Forschungszentrum Jülich
in der Helmholtz-Gemeinschaft

GRE-over-IPSEC

-Vortrag 3E02-

Werner Anrath
Forschungszentrum Jülich
Zentralinstitut für Angewandte Mathematik
(Stand: 29.03.2005)

IT Symposium 2005 in Düsseldorf
07.04.2005

Forschungszentrum Jülich
in der Helmholtz-Gemeinschaft

Inhalt

Forschungszentrum Jülich
in der Helmholtz-Gemeinschaft

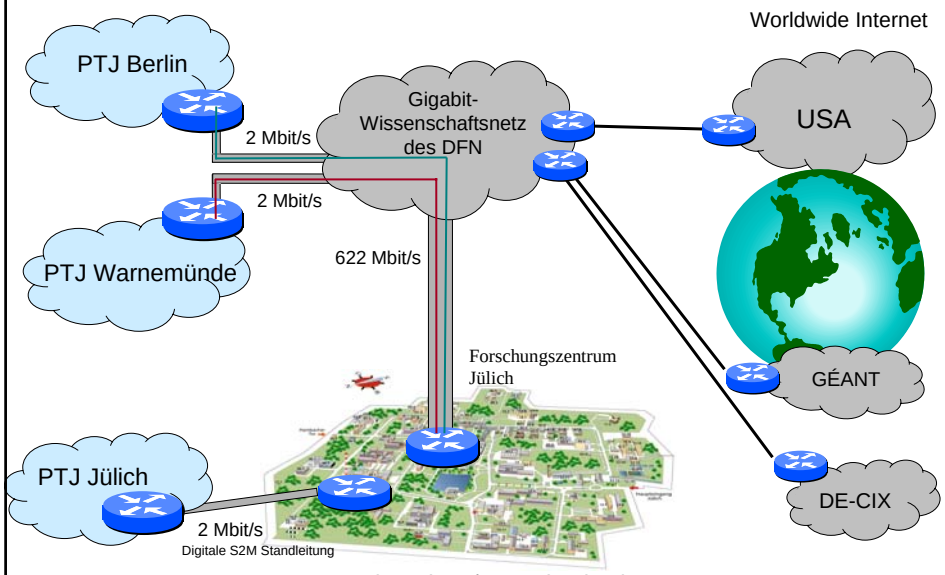
Umfeld im FZJ / ZAM

- GRE-Tunnel zu den Außenstellen der Projektträgerschaften
  - Berlin
  - Rostock
- Realisierung dieser GRE-Tunnel im Jahr 1999/2000
- neue Anforderung:
  - Benutzer: schnellere Kommunikation
  - Rechenzentrum: Sicherheitsaspekte

Werner Anrath - Zentralinstitut für Angewandte Mathematik 3

Forschungszentrum Jülich
in der Helmholtz-Gemeinschaft

Anschluss der PTJ Außenstellen
- bis 10/2004 -



Werner Anrath - Zentralinstitut für Angewandte Mathematik 4

Forschungszentrum Jülich
in der Helmholtz-Gemeinschaft

Überblick und Vergleich
- Alte und neue Anbindung -

- Anbindung 2000-2004
  - Cisco 3620
  - GRE-Tunnel
  - E1 2Mbps G703
  - Provider: DFN G-WiN
  - 10BaseT LAN
  - Backup:
    - Cisco 2500
    - ISDN BRI, 128 Kbps
    - Chap-Authentication
    - Aktivierung manuell

- Oktober 2004
  - Cisco 3745 VPN Router
  - GRE over IPSEC
  - E3 34 Mbps G751
  - Provider: DFN G-WiN
  - 100BaseTx LAN
  - Backup:
    - E1 G703 Module im 3745
    - 2 Mbps / DFN G-WiN
    - GRE over IPSEC
    - Automatische Aktivierung
  - Out of band / Desaster:
    - Cisco 3620 ISDN BRI
    - E1 2Mbps G703, manuell
      - Kabel schwenken

Werner Anrath - Zentralinstitut für Angewandte Mathematik 5

Forschungszentrum Jülich
in der Helmholtz-Gemeinschaft

Hardwareauswahl – Cisco VPN Router
- Herstellerangaben zur Performance –

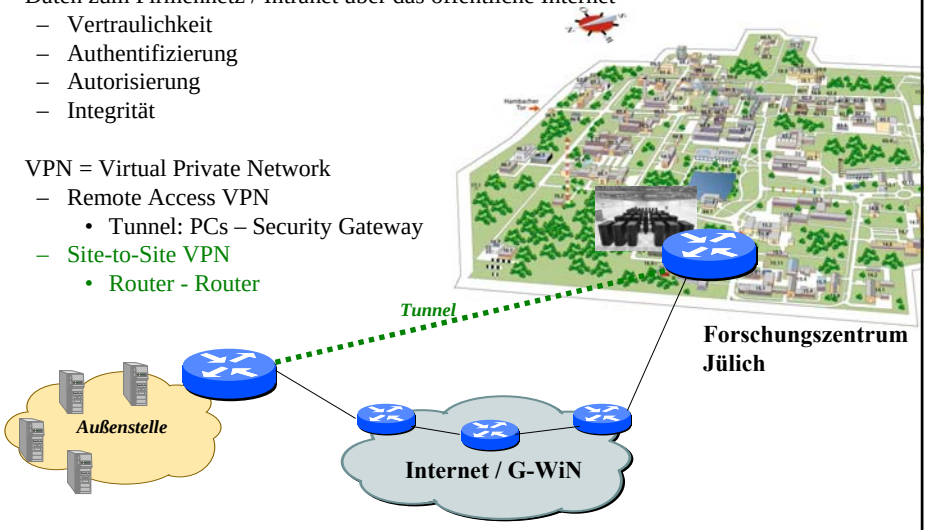
3745 AIM-VPN/HPII	180 Mbps
7206 VXR G1 VAM2 / Dual VAM2	260 Mbps / 460 Mbps
7301 VAM2 VAM2+	 370 Mbps 390 Mbps
Cat 6500 single VPNSM	1.9 Gbps
PIX 535 VAC+	425 Mbps
VPN3030 VPN3060	50 Mbps 100 Mbps

Werner Anrath - Zentralinstitut für Angewandte Mathematik 6

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 = Virtual Private Network
  - Remote Access VPN
    - Tunnel: PCs – Security Gateway
  - Site-to-Site VPN
    - Router - Router



Werner Anrath - Zentralinstitut für Angewandte Mathematik 7

Forschungszentrum Jülich
in der Helmholtz-Gemeinschaft

Generic Routing Encapsulation

- GRE = Generic Routing Encapsulation
  - RFC Standard
    - 1701 / 1702 (GRE over IPv4) / 2784
- Einsatzmöglichkeiten:
  - Aufbau von *unsecured VPN*
    - unabhängig vom Routing der Service Provider
    - vom Backbone/WAN nicht unterstützte Protokolle können über diese Tunnel transportiert werden
- Komponenten:
  - Passenger Protocol: Das Protokoll, das über den Tunnel verschickt werden soll (**IP**, IPX,...)
  - Carrier Protocol: Das „Verpackungs“-Protokoll (**GRE**)
  - Transport Protocol: Das Protokoll, das das „verpackte“ Protokoll transportiert: nur IP

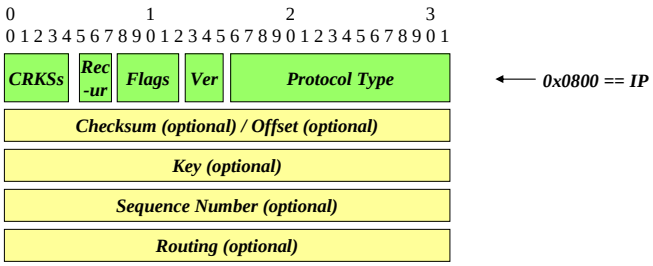
Werner Anrath - Zentralinstitut für Angewandte Mathematik 8

Forschungszentrum Jülich
in der Helmholtz-Gemeinschaft

Generic Routing Encapsulation
- GRE Header -

- IP Protocol Type: 47
- Tunnel Overhead: 24 Byte
  - 4 Byte GRE Header
  - 20 Byte IP Header

GRE HEADER



Forschungszentrum Jülich
in der Helmholtz-Gemeinschaft

Generic Router Encapsulation
- Tunnel Keepalive -

- integriert in Cisco IOS Release 12.2(14)S
- Vorteil: die Interface spezifischen IP Routes werden inaktiv! (Das Line Protocol (hier IP) kann automatisch bei Störungen/Ausbleiben der Keepalive-Nachrichten deaktiviert werden.)

```
Router(config)# interface tunnel 0
Router(config-if)# keepalive 3 5
```

← *Anzahl Retries / Timeout*

ip route 134.94.113.0 255.255.255.0 Tunnel0

ip route 134.94.113.0 255.255.255.0 Tunnel1 240

→ *Umschaltzeit < 20 Sekunden*

Forschungszentrum Jülich
in der Helmholtz-Gemeinschaft

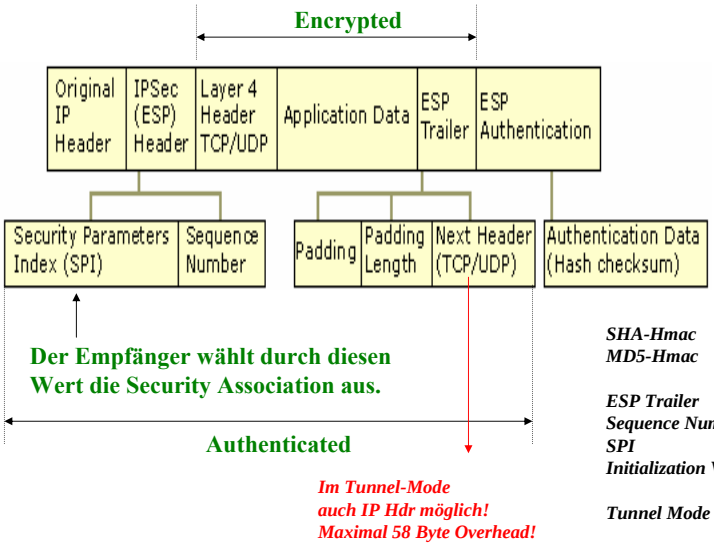
IPSEC Überblick

- **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 Modul
- 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 11

Forschungszentrum Jülich
in der Helmholtz-Gemeinschaft

IPSEC ESP - Header Aufbau

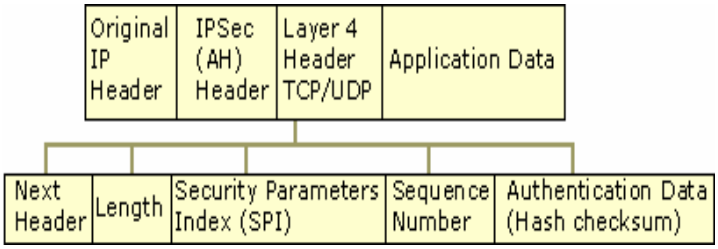


SHA-Hmac	*20 Byte*
MD5-Hmac	*16 Byte*
ESP Trailer	*2 Byte*
Sequence Number	*4 Byte*
SPI	*4 Byte*
Initialization Vector	*8 Byte*
Tunnel Mode IP Hdr	*20 Byte*

Werner Anrath - Zentralinstitut für Angewandte Mathematik 12

Forschungszentrum Jülich
in der Helmholtz-Gemeinschaft

IPSEC AH - Header Aufbau

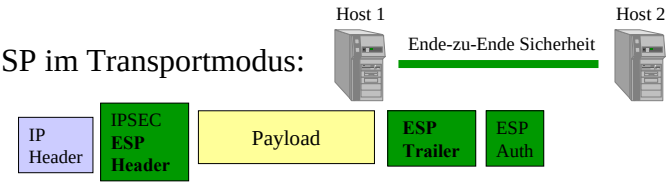


Werner Anrath - Zentralinstitut für Angewandte Mathematik 13

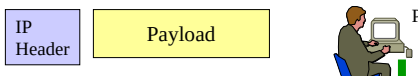
Forschungszentrum Jülich
in der Helmholtz-Gemeinschaft

IPSEC ESP

ESP im Transportmodus:



Original IP Paket:



ESP im Tunnelmodus:

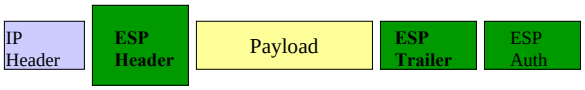
Werner Anrath - Zentralinstitut für Angewandte Mathematik 14

Forschungszentrum Jülich
in der Helmholtz-Gemeinschaft

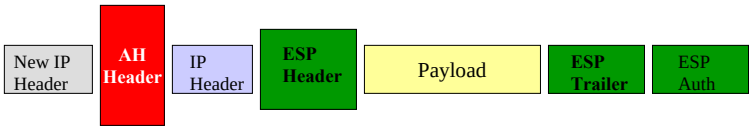
IPSEC - AH und ESP -

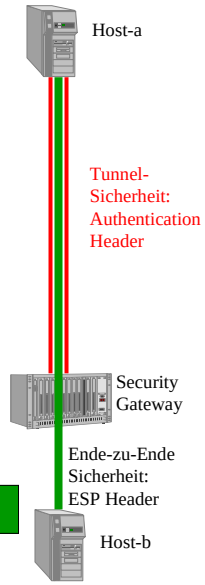
Original IP-Packet: Host-a - Host-b

ESP im Transportmodus: Host-a - Host-b



AH im Tunnelmodus: Host-a - Security Gateway





Werner Anrath - Zentralinstitut für Angewandte Mathematik

15

Forschungszentrum Jülich
in der Helmholtz-Gemeinschaft

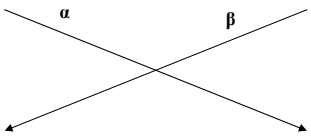
IPSEC und IKE - Diffie Hellman

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

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

16

Forschungszentrum Jülich
in der Helmholtz-Gemeinschaft

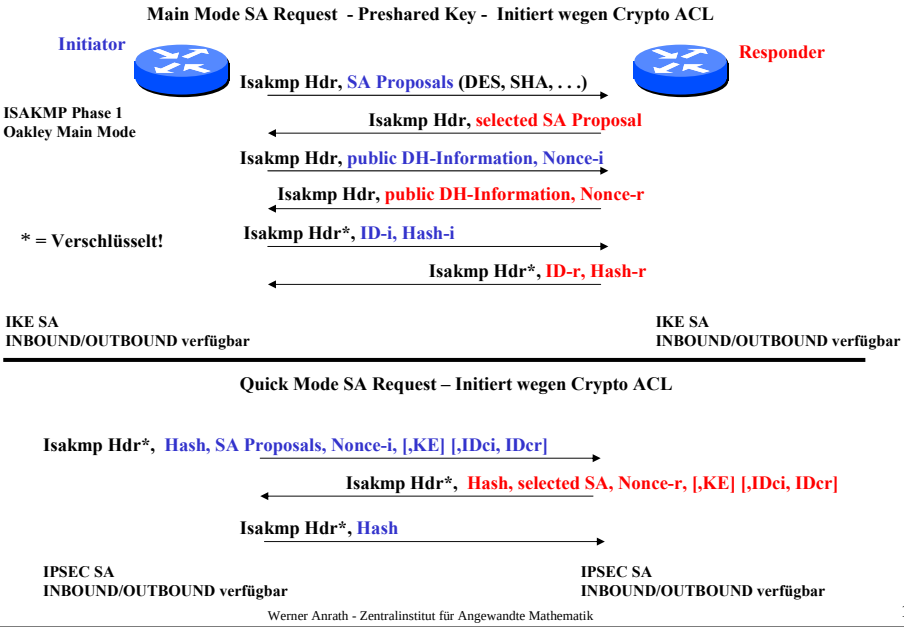
IPSEC und IKE

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

Werner Anrath - Zentralinstitut für Angewandte Mathematik 17

Forschungszentrum Jülich
in der Helmholtz-Gemeinschaft

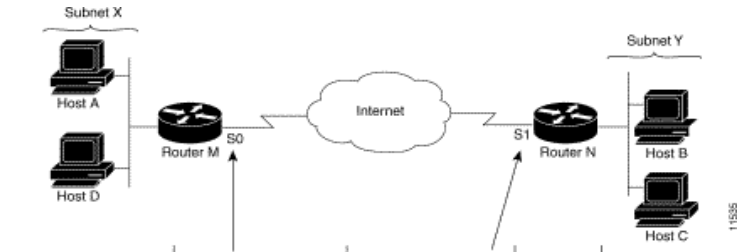
IPSEC und IKE - Main Mode / Quick Mode



Werner Anrath - Zentralinstitut für Angewandte Mathematik 18

IPSEC Site-to-Site VPN - Crypto Access Lists -

Forschungszentrum Jülich
in der Helmholtz-Gemeinschaft



		IPSec access list at S0:	IPSec access list at S1:	1st packet	Result
Mirror image access lists at Router M S0 and Router N S1	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)

Forschungszentrum Jülich
in der Helmholtz-Gemeinschaft

IPSEC und IKE Keepalive

- Möglichkeiten für Stateless Failover
  - IKE SA Keepalives
  - GRE Tunnel
- IKE Keepalives
  - im Standard ist kein Mechanismus vorgesehen, den Ausfall eines IPSEC-Peers zu erkennen, erst bei der zyklischen Erneuerung der Quick Mode SAs (Cisco IOS Default: 60 Minuten !!) wird der Ausfall erkannt
  - CISCO IKE Keepalives: Kontrollmeldungen im Abstand von 10 Sekunden – nach drei unbestätigten Kontrollmeldungen wird auf einen vorkonfigurierten Peer gewechselt:

```
crypto map  test_ike _keepalive  10  isakmp-ipsec
            set peer 172.18.45.1
            set peer 172.18.45.2
            .............
```

  - **Nachteil: es wird nicht auf den ursprünglichen Peer zurückgeschaltet!**

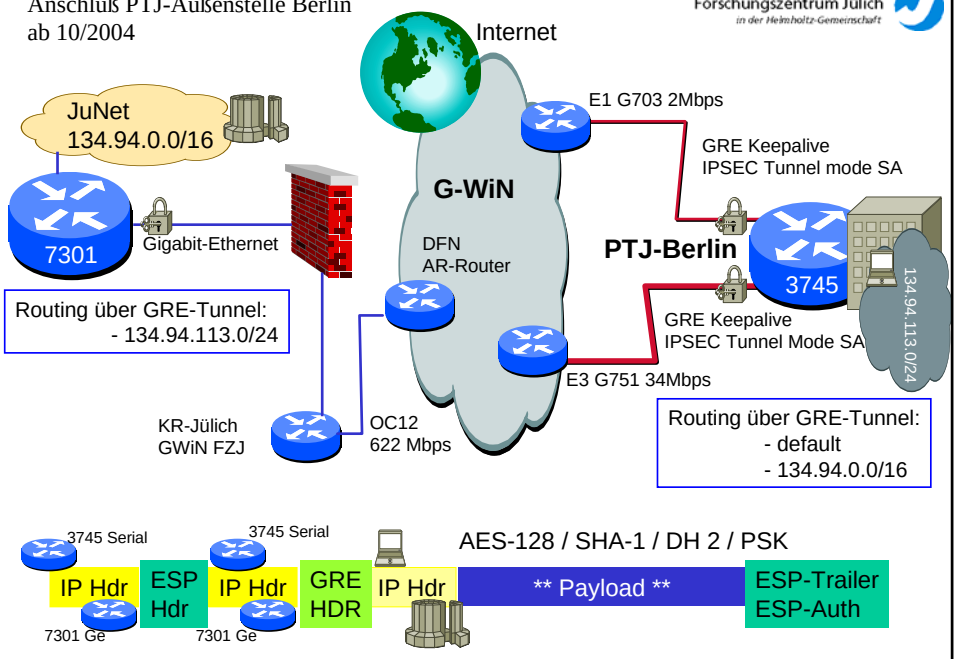
Forschungszentrum Jülich
in der Helmholtz-Gemeinschaft

GRE-over-IPSEC

- GRE Tunnel und IPSEC
  - Tunnel Mode oder Transport Mode konfigurierbar
  - Automatische Umschaltung durch Routing Protocol (Hello Msgs / Keepalives) -> *next best route*
  - die GRE Keepalives werden verschlüsselt und lösen gegebenenfalls die nötigen IKE-Schritte aus, d.h. die IKE SA und die Quick Mode SAs sind stets aktiv, auch auf dem alternativen Pfad
  - weitere Vorteile:
    - Routing Protokolle – OSPF
    - Multicast / Broadcast Traffic
    - non-IP Protocols

Anschluß PTJ-Außenstelle Berlin
ab 10/2004

Forschungszentrum Jülich
in der Helmholtz-Gemeinschaft



Router Konfiguration 7301
- Details -

Forschungszentrum Jülich
in der Helmholtz-Gemeinschaft

```
crypto isakmp policy 1
 encr aes
 authentication pre-share
 group 2
crypto isakmp key ********** ???
crypto isakmp key ********** ???
crypto ipsec transform-set fzj-ipsec-set esp-aes esp-md5-hmac
crypto map 2Mbps_Berlin_Backup 1 ipsec-isakmp
 description GRE-Tunnel mit 2 Mbit/s zu PTJ Berlin
 set peer serial-e1
 set transform-set fzj-ipsec-set
 match address E1_2Mbps_Traffic_Berlin
crypto map 34Mbps_Berlin 1 ipsec-isakmp
 description GRE-Tunnel mit 34 Mbps zu PTJ Berlin
 set peer serial-e3
 set transform-set fzj-ipsec-set
 match address E3_34Mbps_Traffic_Berlin
```

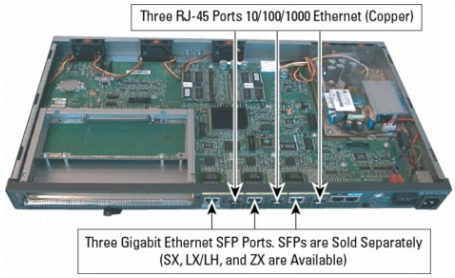
```
interface GigabitEthernet0/1
 description FZJ-Endpunkt fuer 34 Mbps Tunnel zu PTJ Berlin
 ip address ??? ???
 no ip proxy-arp
 duplex auto
 speed auto
 media-type rj45
 no negotiation auto
 no cdp enable
 crypto map 34Mbps_Berlin
!
interface GigabitEthernet0/2
 description FZJ-Endpunkt fuer 2 Mbps Tunnel zu PTJ Berlin
 ip address ??? ???
 no ip proxy-arp
 duplex auto
 speed auto
 media-type rj45
 no negotiation auto
 no cdp enable
 crypto map 2Mbps_Berlin_Backup
!
ip route –für Remote Lan- Tunnel0
ip route –für Remote Lan- Tunnel1 240
ip route - für Remote Serial E3 -
ip route - für Remote Serial E1 -
!
ip access-list extended E1_2Mbps_Traffic_Berlin
 permit gre host gigabiteth0/2 host serial-e1
ip access-list extended E3_34Mbps_Traffic_Berlin
 permit gre host gigabiteth0/1 host serial-e3
```

Werner Anrath - Zentralinstitut für Angewandte Mathematik 23

Router Konfiguration 7301
- Details -

Forschungszentrum Jülich
in der Helmholtz-Gemeinschaft

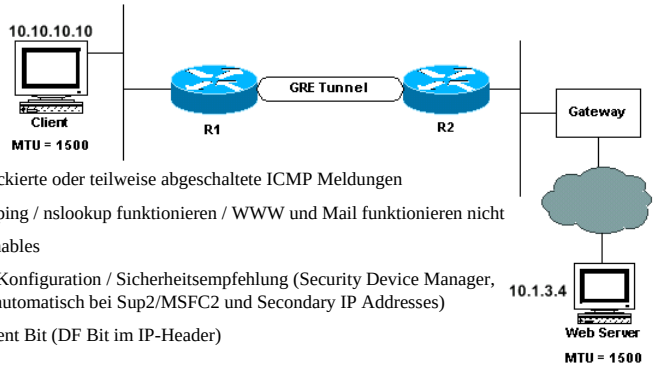
```
interface Tunnel0
 description Tunnel zur PTJ Aussenstelle in Berlin (uebers GWiN, 34 Mbps)
 ip address ???
 ip mtu 1420
 keepalive 10 3
 tunnel source Gigabiteth0/1
 tunnel destination serial-e3
!
interface Tunnel1
 description Tunnel zur PTJ Aussenstelle in Berlin (uebers GWiN, 2 Mbps, Backup)
 ip address ???
 ip mtu 1420
 keepalive 10 3
 tunnel source Gigabiteth0/2
 tunnel destination serial-e1
```



Werner Anrath - Zentralinstitut für Angewandte Mathematik 24

Erfahrungen
- Packet Fragmentation and ICMP -

Forschungszentrum Jülich
in der Helmholtz-Gemeinschaft



PATH MTU Discovery:

- Problem: blockierte oder teilweise abgeschaltete ICMP Meldungen
  - ping / nslookup funktionieren / WWW und Mail funktionieren nicht
- no ip unreachables
  - Konfiguration / Sicherheitsempfehlung (Security Device Manager, automatisch bei Sup2/MSFC2 und Secondary IP Addresses)
- Don‘t Fragment Bit (DF Bit im IP-Header)

Lösungmöglichkeiten:

1.) ip unreachables konfigurieren / zulassen

oder 2.) Anpassen der MTU-Size

- alle Clients - sehr aufwendig, Skalierungsproblem
- oder Tunnel MTU - alle Teilstrecken (1500+24) und maximale MTU bekannt?
- Hilfe: linux> tracepath *hostname*

3.) Proxy-Server

Erfahrungen
- IPSEC Peers und Adressen -

Forschungszentrum Jülich
in der Helmholtz-Gemeinschaft

```
ptj001#show crypto isakmp  ?
  key      Show ISAKMP preshared keys
  peers    Show ISAKMP peer structures
  policy   Show ISAKMP protection suite policy
  profile  Show ISAKMP profiles
  sa       Show ISAKMP Security Associations


ptj001#show crypto isakmp sa det
Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       X - IKE Extended Authentication
       psk - Preshared key, rsig - RSA signature
       renc - RSA encryption
```

Wichtig: IKE Peer IP-Adresse und Peer Interface IP-Adresse müssen identisch sein –> sonst IKE Failure

Forschungszentrum Jülich
in der Helmholtz-Gemeinschaft

Erfahrungen
- IPSEC Tunnel Endpoints -
- Alternative zur FZJ-Konfiguration -

crypto map local-address

To specify and name an identifying interface to be used by the crypto map for IPSec traffic, use the crypto map local-address command in global configuration mode. To remove this command from the configuration, use the no form of this command.

crypto map *map-name* **local-address** *interface-id*
no crypto map *map-name* ***local-address***

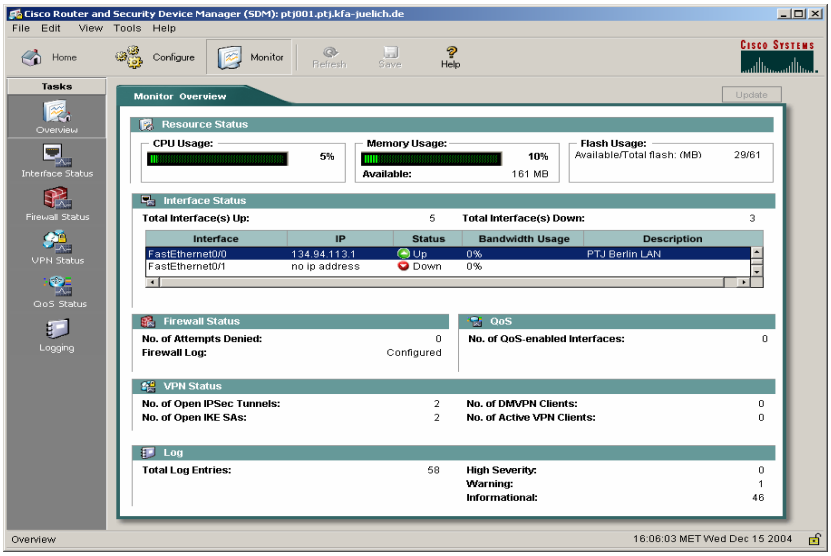
Syntax Description
map-name
Name that identifies the crypto map set. This is the name assigned when the crypto map was created.
interface-id
The identifying interface that should be used by the router to identify itself to remote peers.
If Internet Key Exchange is enabled and you are using a certification authority (CA) to obtain certificates, this should be the interface with the address specified in the CA certificates.

Defaults
No default behavior or values.
Command Modes

Werner Anrath - Zentralinstitut für Angewandte Mathematik 27

Forschungszentrum Jülich
in der Helmholtz-Gemeinschaft

Erfahrungen
- Empfehlung: Security Device Manager -



Werner Anrath - Zentralinstitut für Angewandte Mathematik 28

Forschungszentrum Jülich
in der Helmholtz-Gemeinschaft

Vielen Dank für Ihre Aufmerksamkeit!