



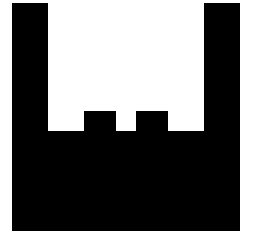
iX-Konferenz 2004



Linux und Ipsec: Aufbau und Verwaltung eines heterogenen VPNs



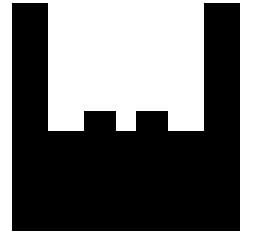
Inhalt



- IPsec Grundlagen: AH und ESP
- Das IKE Protokoll
- KAME Racoon
- Openswan
- Test und Fehlersuche im VPN
- Heterogene VPNs mit Windows



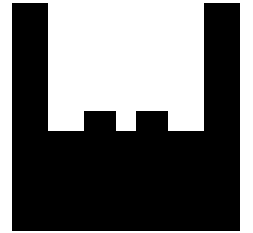
IP-IPsec



- IP ist das grundlegende Internet-Protokoll und bietet keinerlei Sicherheit
- (Fast) alle Informationen werden mit IP übertragen
- IPsec ist eine nahtlose Erweiterung
 - Authentifizierung
 - Integrität
 - Vertraulichkeit



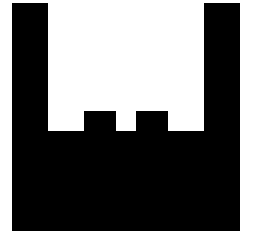
IPsec



- Bestandteil von IPv6
- Bietet
 - Vertraulichkeit
 - Integrität
 - Authentizität



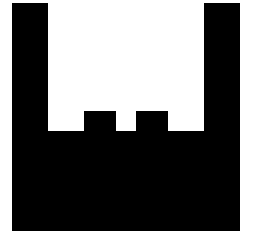
IPsec protocols



- IKE (Internet Key Exchange, RFC 2409)
 - ISAKMP (RFC 2408)
 - IPSEC DOI for ISAKMP (RFC 2407)
 - Oakley Key determination protocol (RFC 2412)
- AH (Authentication Header, RFC 2402)
- ESP (Encapsulated Security Payload, RFC 2406)



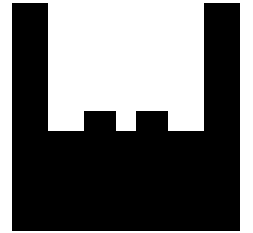
IKE



- UDP port 500
- 1. Phase
 - Aushandlung der ISAKMP SA
 - Authentifizierung und Aufbau eines sicheren Kanals
- 2. Phase
 - Aushandlung der IPsec SAs



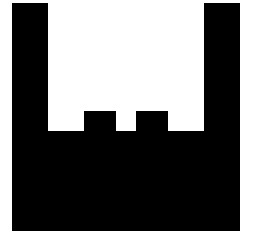
IKE Modi



- Main Modus
 - Identitätsschutz
 - Preshared Keys mit dynamischen IP-Adressen ist problematisch
- Aggressive Modus
 - kein Identitätsschutz
 - Offen für Angriff (DoS, ikecrack)
 - Unterstützt PSKs mit dynamischen IP-Adressen

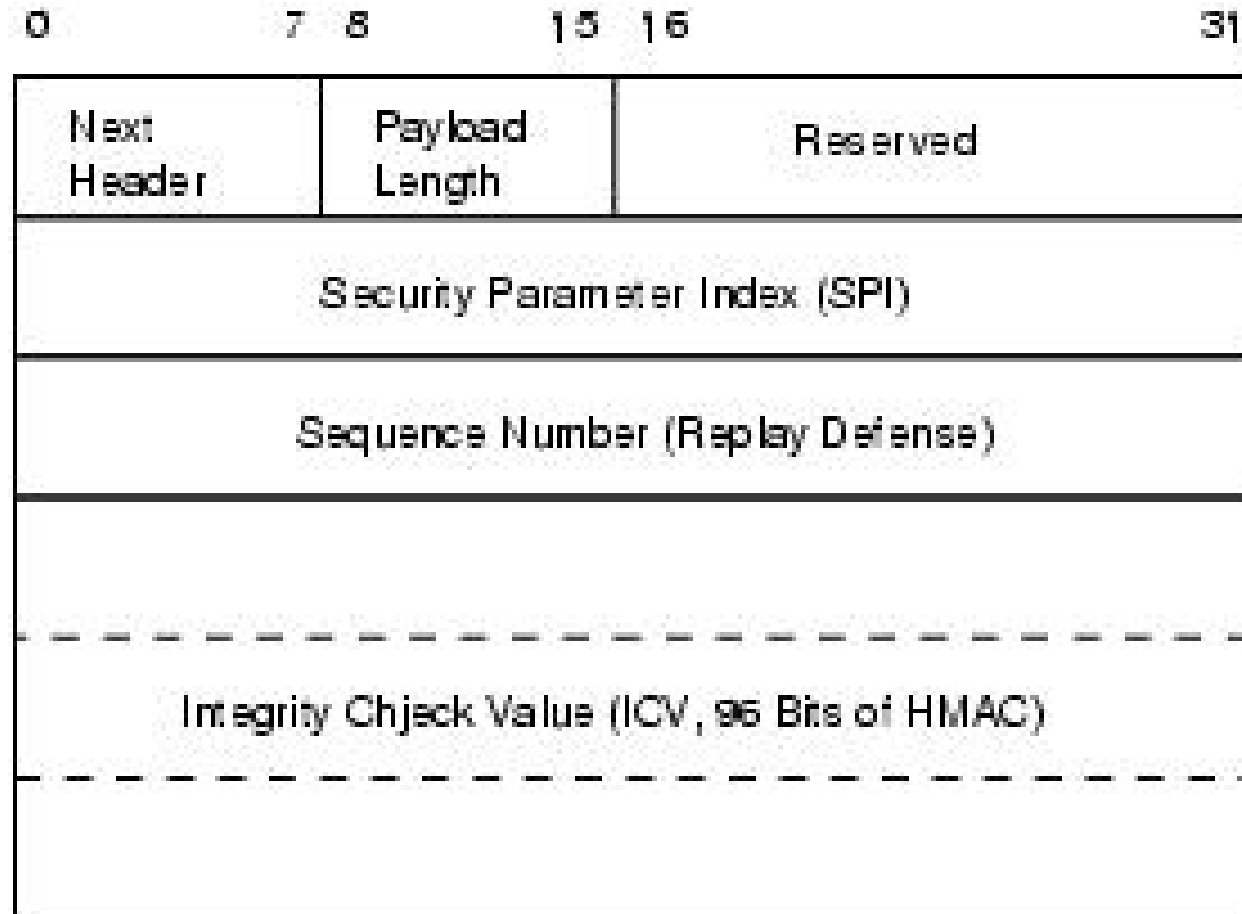
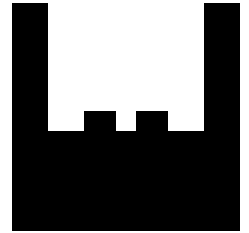


AH



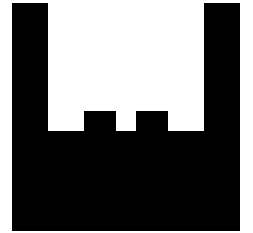
- IP Protokoll #51
- Authentifizierung
 - HMAC-SHA-96
 - HMAC-MD5-96
 - Sequenznummern
 - Schließt die unveränderlichen Teile des äußeren IP-Headers mit ein
- Transport- oder Tunnelmodus

AH-Header



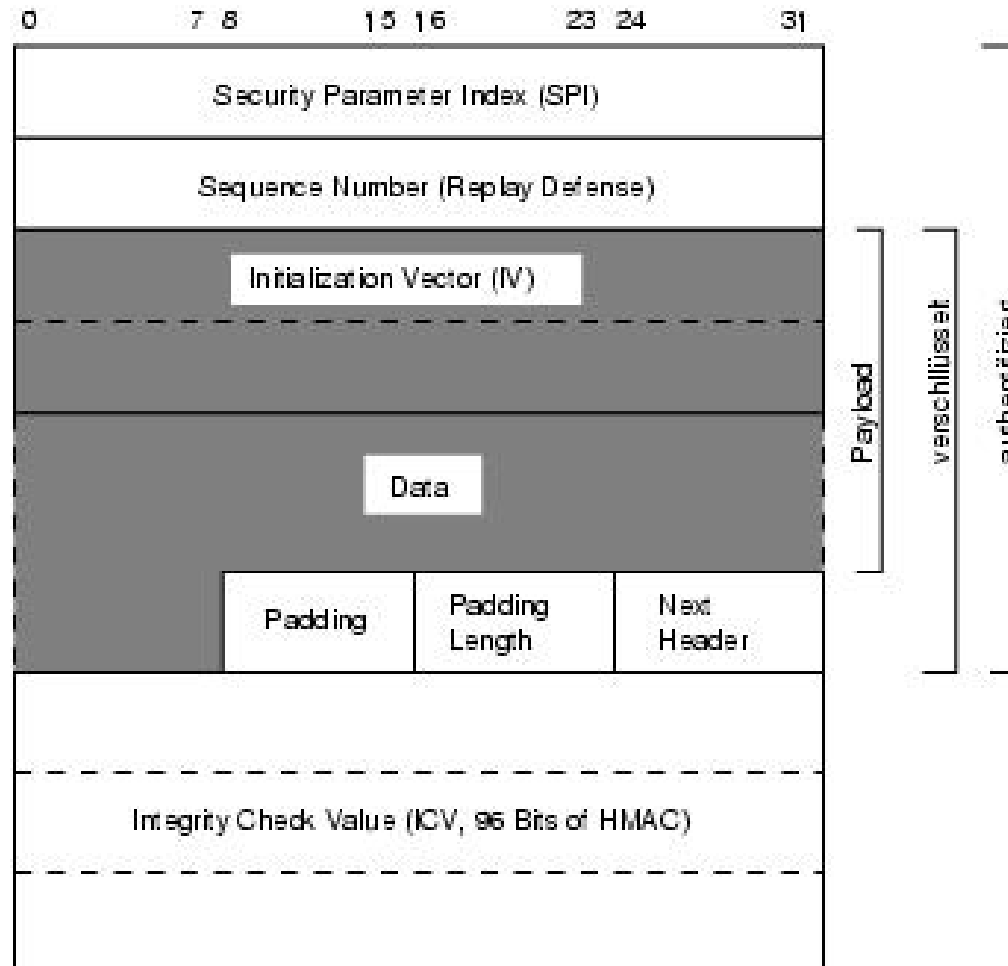


ESP

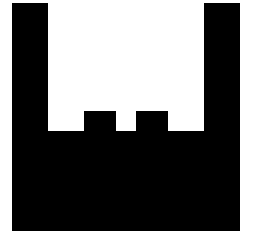


- IP Protokoll # 50
- Authentifizierung (ohne IP-Header)
 - HMAC-SHA-96
 - HMAC-MD5-96
 - Sequenznummern
- Symmetrische Verschlüsselung
- Transport- oder Tunnelmodus

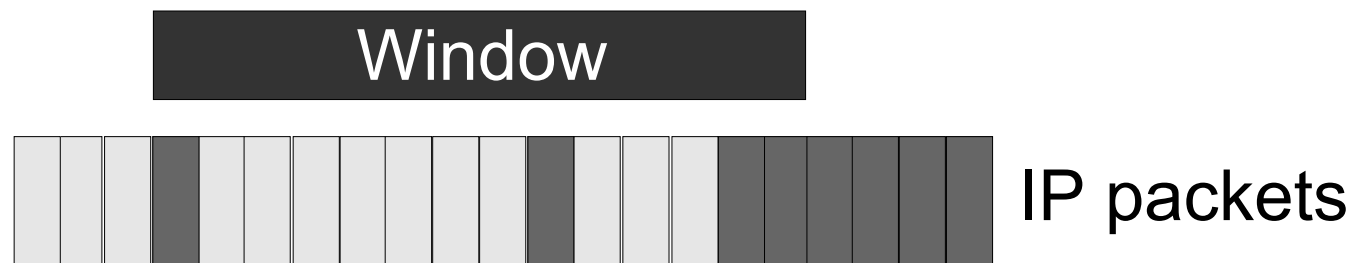
ESP-Header



Replay Schutz

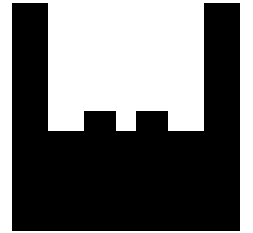


- Schiebefenster (Sequenznummern)

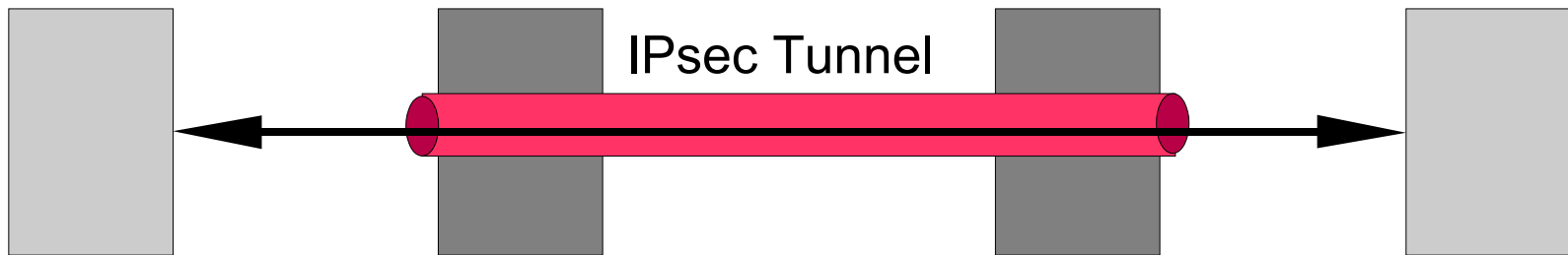


- Nur Pakete innerhalb und rechts des Fensters werden akzeptiert
- Neue Sequenznummern verschieben das Fenster nach rechts

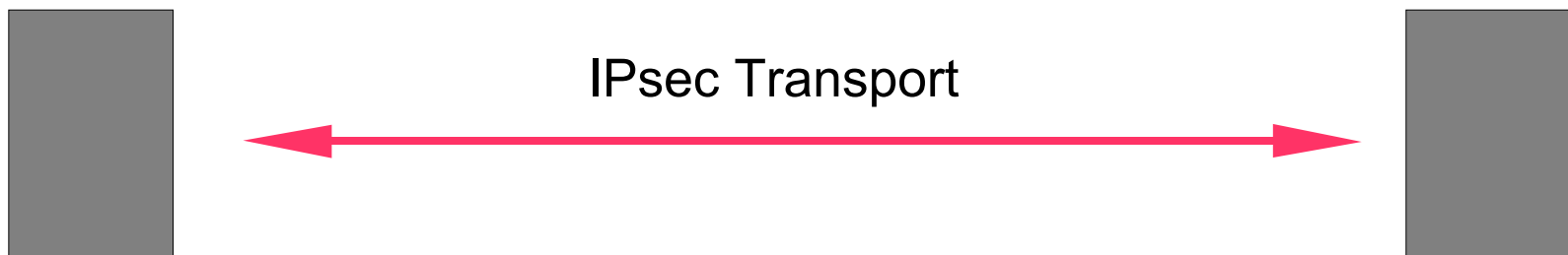
IPsec Modi



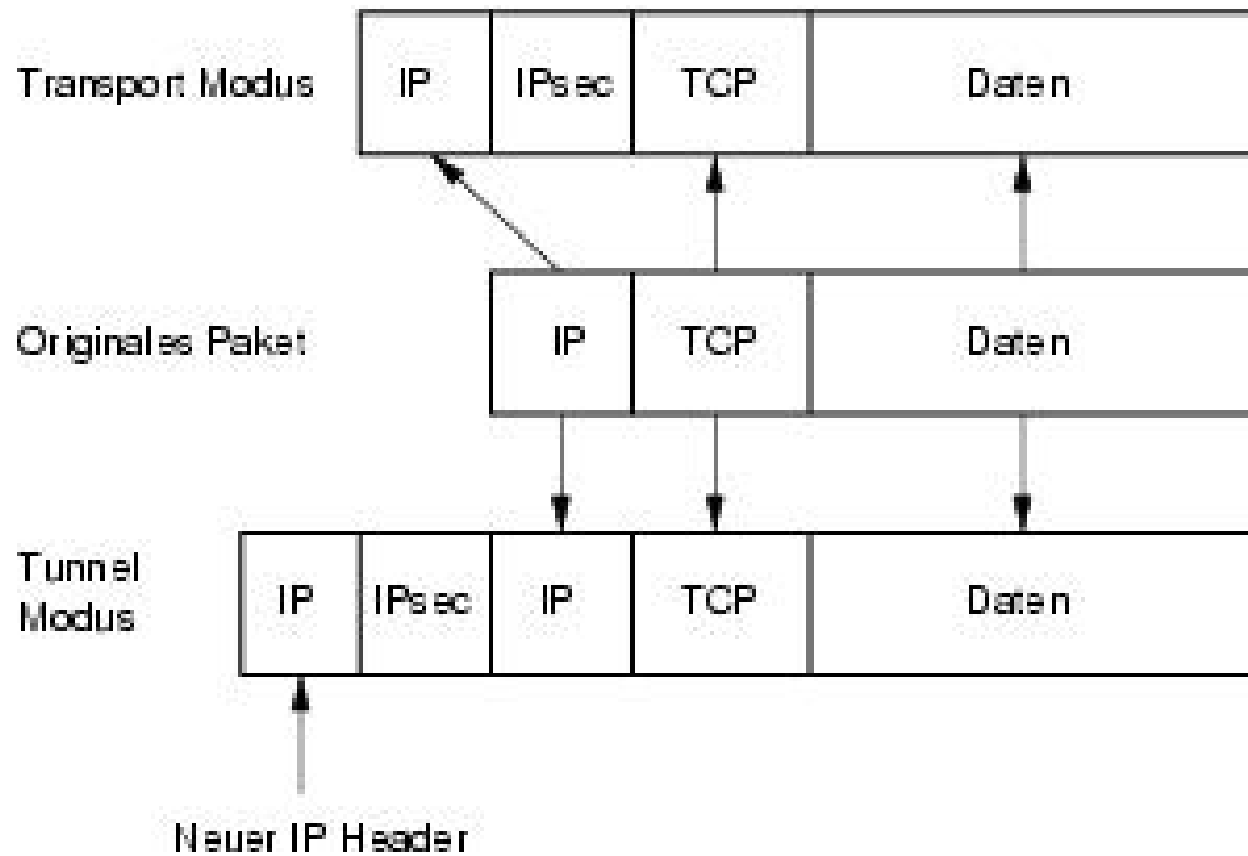
- Tunnel Modus



- Transport Modus

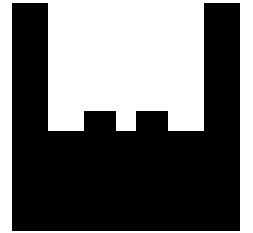


IPsec Modi II





IPsec Implementierungen



- FreeS/WAN (1996)
- PIPSEC (1998)
- IPNSEC (1998)
- NIST Cerberus (1999)
- U Arizona x-kernel (1998)



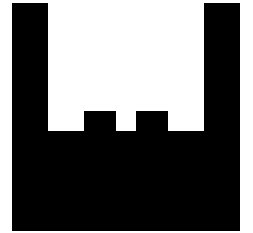
Henry Spencer



And, in fairness, KLIPS is the ugliest and least maintainable part of FreeS/WAN and deserves to be supplanted.



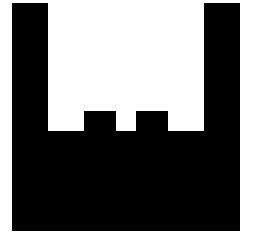
Native Implementierung



- Dave Miller
- Alexey Kuznetsov
- neue native Implementierung in 2.5.45
- basierend auf USAGI und KAME Projekten
- verwendet die CryptoAPI



SA vs. SP



- Security Association
 - Wie werden die Daten geschützt?
 - algorithms, session keys, SPIs and IP-addresses
 - Security Association Database (SAD)
- Security Policy
 - Welche Daten werden geschützt?
 - SPD



Definition der SAs



```
#!/usr/sbin/setkey -f

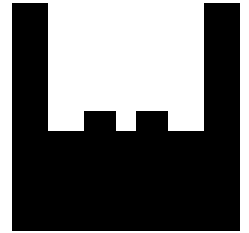
# Flush SAD
flush;

# manual settings for AH SAs
add 3.0.0.1 5.0.0.1 ah 0x200 -A hmac-md5
0xbf9a081e7ebdd4fa824c822ed94f5226;
add 5.0.0.1 3.0.0.1 ah 0x300 -A hmac-md5
0xbf9a081e7ebdd4fa824c822ed94f5226;

# manual settings for ESP SAs
add 3.0.0.1 5.0.0.1 esp 0x201 -E 3des-cbc
0x3f0b868ad03e68acc6e4e4644ac8bb80ecea3426d3d30ada;
add 5.0.0.1 3.0.0.1 esp 0x301 -E 3des-cbc
0x3f0b868ad03e68acc6e4e4644ac8bb80ecea3426d3d30ada;
```



Definition der SPs



```
#!/usr/sbin/setkey -f

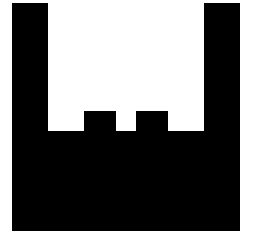
# Flush the SPD
spdflush;

# Defining the Security Policies
spdadd 3.0.0.1 5.0.0.1 any -P out ipsec
        esp/transport//require
        ah/transport//require;

spdadd 5.0.0.1 3.0.0.1 any -P in ipsec
        esp/transport//require
        ah/transport//require;
```



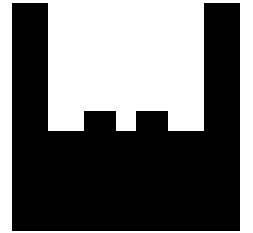
Native Implementierung II



- IPsec Konfiguration kann erfolgen mit
 - setkey/racoon (KAME)
 - isakmpd (OpenBSD)
 - FreeS/WAN
 - Openswan
 - Strongswan



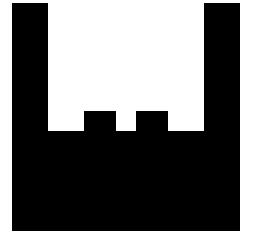
Openswan Komponenten



- Pluto
 - IKE Protokoll Daemon
- ipsec
- Konfiguration Dateien
 - /etc/ipsec.conf
 - /etc/ipsec.secrets



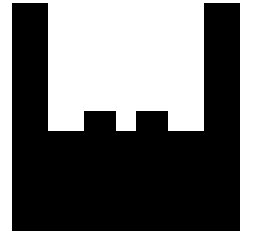
ipsec



- Zentraler Befehl
- ipsec
 - setup
 - auto
 - look / barf



Konfigurationsdateien



- ipsec.secrets
 - Private Schlüssel
 - Geheime Kennwörter
- ipsec.conf
 - Konfiguration der Tunnel



ipsec.conf I



```
config setup
```

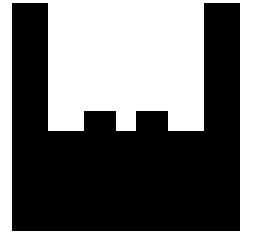
```
plutodebug      = none
```

```
klipsdebug      = none
```

```
uniqueids       = yes
```



ipsec.conf II



- Default Werte

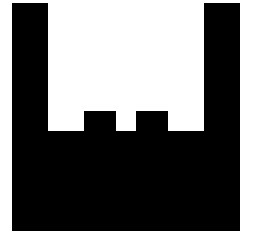
```
conn %default
```

```
keyingtries          = 0
```

```
authby               = secret
```



ipsec.conf III

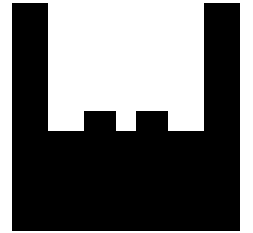


- Tunneldefinition

```
# sunset-west-router-east-sunrise
conn west-east
    left                = 192.168.1.1
    leftnexthop         = 192.168.1.254
    leftsubnet          = 10.0.1.0/24
    right               = ....
    auto                = start
```



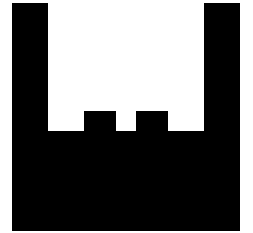
Road Warrior



- Rechner mit dynamischen IP-Adressen
 - Handelsreisende
 - Telearbeiter
- Adresse kann nicht zur Authentifizierung genutzt werden
- Keine dauerhafte Verfügbarkeit
 - Gateway darf nicht die Verbindung starten



Road Warrior ipsec.conf



- Gateway (Auszug):

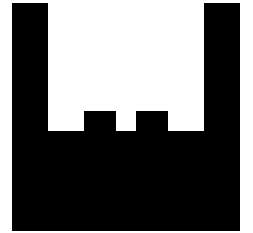
```
right          =0.0.0.0 # or %any
auto           =add
keyingtries    =1
```

- Roadwarrior (Auszug):

```
right          =%defaultroute
auto           =start
keyingtries    =0
```



Racoon



- Authentifizierung mit PSKs / X.509 / Kerberos
- NAT-Traversal
- Keine Unterstützung von Variablen
- Keine Hooks für up/down Ereignisse



Racoon



```
path pre_shared_key "/etc/psk.txt";

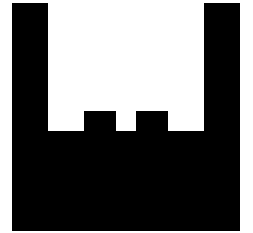
remote 3.0.0.1 {
    exchange_mode main;
    proposal {
        encryption_algorithm 3des;
        hash_algorithm md5;
        authentication_method pre_shared_key;
        dh_group modp1024;
    }
}

sainfo address 10.0.2.0/24 any address 10.0.1.0/24 any {
    pfs_group 768;
    encryption_algorithm 3des;
    authentication_algorithm hmac_md5;
    compression_algorithm deflate;
}
```

```
# IPv4 addresses
10.0.5.1          bad psk
5.0.0.1          0xe10bd52b0529b54aac97db63462850f3
```



Kernel ruft Racoon



```
#!/usr/sbin/setkey -f
#
# Flush SAD and SPD
flush;
spdflush;

# Define the policies to use ipsec. When no SA exists racoon will
# be called

spdadd 10.0.1.0/24 10.0.2.0/24 any -P out ipsec
        esp/tunnel/3.0.0.1-5.0.0.1/require;

spdadd 10.0.2.0/24 10.0.1.0/24 any -P in ipsec
        esp/tunnel/5.0.0.1-3.0.0.1/require;
```



Racoon mit X.509



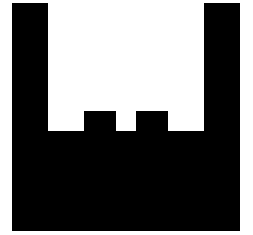
```
path certificate "/etc/certs";

remote 3.0.0.1 {
    exchange_mode main;
    certificate_type x509 "my_cert.pem" "my_req.pem";
    my_identifier asn1dn;
    peers_identifier asn1dn;
    proposal {
        encryption_algorithm 3des;
        hash_algorithm md5;
        authentication_method rsasig;
        dh_group modp1024;
    }
}

sainfo address 10.0.2.0/24 any address 10.0.1.0/24 any {
    pfs_group modp768;
    encryption_algorithm 3des;
    authentication_algorithm hmac_md5;
    compression_algorithm deflate;
}
```

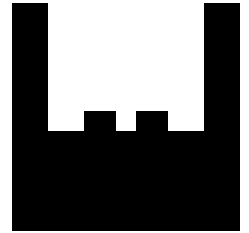


Isakmpd



- Authentifizierung mit PSKs / X.509
- IKE Mode Config
- Kein NAT-Traversal
- Keine Unterstützung von Variablen
- Keine Hooks für up/down Ereignisse

isakmpd.conf



```
[General]
Listen-on= 3.0.0.1

[Phase 1]
5.0.0.1= ISAKMP-peer-east

[Phase 2]
Connections= IPsec-west-east

[ISAKMP-peer-east]
Phase= 1
Transport= udp
Address= 5.0.0.1
Local-address= 3.0.0.1
Configuration= Default-main-mode
ID= West

[West]
ID-type= IPV4_ADDR
Address= 3.0.0.1

[IPsec-west-east]
Phase= 2
ISAKMP-peer= ISAKMP-peer-east
Configuration= Default-quick-mode
Local-ID= Net-west
Remote-ID= Net-east

[Net-west]
ID-type= IPV4_ADDR_SUBNET
Network= 10.0.1.0
Netmask= 255.255.255.0

[Net-east]
ID-type= IPV4_ADDR_SUBNET
Network= 10.0.2.0
Netmask= 255.255.255.0

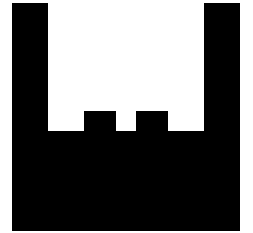
[Default-main-mode]
DOI= IPSEC
EXCHANGE_TYPE= ID_PROT
Transforms= 3DES-SHA-RSA_SIG, 3DES-MD5-RSA_SIG, BLF-MD5-RSA_SIG, BLF-SHA-RSA_SIG

[Default-quick-mode]
DOI= IPSEC
EXCHANGE_TYPE= QUICK_MODE
Suites= QM-ESP-AES-SHA-PFS-SUITE

[X509-certificates]
CA-directory= /etc/isakmpd/ca/
Cert-directory= /etc/isakmpd/certs/
CRL-directory= /etc/isakmpd/crls
Private-key= /etc/isakmpd/private/local.key
```



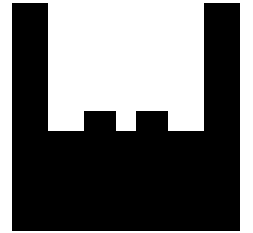
Heterogene VPNs



- Standardisierung erlaubt den Aufbau heterogener VPNs
- IPsec Protokolle AH und ESP sind hoch kompatibel
- IKE erzeugt Probleme
- Interoperabilitätstest
 - <http://www.hsc.fr/ressources/ipsec/ipsec2001/>

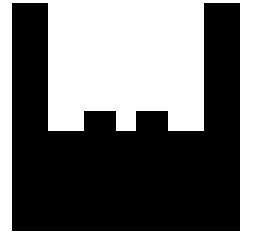


Windows 2000/XP



- Komplizierte Konfiguration
- Markus Müller: ipsec.exe erlaubt die einfache Konfiguration
- Erforderlich
 - vpn-package.zip (<http://vpn.ebootis.de>)
 - ipsecpol (Win2k)
 - ipseccmd (WinXP)
 - SrvPck 2 (Win2k)

Windows 2000/XP Konfiguration

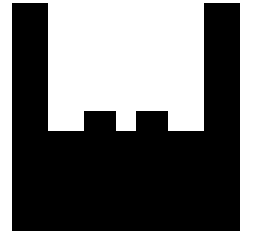


- Zertifikate werden als PKCS#12 importiert
- Einfache Konfigurationsdatei

```
conn default
    dial=ISP-Provider
conn vpn
    left=%any
    right=194.139.117.253
    rightsubnet=192.168.8.0/24
    # rightca='C=DE, ST=NRW, L=Steinfurt,
O=OpenSourceSecurity, OU=RootCA, CN=RootCA 2001'
    presharedkey=geheim
    network=auto (or ras or lan)
    auto=start
    pfs=yes
```



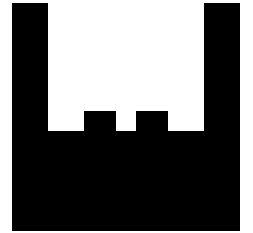
Start des Tunnels



- ipsec.exe konfiguriert den Tunnel mit allen notwendigen Informationen
- Automatische Einwahl bei Anforderung

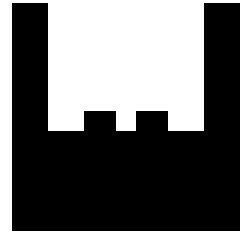


IPsec Probleme/Lösungen

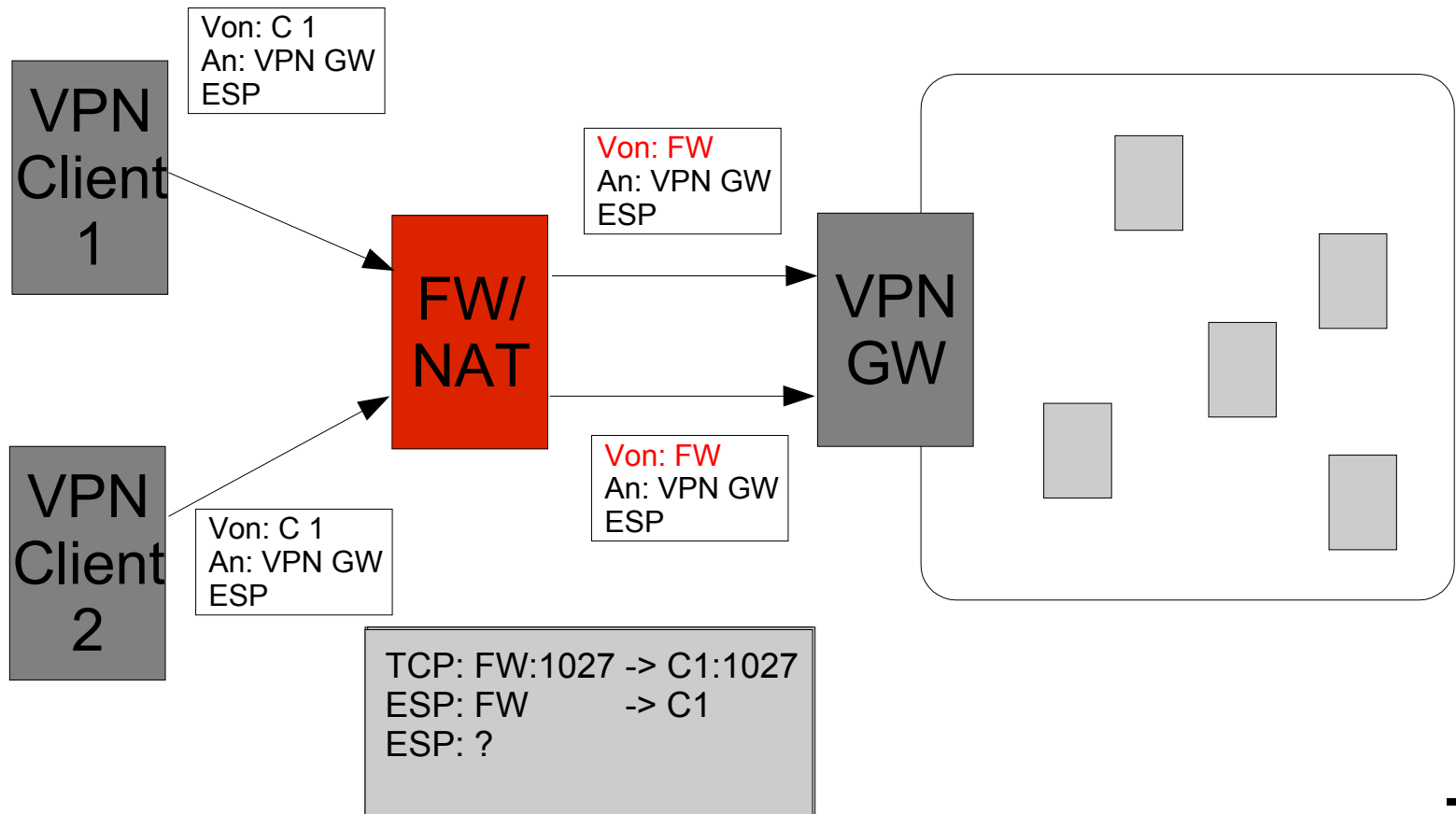


- Keine Zuweisung von IP-Adressen
 - IKE Mode Config
 - DHCP-over-IPsec
 - L2TP
- Keine NAT-Fähigkeit
 - IPsec Passthrough
 - NAT-Traversal
- Keine Benutzerauthentifizierung
 - xauth
 - L2TP

NAT

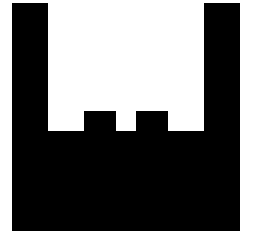


- AH und NAT ist gleichzeitig nicht einsetzbar



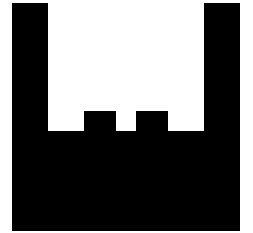


Vor- und Nachteile

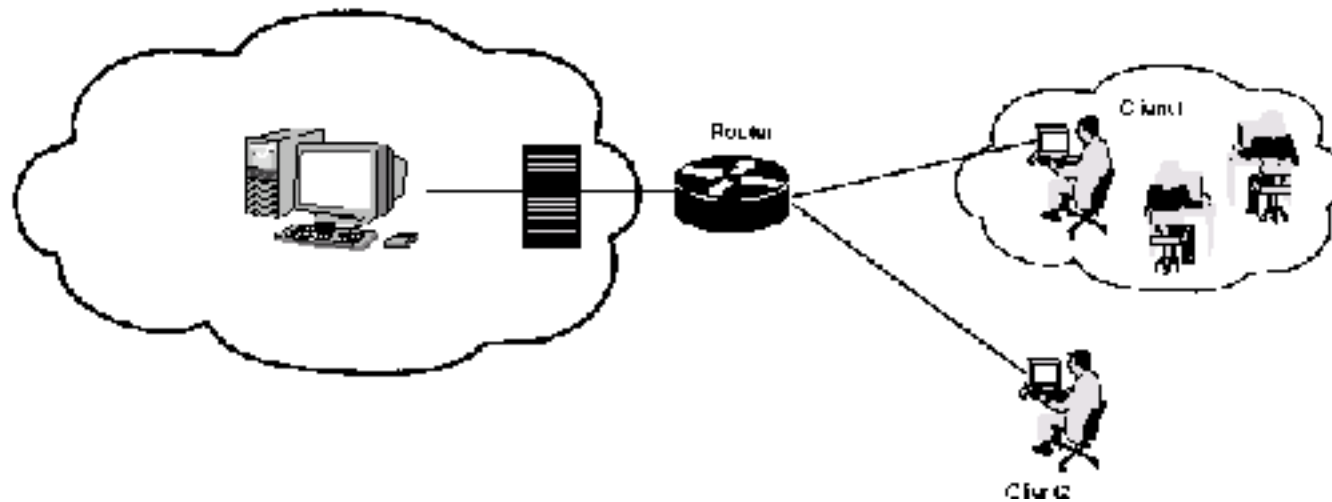


- Kein virtuelles ipsec0 Interface
- Kein Firewalling im Transportmodus möglich
- Eingeschränktes Firewalling im Tunnel
 - Erste Verbesserungen
 - policy match

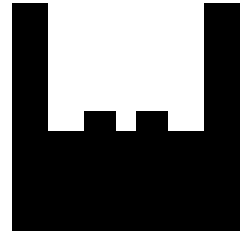
Pilotprojekt



- Racoon
- L2TP
- Authentifizierung gegen SAMBA DC



Schulungen/Unterstützung



- Dozent
 - Schulungen seit 1999
- Referenzenauswahl
 - T-Systems
 - Red Hat
 - Triaton
 - ESAG
 - TSTG Schienentechnik
 - Stuttgarter Versicherung

