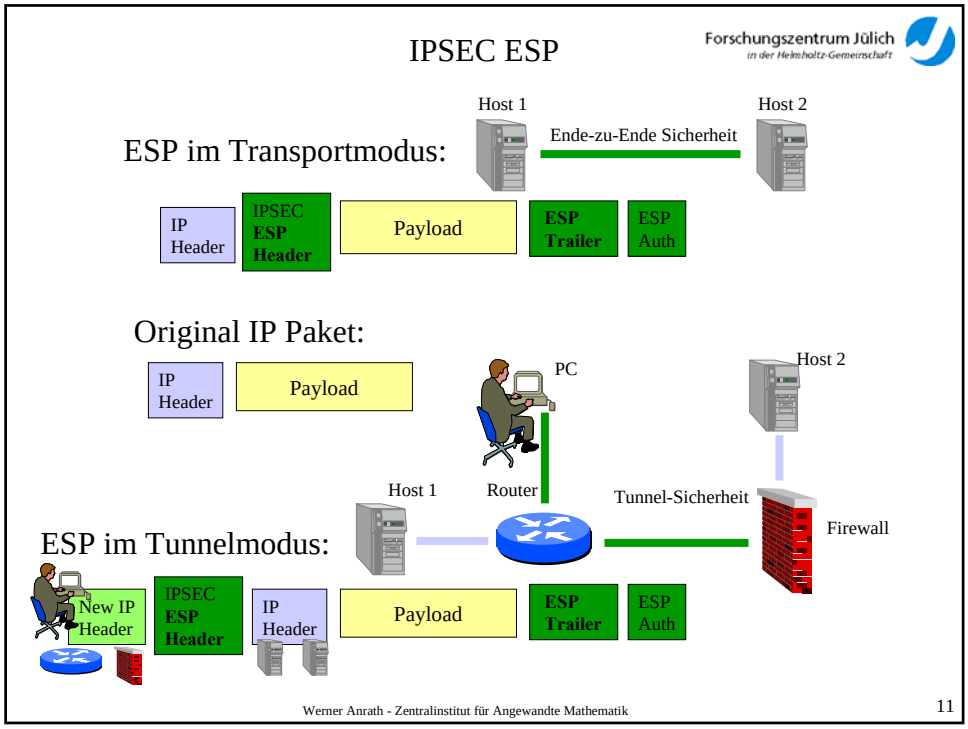
Werner Anrath - Zentralinstitut für Angewandte Mathematik 9

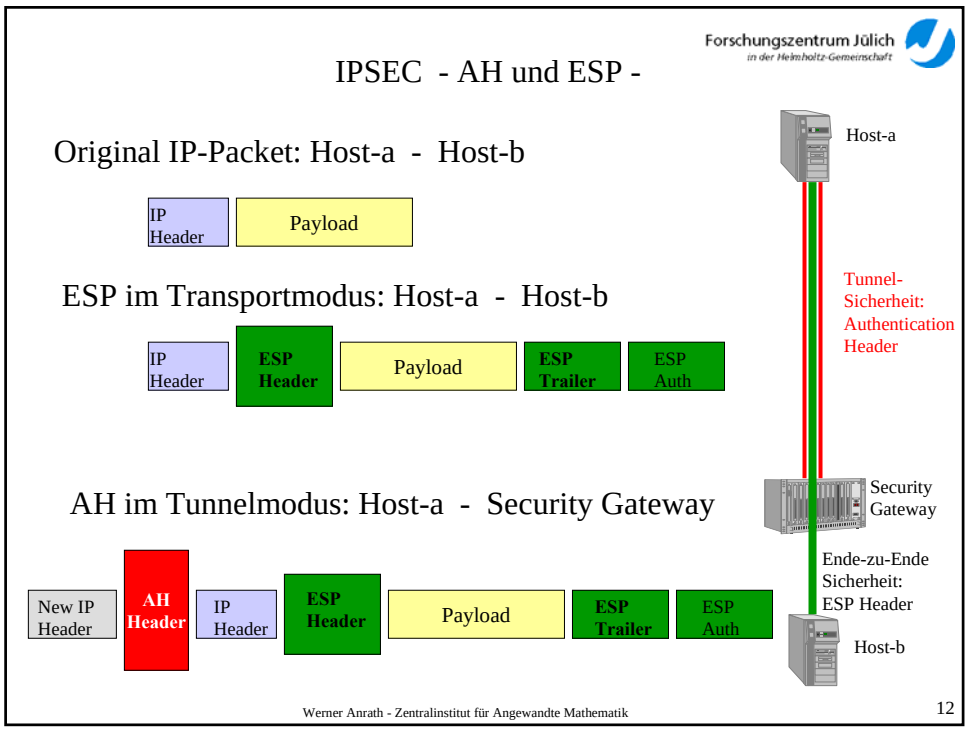
Forschungszentrum Jülich
in der Helmholtz-Gemeinschaft

IPSEC AH - Header Aufbau



Werner Anrath - Zentralinstitut für Angewandte Mathematik 10


IPSEC ESP
Forschungszentrum Jülich
in der Helmholtz-Gemeinschaft
ESP im Transportmodus:
Host 1
Host 2
Ende-zu-Ende Sicherheit
IP Header
IPSEC ESP Header
Payload
ESP Trailer
ESP Auth
Original IP Paket:
IP Header
Payload
PC
Host 2
Host 1
Router
Tunnel-Sicherheit
Firewall
ESP im Tunnelmodus:
New IP Header
IPSEC ESP Header
IP Header
Payload
ESP Trailer
ESP Auth
Werner Anrath - Zentralinstitut für Angewandte Mathematik
11


IPSEC - AH und ESP -
Forschungszentrum Jülich
in der Helmholtz-Gemeinschaft
Original IP-Packet: Host-a - Host-b
Host-a
IP Header
Payload
ESP im Transportmodus: Host-a - Host-b
Tunnel-Sicherheit: Authentication Header
IP Header
ESP Header
Payload
ESP Trailer
ESP Auth
AH im Tunnelmodus: Host-a - Security Gateway
Security Gateway
Ende-zu-Ende Sicherheit: ESP Header
New IP Header
AH Header
IP Header
ESP Header
Payload
ESP Trailer
ESP Auth
Host-b
Werner Anrath - Zentralinstitut für Angewandte Mathematik
12

Forschungszentrum Jülich
in der Helmholtz-Gemeinschaft

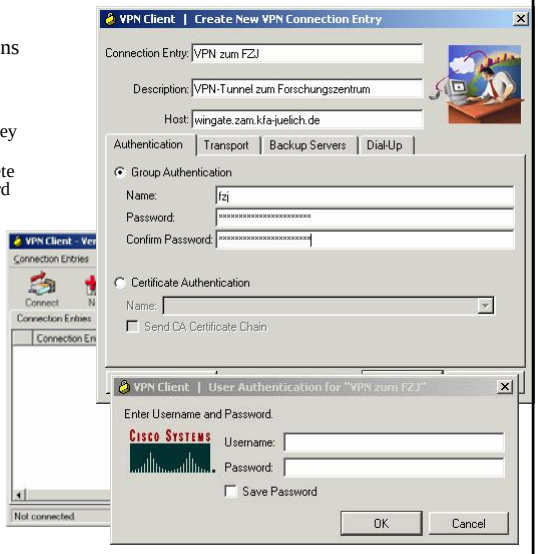
VPN-Zugang ins Forschungszentrum Jülich

- Remote Access VPN: Cisco VPN Client Software
  - Support weit verbreiteter Betriebssysteme wie Windows und LINUX (x86)
  - einfache Installation / komfortable Bedienung der Benutzeroberfläche
  - insgesamt gute Softwarequalität
  - Alternative: L2TP-over-IPSEC
- Remote Access VPN Security Gateways:
  - Firewall Cisco PIX 535
    - bis zu 2000 VPN-Sessions / Tunnelendpunkt für WLAN
    - 3DES Hardware-Support, 95 MBit/s
    - Logging (Syslog) und Accounting (Radius)
    - Split Tunneling ist zwingend erforderlich
    - *small* Site-to-Site IPSEC VPNs
  - VPN Access Concentrators 3030
    - 3DES Hardware-Support, 50 Mbit/s
    - Reduzierung der Wechselwirkung bei Software-Updates und Konfigurationsänderungen
    - Funktionalitäten wie NAT-Unterstützung, Komprimierung, Policy Push für Personal Firewalls sind verfügbar

Forschungszentrum Jülich
in der Helmholtz-Gemeinschaft

IPSEC und IKE

- IKE Aufgabe: automatische Aushandlung von Security Associations (SA)
  - Ebene 7 erbringt Dienstleistung für Ebene 3
  - RFC 2409, RFC 2408 ISAKMP/Oakley Payload
  - Detail: 6 Pakete Main Mode + 3 Pakete Quick Mode (optional Perfect Forward Secrecy)
- IKE-Varianten
  - kein IKE, d.h. Manual Keying
  - ISAKMP/Oakley Payload
  - pre-shared key
  - Zertifikate / RSA
- automatische Generierung des Schlüsselmaterials
  - wichtig für Skalierung
- Kryptografie
  - DES, 3-DES, AES
  - MD5, SHA1
  - Diffie-Hellman Key Exchange



Forschungszentrum Jülich
in der Helmholtz-Gemeinschaft

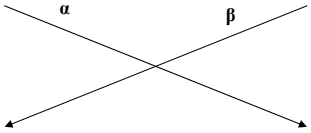
IPSEC und IKE - Diffie Hellman

$k \rightarrow g^k \bmod p \quad (1 \leq k \leq p-1)$

Die Exponenten a, b sind geheim; p (Primzahl), g (Basis) sind öffentlich.

A
wählt zufällig eine Zahl a.
Berechnet
$\alpha := g^a \bmod p$

B
wählt zufällig eine Zahl b.
Berechnet
$\beta := g^b \bmod p$



Berechnet
$\beta^a \bmod p$

Berechnet
$\alpha^b \bmod p$

Einwegeigenschaft und Kommutativität der Exponenten.

$\beta^a \bmod p = (g^b)^a \bmod p = g^{(ab)} \bmod p = (g^a)^b \bmod p = \alpha^b \bmod p$

Werner Anrath - Zentralinstitut für Angewandte Mathematik 15

Forschungszentrum Jülich
in der Helmholtz-Gemeinschaft

IPSEC und IKE - Main Mode / Quick Mode

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

Initiator  Responder 

ISAKMP Phase 1
Oakley Main Mode

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 Hdr*, ID-i, Hash-i →
← Isakmp Hdr*, ID-r, Hash-r

* = Verschlüsselt!

IKE SA
INBOUND/OUTBOUND verfügbar

IKE SA
INBOUND/OUTBOUND verfügbar

Quick Mode SA Request – Initiert wegen Crypto ACL

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 16

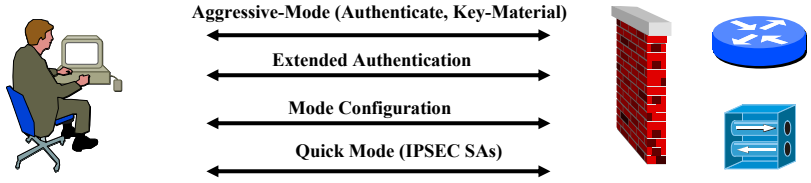
Forschungszentrum Jülich
in der Helmholtz-Gemeinschaft

IPSEC und IKE – Cisco VPN Client

- IKE Cisco Erweiterungen
  - MAIN Mode nur in Verbindung mit Zertifikaten
  - Aggressive Mode bei pre-shared Key (plus Xauth)
  - Extended Authentication (Xauth): Username / Password
  - Mode Configuration: IP-Adresse, DNS, WINS, Tunnel-Policy
  - Vorteil:
    - sehr gute Skalierung in Remote-Access-Szenarien
    - Split Tunneling: VPN und INTERNET Upstream gleichzeitig

Cisco VPN Client

PIX, Cisco IOS,
VPN Concentrator

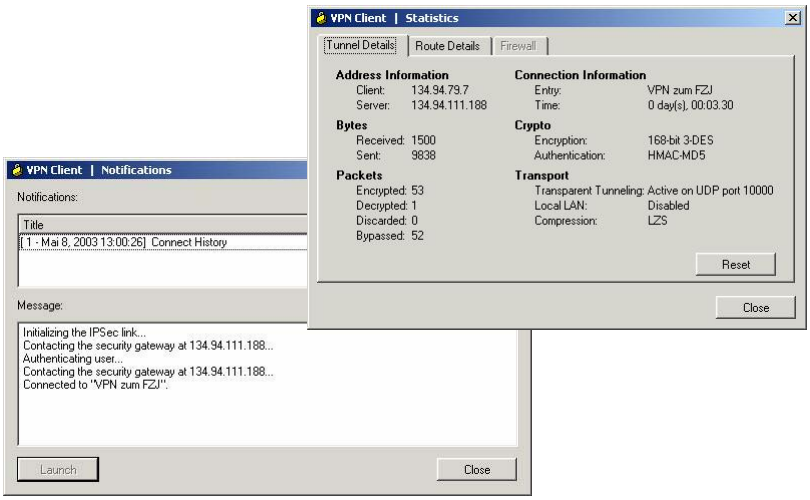


Werner Anrath - Zentralinstitut für Angewandte Mathematik 17

Forschungszentrum Jülich
in der Helmholtz-Gemeinschaft

IPSEC und IKE - **IKE SA und IPSEC SAs**

Cisco VPN Client für Windows



Werner Anrath - Zentralinstitut für Angewandte Mathematik 18

IPSEC und IKE Aggressive Mode - Client Debug

Forschungszentrum Jülich
in der Helmholtz-Gemeinschaft

```
3     13:42:52.180  07/06/02  Sev=Info/4          CM/0x63100026
Attempt connection with server "nasgate.zam.kfa-juelich.de"
4     13:42:52.520  07/06/02  Sev=Info/6          IKE/0x6300003B
Attempting to establish a connection with 134.94.111.169.
5     13:42:52.580  07/06/02  Sev=Info/4          IKE/0x63000013

SENDING >>> ISAKMP OAK AG (SA, KE, NON, ID, VID, VID, VID) to 134.94.111.169
.......
RECEIVING <<< ISAKMP OAK AG (SA, VID, VID, VID, KE, ID, NON, HASH) from
      134.94.111.169

9     13:42:52.981  07/06/02  Sev=Info/5          IKE/0x63000059
Vendor ID payload = 12F5F28C457168A9702D9FE274CC0100
10    13:42:52.981  07/06/02  Sev=Info/5          IKE/0x63000001
Peer is a Cisco-Unity compliant peer
11    13:42:52.981  07/06/02  Sev=Info/5          IKE/0x63000059
Vendor ID payload = AFCAD71368A1F1C96B8696FC77570100
12    13:42:52.981  07/06/02  Sev=Info/5          IKE/0x63000001
Peer supports DPD
13    13:42:52.981  07/06/02  Sev=Info/5          IKE/0x63000059
Vendor ID payload = 1DE2A5CCC060E075442A2DEB6EF73592

14    13:42:53.001  07/06/02  Sev=Info/4          IKE/0x63000013

SENDING >>> ISAKMP OAK AG *(HASH, NOTIFY:STATUS_INITIAL_CONTACT) to
      134.94.111.169
```

Public Diffie-Hellman Information

Group: fzj

fwoutside.zam.kfa-juelich.de

IPSEC und IKE Aggressive Mode - Sniffer Log

Forschungszentrum Jülich
in der Helmholtz-Gemeinschaft

```
⊞ User Datagram Protocol
⊟ Internet Security Association and Key Management Protocol
    Initiator cookie
    Responder cookie
    Next payload: Security Association (1)
    Version: 1.0
    Exchange type: Aggressive (4)
  ⊞ Flags
    Message ID: 0x00000000
    Length: 555
  ⊟ Security Association payload
      Next payload: Key Exchange (4)
      Length: 308
      Domain of interpretation: IPSEC (1)
      Situation: IDENTITY (1)
    ⊟ Proposal payload
        Next payload: NONE (0)
        Length: 296
        Proposal number: 1
        Protocol ID: ISAKMP (1)
        SPI size: 0
        Number of transforms: 8
      ⊞ Transform payload
      ⊟ Transform payload
          Next payload: Transform (3)
          Length: 36
          Transform number: 2
          Transform ID: KEY_IKE (1)
          Encryption-Algorithm (1): 3DES-CBC (5)
          Hash-Algorithm (2): MD5 (1)
          Group-Description (4): Group-Value (2)
          Authentication-Method (3): XAUTHInitPreShared (65001)
          Life-Type (11): Seconds (1)
          Life-Duration (12): Duration-Value (2147483)
      ⊞ Transform payload
```

IPSEC und IKE Quick Mode - VPN Client Debug

Forschungszentrum Jülich
in der Helmholtz-Gemeinschaft

61 13:48:08.544 07/06/02 Sev=Info/5 IKE/0x63000055
Received a key request from Driver for IP address 134.94.80.2, GW IP = 134.94.111.169

62 13:48:08.544 07/06/02 Sev=Info/4 IKE/0x63000013
SENDING >>> ISAKMP OAK QM *(HASH, SA, NON, ID, ID) to 134.94.111.169

63 13:48:09.015 07/06/02 Sev=Info/5 IKE/0x6300002F
Received ISAKMP packet: peer = 134.94.111.169

64 13:48:09.015 07/06/02 Sev=Info/4 IKE/0x63000014
RECEIVING <<< ISAKMP OAK QM *(HASH, SA, NON, ID, ID, NOTIFY:STATUS_RESP_LIFETIME) from 134.94.111.169

65 13:48:09.015 07/06/02 Sev=Info/5 IKE/0x63000044
RESPONDER-LIFETIME notify has value of 28800 seconds

66 13:48:09.015 07/06/02 Sev=Info/5 IKE/0x63000045
RESPONDER-LIFETIME notify has value of 4608000 kb

67 13:48:09.015 07/06/02 Sev=Info/4 IKE/0x63000013
SENDING >>> ISAKMP OAK QM *(HASH) to 134.94.111.169

68 13:48:09.015 07/06/02 Sev=Info/5 IKE/0x63000058
Loading IPsec SA (Message ID = 0x42EB4F4A OUTBOUND SPI = 0x1D4D8FC8 INBOUND SPI = 0x28BF4C5F)

69 13:48:09.015 07/06/02 Sev=Info/5 IKE/0x63000025
Loaded OUTBOUND ESP SPI: 0x1D4D8FC8

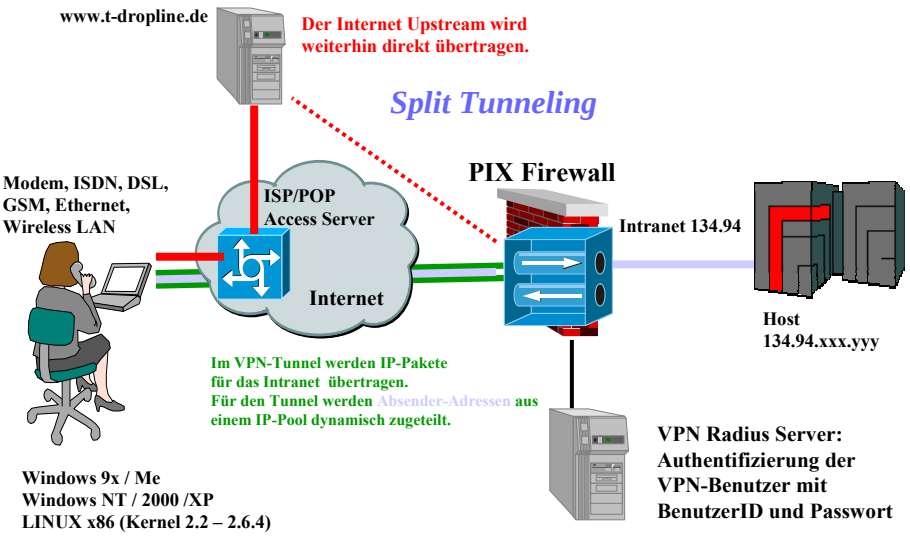
70 13:48:09.015 07/06/02 Sev=Info/5 IKE/0x63000026
Loaded INBOUND ESP SPI: 0x28BF4C5F

71 13:48:09.015 07/06/02 Sev=Info/4 CM/0x63100022
Additional Phase 2 SA established.

Werner Anrath - Zentralinstitut für Angewandte Mathematik 21

IPSEC und IKE - Cisco VPN Client

Forschungszentrum Jülich
in der Helmholtz-Gemeinschaft



Werner Anrath - Zentralinstitut für Angewandte Mathematik 22

VPN Client für LINUX - *kurz vorgestellt*

Forschungszentrum Jülich
in der Helmholtz-Gemeinschaft

```
zam036:~ # vpnclient  connect  fzj

Cisco Systems VPN Client Version 3.0.8
Copyright (C) 1998-2001 Cisco Systems, Inc. All Rights Reserved.
Client Type(s): Linux
Running on: Linux 2.4.4-4GB #1 Wed May 16 00:37:55 GMT 2001 i686

Enter a group password:
Initializing the IPSec link.
Contacting the security gateway at 134.94.111.185
Authenticating user.
User Authentication for fzj...

The server has requested the following information to complete the user authentication:

Username [w.anrath]:
Password []:
Contacting the security gateway at 134.94.111.185
Negotiating security policies.
Securing communication channel.
Your link is secure.

IPSec tunnel information.
Client address: 134.94.112.1
Server address: 134.94.111.185
Encryption: 168-bit 3-DES
Authentication: HMAC-MD5
IP Compression: None
NAT passthrough is inactive.
```

Linux Kernel 2.2 – 2.6.8 (x86)

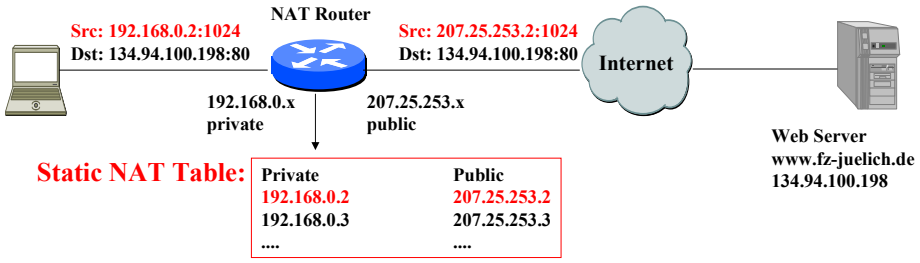
```
zam036:~ # vpnclient  disconnect

Cisco Systems VPN Client Version 3.0.8
Copyright (C) 1998-2001 Cisco Systems, Inc. All Rights Reserved.
Client Type(s): Linux
Running on: Linux 2.4.4-4GB #1 Wed May 16 00:37:55 GMT 2001 i686

Disconnecting the IPSEC link.
zam036:~ # Your IPSec link has been disconnected.
```

```
zam036:~ # vpnclient  stat

Cisco Systems VPN Client Version 3.0.8
Copyright (C) 1998-2001 Cisco Systems, Inc. All Rights Reserved.
Client Type(s): Linux
Running on: Linux 2.4.4-4GB #1 Wed May 16 00:37:55 GMT 2001 i686

IPSec tunnel information.
Client address: 134.94.112.1
Server address: 134.94.111.185
Encryption: 168-bit 3-DES
Authentication: HMAC-MD5
IP Compression: None
NAT passthrough is inactive.

VPN traffic summary.
Time connected: 0 day(s), 00:31.04
Bytes out: 307703
Bytes in: 422758
Packets encrypted: 3689
Packets decrypted: 2289
Packets bypassed: 60
Packets discarded: 1

Configured routes
Secured  Network Destination    Netmask          Bytes
  *      134.94.111.185        255.255.255.255      0
  *      134.94.0.0            255.255.0.0       526215
```

Werner Anrath - Zentralinstitut für Angewandte Mathematik 23

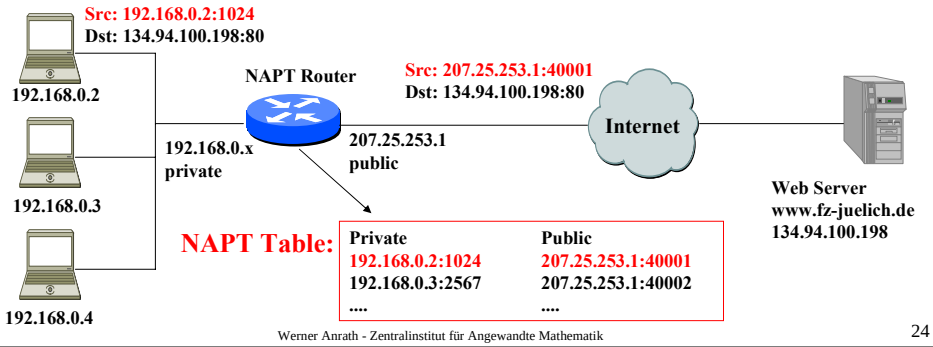
IPSEC VPNs - NAT / PAT Problematik

Forschungszentrum Jülich
in der Helmholtz-Gemeinschaft



Static NAT Table:

Private	Public
192.168.0.2	207.25.253.2
192.168.0.3	207.25.253.3
....	....



NAPT Table:

Private	Public
192.168.0.2:1024	207.25.253.1:40001
192.168.0.3:2567	207.25.253.1:40002
....	....

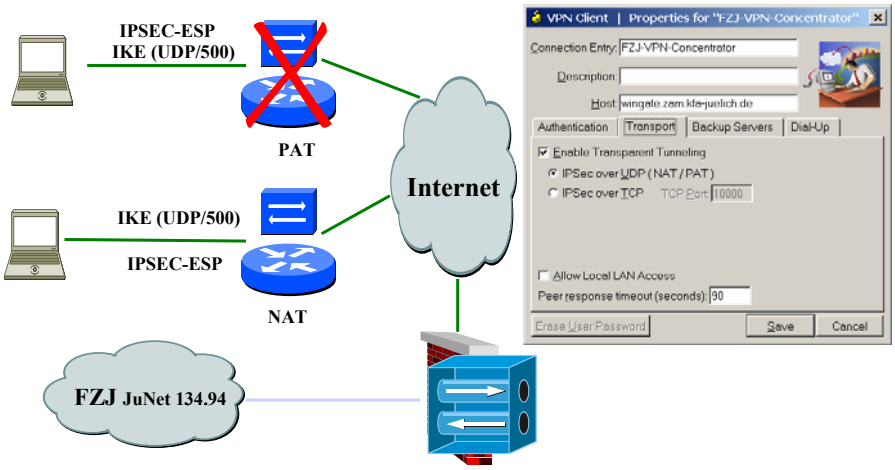
Werner Anrath - Zentralinstitut für Angewandte Mathematik 24

IPSEC VPNs - NAT / PAT Problematik

Forschungszentrum Jülich
in der Helmholtz-Gemeinschaft

Lösung:

New IP Header	UDP /TCP Header	**ESP Header**	IP Header	Payload	ESP Trailer und Auth



Erfahrungen beim VPN Zugang / Performance

Forschungszentrum Jülich
in der Helmholtz-Gemeinschaft

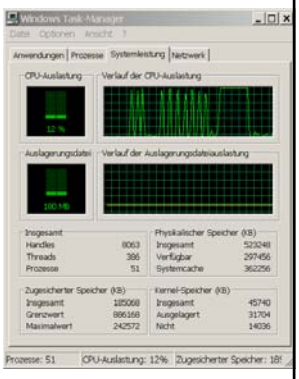
PC Pentium III 850 MHz 3COM → PIX 535 3DES MD5

File Transfer –binary-	Cisco VPN Client aktiviert	Cisco VPN Client deaktiviert
Mini PCI Ethernet 10/100 → PIX 535	21 Mbps	74 Mbps
FE574BT 10/100 PCMCIA LAN Card → PIX 535	7.5 Mbps	12.1 Mbps (16 Bit LAN Card)
CISCO Aironet 340 WLAN	4.6 Mbps	4.7 Mbps

PC Pentium IV 2.4 GHz 3DES MD5

File Transfer –binary-	Cisco VPN Client aktiviert	Cisco VPN Client deaktiviert
Intel Pro/100 → PIX 535	49 Mbps	91 Mbps
Intel Pro/100 → VPN3030	47 Mbps (3DES MD5) 16 Mbps (AES MD5)	91 Mbps
Intel Pro/100 – IOS 3745 AIM/HPII	45 Mbps (3DES MD5) 53 Mbps (AES MD5) 65 Mbps (Null MD5)	91 Mbps

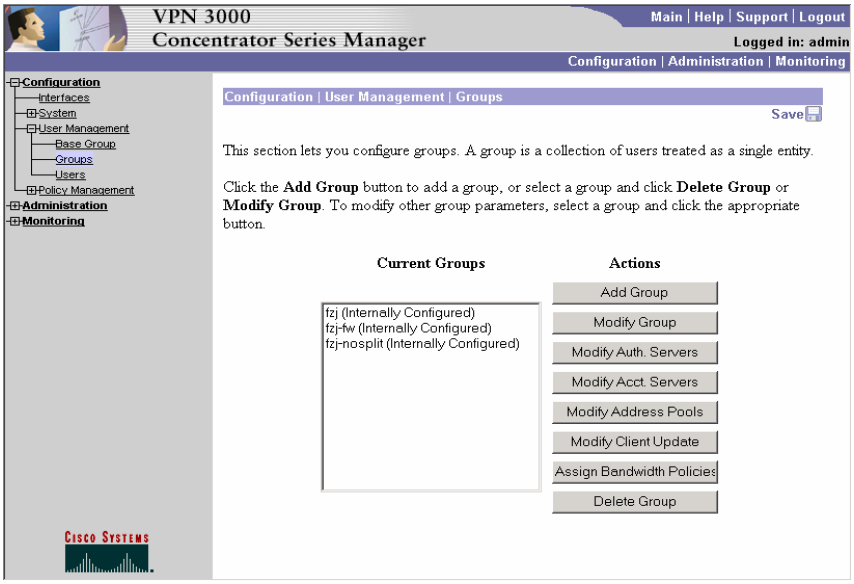
Komprimierung vor dem Verschlüsseln ist bei ISDN- und Modemverbindungen zu empfehlen!



In Zukunft: AES favorisieren! (Effizienter in Softwareimplementierungen)

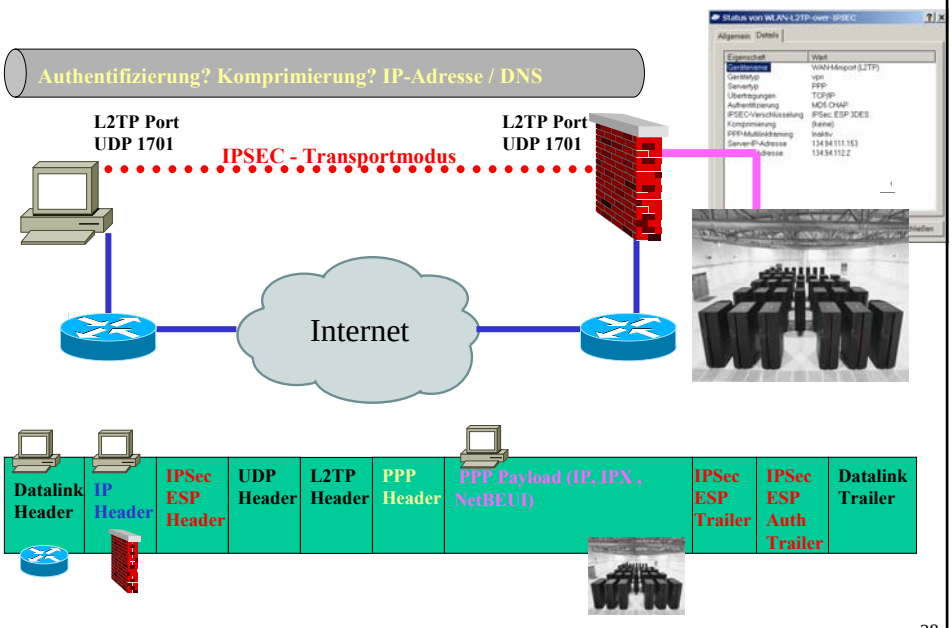
VPN 3030 Concentrator

Forschungszentrum Jülich
in der Helmholtz-Gemeinschaft



L2TP over IPSEC Bausteine - Funktion -

Forschungszentrum Jülich
in der Helmholtz-Gemeinschaft



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)

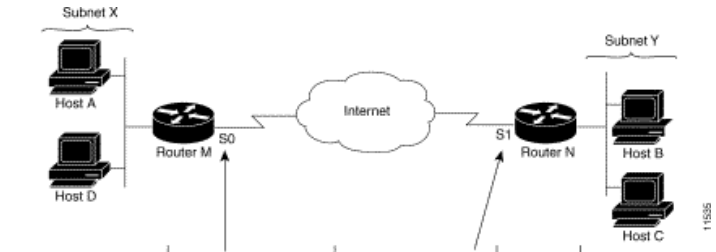
Fazit: Gute Ergänzung zur Cisco VPN-Lösung ohne Deployment Overhead!

Forschungszentrum Jülich
in der Helmholtz-Gemeinschaft

	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

Site-to-Site VPN - Crypto Access Lists -

Forschungszentrum Jülich
in der Helmholtz-Gemeinschaft



Mirror image access lists at Router M S0 and Router N S1

	IPSec access list at S0:	IPSec access list at S1:	1st packet	Result
Case 1	permits Host A → Host B	permits Host B → Host A	A → B or B → A	SAs established for traffic A↔B (good)
Case 2	permits Subnet X → Subnet Y	permits Subnet Y → Subnet X	A → B or B → A or A → C or C → D and so on	SAs established for traffic X↔Y (good)
Case 3	permits Host A → Host B	permits Subnet Y → Subnet X	A → B	SAs established for traffic A↔B (good)
Case 4			B → A	SAs cannot be established and packets from Host B to Host A are dropped (bad)

Site-to-Site VPN und PIX-Firewall - Konfiguration

Forschungszentrum Jülich
in der Helmholtz-Gemeinschaft

isakmp key ****** address 134.94.117.250 netmask 255.255.255.255 no-xauth no-mode-config**
crypto map partner-map 19 set peer 134.94.117.250
crypto map partner-map 19 set transform-set vpn-set-1 vpn-set-2
vpn-set-3 vpn-set-4
crypto map partner-map 19 match address acl-peer2peer
crypto map partner-map 19 ipsec-isakmp
access-list acl-peer2peer permit ip 134.94.168.0 255.255.248.0 host 134.94.117.250 ; Tunnel-Filter
; Tunnel-Filter symmetrisch zur Definition auf dem PEER

Windows 2000 Peer:

- **Start -> Einstellungen -> Systemsteurung -> Verwaltung**
- **-> Lokale Sicherheitsrichtlinie**
- **-> IP-Sicherheitsrichtlinien auf lokalem Computer-> rechte Maustaste -> lokale Sicherheitsrichtlinie erstellen**
- **(Wizard) -> Weiter -> Namen eintragen und Beschreibung (optional) -> Weiter -> Standardantwortregel aktivieren -> Weiter -> Schlüssel angeben -> weiter -> fertig stellen**

Hinzufügen von Filterregeln:

- **Im rechten Fenster „Doppelklick“ auf die Sicherheitsrichtlinie**
- **Hinzufügen -> Weiter -> PIX IP-Adresse als Tunnelendpunkt eintragen -> Weiter -> LAN-Verbindung wählen -> weiter -> Schlüssel eintragen -> weiter -> Name der Filterregeln eintragen („Zum inside Netz“) und Hinzufügen -> weiter -> Quelladresse „Eigene IP-Adresse“ -> weiter -> Ziel-Adresse „spezielles IP-Subnetz“ Adresse und richtige Subnetzmaske eintragen -> weiter -> Protokolltyp beliebig wählen und fertig stellen.**

Forschungszentrum Jülich
in der Helmholtz-Gemeinschaft

.... Fortsetzung folgt:

GRE-over-IPSEC

Werner Anrath
Forschungszentrum Jülich
Zentralinstitut für Angewandte Mathematik

IT Symposium 2005 in Düsseldorf
07.04.2005

Forschungszentrum Jülich
in der Helmholtz-Gemeinschaft

Vielen Dank für Ihre Aufmerksamkeit!