



---

## Vorlesung

VPN: Drahtgebunden und drahtlos

Fachbereich Informatik (FB 20)

Lehrstuhl Prof. J. Buchmann

WS-05 / V2 - 20.205.1

In Zusammenarbeit mit dem CAST-Forum

Dr. Wolfgang Böhmer

Skript: <http://www.cdc.informatik.tu-darmstadt.de/~wboehmer/>

Email: [wboehmer@cdc.informatik.tu-darmstadt.de](mailto:wboehmer@cdc.informatik.tu-darmstadt.de)

---





## 6. Layer-3-Techniken und der Sicherheitsstandard für das Internet (IPSec)

1. Das Ziel von IPSec
2. IPSec-Sicherheitsvereinbarungen (SA) / Initiierung und Kombination
3. IPSec-AH-Header
4. IPSec-ESP-Header
5. IPSec und Remote Access (siehe Exkurs WLAN)
6. Internet-Key-Exchange-Management (IKE) (Phase-1 /Phase-2)
7. ISAKMP/Oakley und Skip
8. Layer-2- und Layer-3-Vergleich

## 7. Layer-4-Techniken

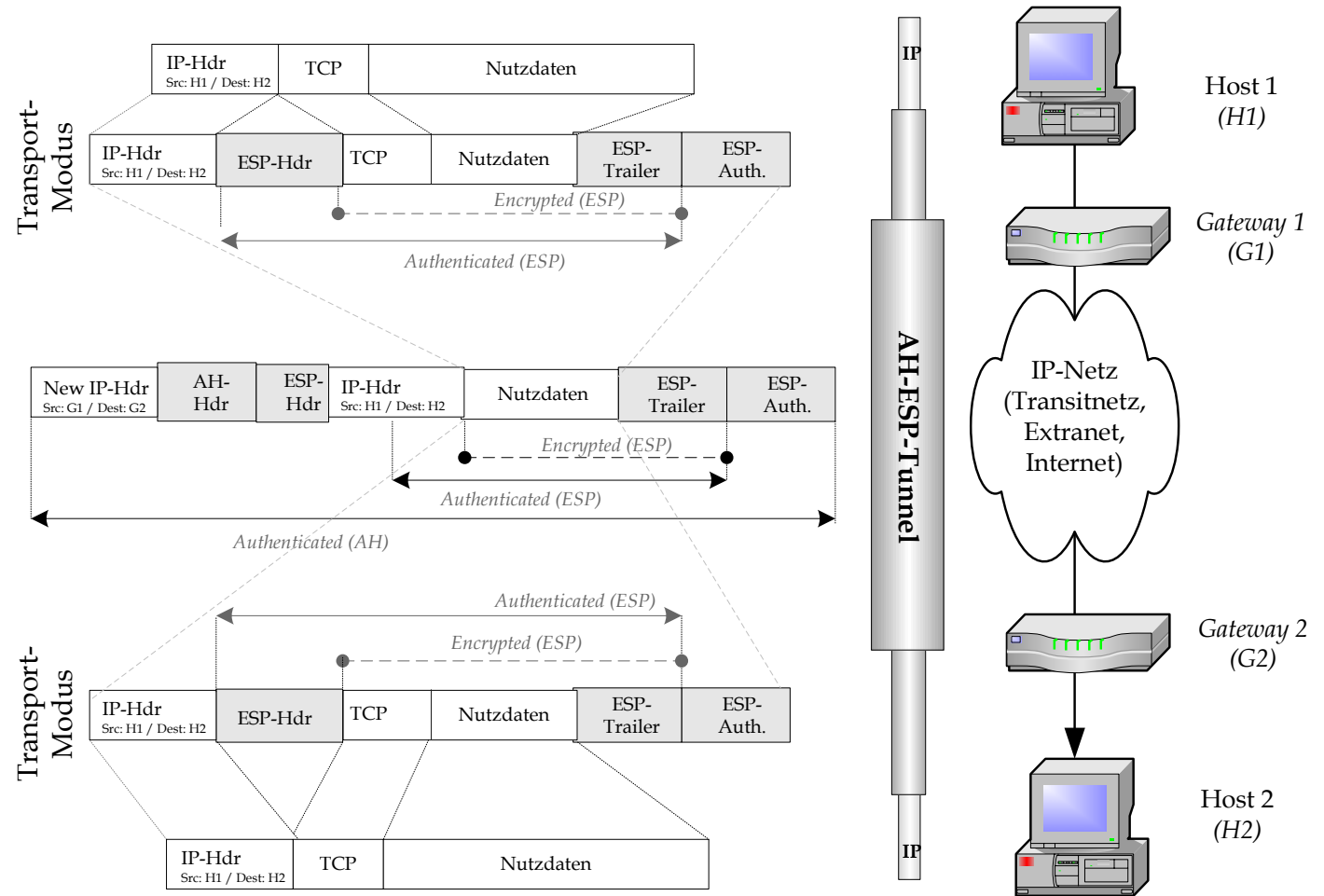
1. Secure Socket Layer (SSL) und Transport Layer Sicherheit (TLS)
2. Vergleich IPSec und SSL/TLS

## 8. Layer-5-Techniken

1. Socks V.5



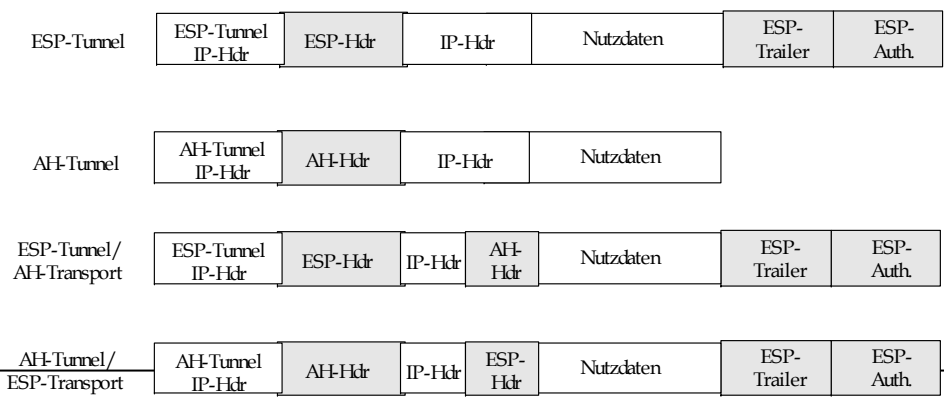
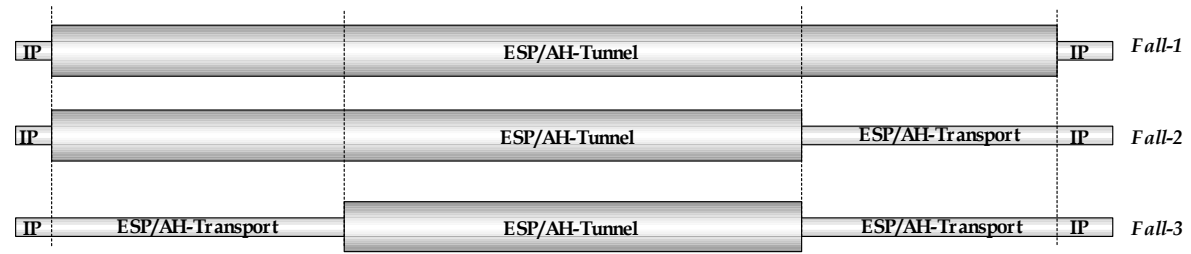
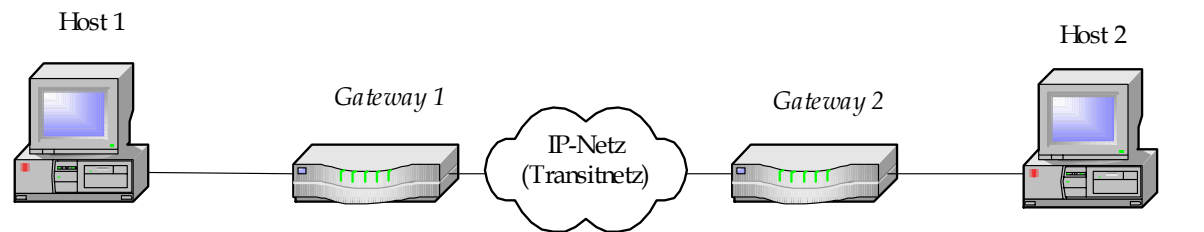
# IPSec-Verbindung im Tunnel Modus zwischen Host-H1 und Host-H2 sowie den Gateways G1 und G2





# Kombinationen von Security Associations (SA)

- **Fall-1:** Zwischen beiden Host-Systemen kann jeweils ein SA-AH-Tunnel oder ein SA-ESP-Tunnel ausgehandelt werden. G1 und G2 stellen reguläre Router dar.
- **Fall-2:** Ein Tunnel wird von H1 zu G2 aufgebaut. Damit können SA-AH und SA-ESP-Vertragsverhandlungen erfolgen, jedoch sind auch einfache SA-AH-ESP oder SA-ESP-AH möglich
- **Fall-3:** Typische VPN-Situation; nur zwischen G1 und G2 sind existierende gesicherte Verbindungen. Es wird eine SA-AH oder SA-ESP aufgebaut.



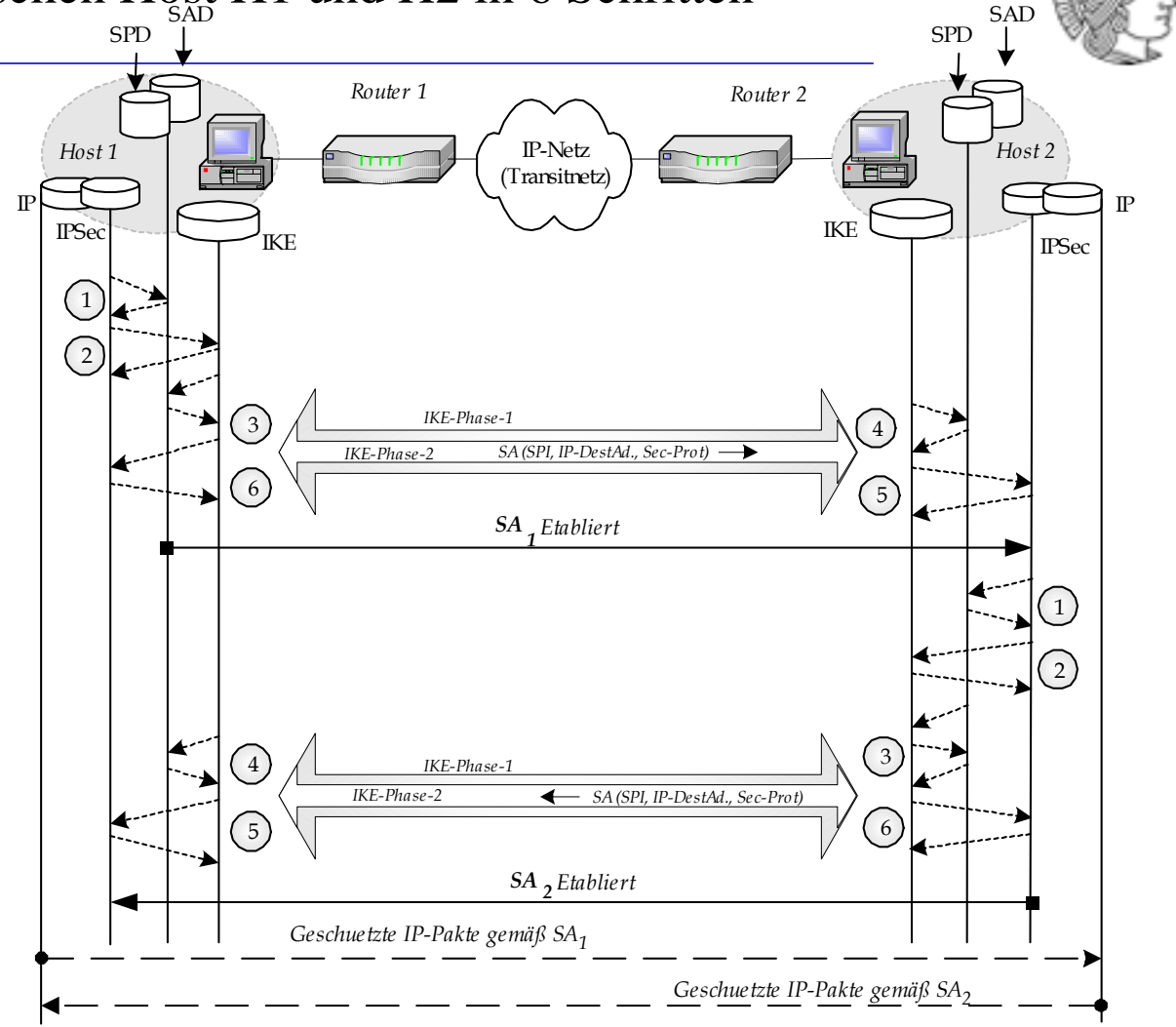


## Initiierung einer Security Association

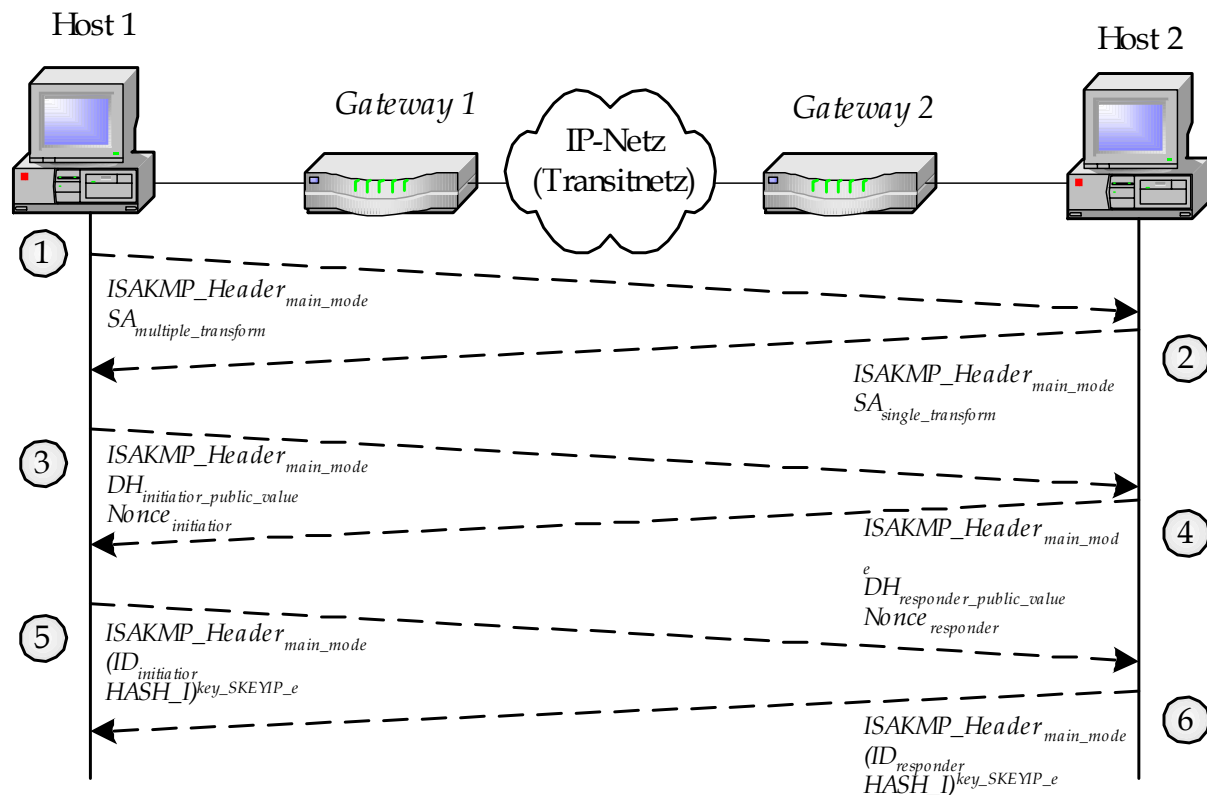
- Bisherige Betrachtungen legen eine durchgeführte Identifizierung der Kommunikationspartner zugrunde
- Schlüsselaustausch wurde vorab ebenfalls vollzogen
- Bevor zwischen zwei Host-Systemen ein aktiver Paket-Austausch stattfinden kann, müssen SA vereinbart werden
  - jeder Host muß eine eigene SPD haben
  - Konkrete Eintragungen werden für eine SA an die SAD vererbt.
- Zur Absicherung findet ein Schlüsselaustausch nach IKE statt
  - Phase-1 (IKE-Control-Channel)
  - Phase-2 (IKE-SA)



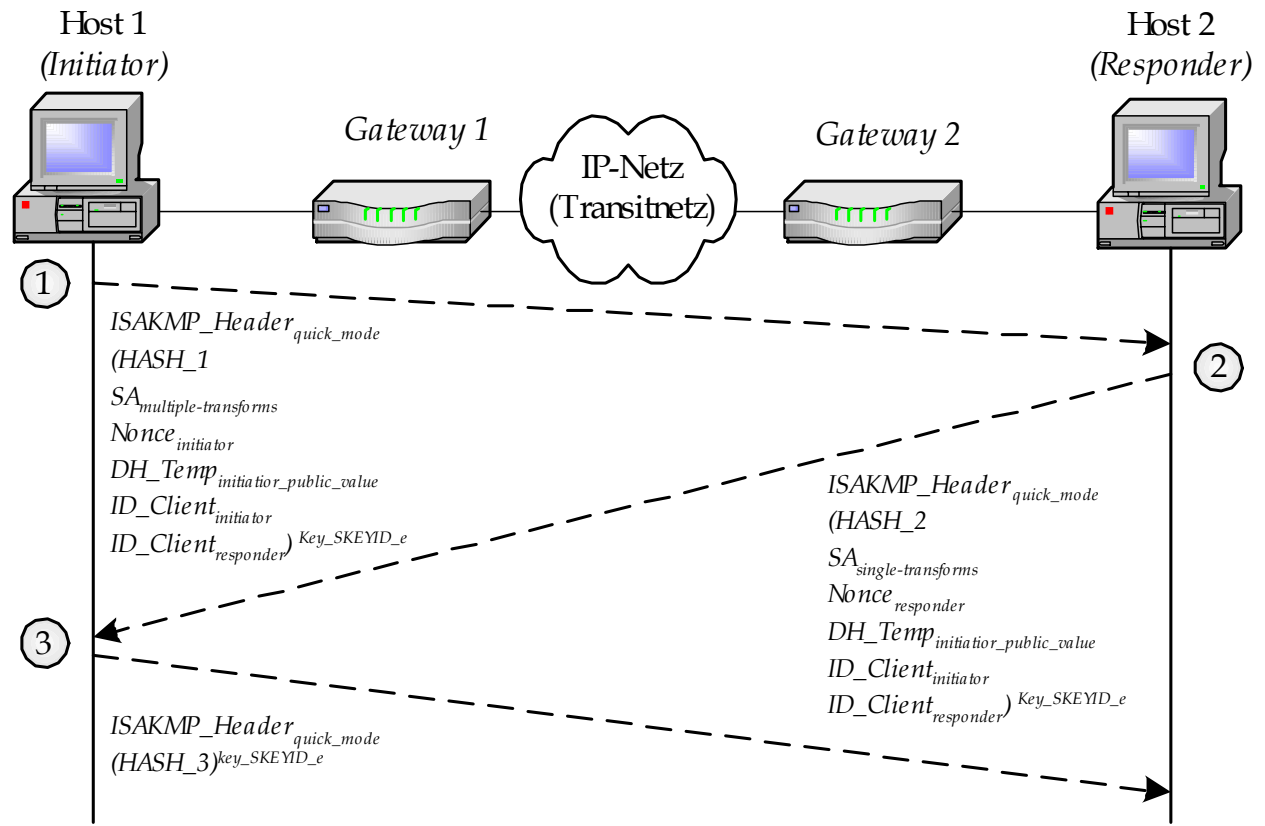
# SA-Initiierung zwischen Host H1 und H2 in 6 Schritten



# IKE-Phase-1 im Main Mode mit *Pre-shared-Keys*



# IKE-Phase-2 im Quick Mode





# IPSec-Mitschnitt

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.200.1	192.168.200.2	ISAKMP	Identity Protection (Main Mode)
2	0.104506	192.168.200.2	192.168.200.1	ISAKMP	Identity Protection (Main Mode)
3	0.184914	192.168.200.1	192.168.200.2	ISAKMP	Identity Protection (Main Mode)
4	0.220083	192.168.200.2	192.168.200.1	ISAKMP	Identity Protection (Main Mode)
5	0.248582	192.168.200.1	192.168.200.2	ISAKMP	Identity Protection (Main Mode)
6	0.250228	192.168.200.2	192.168.200.1	ISAKMP	Identity Protection (Main Mode)
7	0.252400	192.168.200.1	192.168.200.2	ISAKMP	Quick Mode
8	0.254069	192.168.200.2	192.168.200.1	ISAKMP	Quick Mode
9	0.254976	192.168.200.1	192.168.200.2	ISAKMP	Quick Mode
10	0.256527	192.168.200.2	192.168.200.1	ISAKMP	Quick Mode
11	0.258657	192.168.200.1	192.168.200.2	ESP	ESP (SPI=0x481c3663)
12	0.258964	192.168.200.2	192.168.200.1	ESP	ESP (SPI=0x652c1f92)
13	4.784306	192.168.200.1	192.168.200.2	ESP	ESP (SPI=0x481c3663)
14	4.784722	192.168.200.2	192.168.200.1	ESP	ESP (SPI=0x652c1f92)
15	5.778338	192.168.200.1	192.168.200.2	ESP	ESP (SPI=0x481c3663)
16	5.778737	192.168.200.2	192.168.200.1	ESP	ESP (SPI=0x652c1f92)
17	6.777294	192.168.200.1	192.168.200.2	ESP	ESP (SPI=0x481c3663)

Protocol: UDP (0x11)  
Header checksum: 0x360d (correct)  
Source: 192.168.200.1 (192.168.200.1)  
Destination: 192.168.200.2 (192.168.200.2)  
 User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)  
Source port: isakmp (500)  
Destination port: isakmp (500)  
Length: 116  
Checksum: 0x1dae (correct)  
 Internet Security Association and Key Management Protocol  
Initiator cookie  
Responder cookie  
Next payload: Security Association (1)  
Version: 1.0  
Exchange type: Identity Protection (Main Mode) (2)  
 Flags  
Message ID: 0x00000000  
Length: 108  
 Security Association payload  
 Vendor ID payload

```
0030  c9 bd 09 21 29 29 91 60 00 4f 65 2c 1f 92 00 00  ...!)... :oe.█..
0040  00 05 b0 43 b0 a6 16 25 27 3f d8 11 29 12 e0 67  ...C...% ?...g
0050  8d 78 5a 80 38 0e 1d eb bd e1 ab 74 d5 ce 56 d3  .xZ.8... ..t..v.
0060  e4 2e 8b 7f e1 7d 04 d8 1d 9b b2 02 65 4e d4 0c  ...|.}... .en..
0070  e8 56 a6 5c 38 9b ea f2 f9 f5 33 30 94 92 23 a2  .v.\8... ..30..#.
```





## Angriffe auf IPSec (i) / Sammeln der Informationen

- VPN-Verschlüsselung ist kaum zu überwinden
- Die Endpunkte bieten die besten Angriffspunkte
  - ➔ Notebook und VPN-Gateways
- Vorbereitung des Angriffs  
Portscanning mittels nmap.
  - Aus den Fingerprint ist eindeutig eine Checkpoint NG zu erkennen.
  - Der Port 500/udp zeigt isakmp an
  - Es könnte sich um ein L2TP/IPSec VPN handeln.

```
# nmap -sSUV -O 10.1.1.254
Starting nmap 3.70 (Interesting ports on 10.1.1.254:
PORT STATE SERVICE
256/tcp open fw1-secureremote
257/tcp open fw1-log service
259/udp open|filtered firewall1-rdp
500/udp open|filtered isakmp
1701/udp open|filtered L2TP
Device type: firewall
Running: Checkpoint Windows NT/2K/XP
OS details: Checkpoint SecurePlatform NG FP3
```





## Angriffe auf IPSec (ii) Fingerabdrücke

- IKE-scan mit der Option trans=5.2.1.5 prüft die kryptografischen Parameter an: 3DES, SHA1, pre-shared Key, Diffie Hellman Group 5
- Die Meldung IKE Main Mode Handshake, zeigt das das VPN-GW die Parameter akzeptiert. Es wird auch gleich der Hersteller angezeigt.
- Der erfolgreiche Einsatz des Tools ist allerdings stark von der Konfiguration und den unterstützenden Parametern des VPN-GW abhängig.
- Wenn mit PSK gearbeitet wird, wird das GW in Aggressive Mode arbeiten.
- Der Aggressive Mode verkürzt das Handshake zum Schlüsselaustausch von sechs Pakete auf drei Pakete. Damit gezielte Angriffe auf den PSK möglich.

```
#ike-scan 10.1.1.254 --trans=5,2,1,5 -o
Starting ike-scan 1.2 with 1 hosts
10.1.1.254
IKE Main Mode Handshake returned (1 transforms)
IKE Backoff Patterns:
IP Address No. Recv time Delta Time
10.1.1.254 1 1092956328.817392 0.000000
10.1.1.254 2 1092956330.923392 2.106000
10.1.1.254 3 1092956332.885392 1.962000
10.1.1.254 4 1092956334.833392 1.948000
10.1.1.254 5 1092956336.836392 2.003000
10.1.1.254 6 1092956338.835392 1.999000
10.1.1.254 7 1092956340.844392 2.009000
10.1.1.254 8 1092956344.875392 4.031000
10.1.1.254 9 1092956348.882392 4.007000
10.1.1.254 10 1092956352.866392 3.984000
10.1.1.254 11 1092956356.902392 4.036000
10.1.1.254 12 1092956360.883392 3.981000
10.1.1.254 Implementation guess: Firewall-1 4.1/NG
```





## Angriffe auf IPSec (iii) IKEprobe /VPN-Client

- IKEprobe simuliert einen VPN-Client und versucht ein IKE-Handshake im Aggressive Mode. Es werden alle Parameter geprüft um einen PSK Hash vom GW zu bekommen.
- Sobald dies vorliegt ist es angreifbar.
- Der PSK-Hash wird im Aggressive Mode bereits beim Kontaktversuch eines VPN-Clients übers Netz gesendet.
- Jetzt muss nur noch der PSK-Key errechnet werden.

```
#ikeprobe 10.1.1.254
IKE Aggressive Mode PSK Vulnerability Scanner
Supported Attributes
Ciphers : DES, 3DES, AES-128, CAST
Hashes : MD5, SHA1
Diffie Hellman Groups: DH Groups 1, 2 and 5
IKE Proposal for Peer: 10.1.1.254
Aggressive Mode activated ...
Attribute Settings:
Cipher DES
Hash SHA1
Diffie Hellman Group 1
0.000 3: ph1_initiated(00443ee0, 00384708)
0.010 3: << ph1 (00443ee0, 244)
0.030 3: >> 40
0.030 2: sx_recv_notify: invalid doi
2.532 3: << ph1 (00443ee0, 244)
5.537 3: << ph1 (00443ee0, 244)
8.541 3: ph1_disposed(00443ee0)
(...)
Attribute Settings:
Cipher 3DES
Hash SHA1
Diffie Hellman Group 5
64.551 3: ph1_initiated(00443ee0, 00384708)
64.662 3: << ph1 (00443ee0, 340)
64.692 3: >> 328
64.842 3: ph1_get_psk(00443ee0)
System is vulnerable!!
```





## Angriffe auf IPSec (iv) Cain & Abel / IKE-Parser

- Das PASSwort-Sniffing und –Cracking-Tool Cain & Abel kann bei einem IKEProbe-Lauf den IKE-Verkehr mitlesen
- Mit dem eingebauten IKE-Parser kann der Hash extrahiert werden.
- Mit dem eingebauten Wörterbuch kann versucht werden eine Brute-Force-Attacke durchzuführen.

The screenshot shows the main interface of Cain & Abel. The menu bar includes 'Figure', 'Tools', and 'Help'. The toolbar contains various icons for network analysis. Below the toolbar, there are several tool buttons: 'Network', 'Sniffer', 'LSA Secrets', 'Cracker', 'Traceroute', 'CCDU', and 'Wireless'. The 'Cracker' button is highlighted. Below the tool buttons, there is a table displaying captured IKE traffic.

Timestamp	Responder	Initiator	Identification	R-Cookie	I-Cookie
20/08/2004 - 01:02:53	10.1.1.254	10.1.1.80	□□□P	3EC70D704D1B...	FBD70C2E



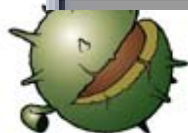


## Angriffe auf IPSec (v) Cain & Abel / IKE-Parser

- Ein Grund für den erfolgreichen Hack sind schwache Passwörter
- Durchprobieren einer Liste mit einer Million Wörter dauert weniger als eine Minute
- Um z.B. alle Kombinationen kleiner Buchstaben eines sechsstelligen Keys durchzuprobieren, benötigt ein PC (P4) mit 1,2 Ghz nur ca. zwei Stunden.
- Doch zwei stellen mehr erhöhen die Rechenzeit auf 55 Tage.
- Sind zusätzlich Großbuchstaben und Zahlen erlaubt ist eine Rechenzeit von 148 Jahre notwendig.

The screenshot shows the main interface of Cain & Abel. The menu bar includes 'File', 'Tools', and 'Help'. The toolbar contains various icons for network analysis. Below the toolbar is a row of tool buttons: Network, Sniffer, LSA Secrets, Cracker, Traceroute, CCDU, and Wirele. The main display area shows a table with the following data:

Identification	PSK	R-Hash	INonce+RNonce	PacketBytes
□□□□	password	C49E81F503D8...	11E3AB76C98346D...	442E1FB63FFF...





## IPSec: Bekannte Probleme bei Remote Access (i)

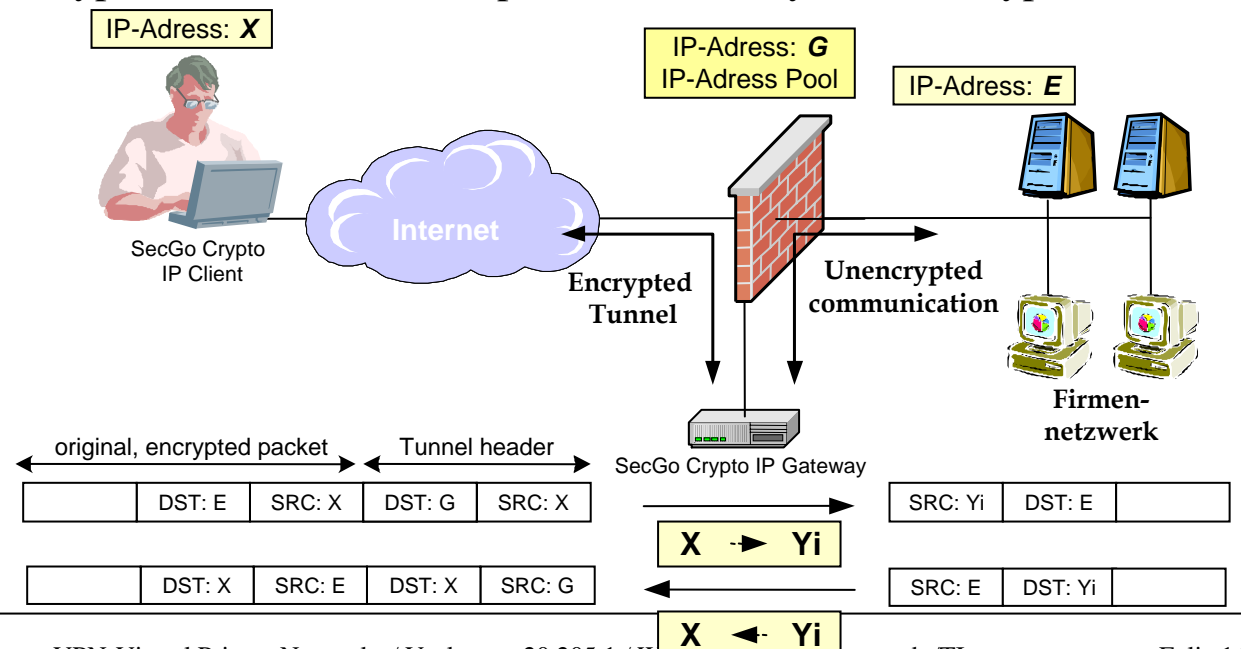
- Falls preshared Keys, Main Mode und dynamische IP-Adressen genutzt werden, müssen die preshared Keys für alle IPSec-Clients gleich sein.
- IPSec unterstützt nicht die traditionellen Authentifizierungsmethoden beim Fernzugriff wie Radius (PAP/CHAP), Secure-ID oder OTP.
- Es können offene Verbindungselemente verbleiben, wenn IPSec-Clients ihre PPP-Verbindung unterbrechen und ihre eigene SA löschen.
- Es darf zwischen IPSec-Client und VPN-Gateway kein IP-NAT-Verfahren eingesetzt werden
- In umfangreichen Remote-Access-Installationen ist die Konfig. und Admin der SPD-Einträge auf Clientseite als auch im Zentralsystem sehr Zeit aufwendig





## IPSec: Bekannte Probleme beim Remote Access (ii)

- Standard IPSec Technologie versagt bei dynamischer Port Vergabe und beim NAT.
- IP NAT-Traversal ist für eine point-to-point IPSec Verbindung die Problemlösung.
  - Es kann mit NAT Traversal eine sichere Verbindung aufgebaut werden, die durch Firewall-Systeme und anderen VPN-Devices hindurchgeht. Es wird dazu ein spezieller Client (SecGo Crypto IP-Client) und ein spezielles Gateway (SecGo Crypto IP-Gateway) erforderlich



# Übungen

---



1. Frage: Wie wird bei IKE ein „Man-in-the-middle“ Angriff unterbunden?
2. Frage: Was ist der Unterschied zwischen einer SAD und SPD?
3. Worin unterscheiden sich Aggressive Mode und Main Mode?
4. Warum ist der Main Mode zu bevorzugen?
5. Frage: Wie kann/muss ein IPSEC-Tunnel zwischen zwei Gateways aussehen, wenn von „außen“ die Payload nicht sichtbar sein darf, die Integrität der Payload als auch der des Headers sichergestellt sein muss?





# Literatur

---

- <http://www.tu-darmstadt.de/vv/20.205.1>.
- **Huston G.: Internet Performance Survival Guide, QoS Strategies for Multiservice Networks, ISBN 0-471-37808-9**
- **Comer, 1995: Internetworking with TCP/IP Vol. I., ISBN 0-13-216987-8**
- **Davis, C.R.: IPSec-Tunneling im Internet, mitp-Verlag, 1. Auflage 2002, ISBN 3-8266-0809-7.**
- **Aurand, A.: Sicherheit in Cisco- und Windows-2000-Netzwerken, Installation und Troubleshooting von IPSec in der Praxis, Addison-Wesley Verlag 2001, ISBN 3-8273-1930-7. (Teil 2- IPSec-Architektur)**
- **Schneier, B.: IPSec an critical description**
- **Liste der RFC die für IPSec geschrieben wurden (Stand 2003):**  
1191, 1321, 1421, 1422, 1423, 1424, 1701, 1827, 1728, 2093, 2094, 2104, 2246, 2311, 2312, 2315, 2394, 2395, 2401, 2403, 2404, 2405, 2408, 2409, 2410, 2411, 2412, 2437, 2451, 2507, 2510, 2511, 2522, 2523, 2535, 2549, 2559, 2560, 2585, 2627, 2631, 2633, 2660, 2661, 2828, 2845, 2857, 2888, 2898, 2931, 2944, 2945, 2985, 2986, 3007, 3008, 3039, 3051, 3526, 3554, 3566, 3602.

