

VPN - Grundlagen, Technologien, Implementierungen⁰

- Anforderungen
- TCP/IP
- Methoden
- Topologien
- kryptographische Verfahren
- Applikationen
- IP-Tunnel vs Ethernet-Bridging

⁰Folien auf <http://www.kyb.tuebingen.mpg.de/~renner/>

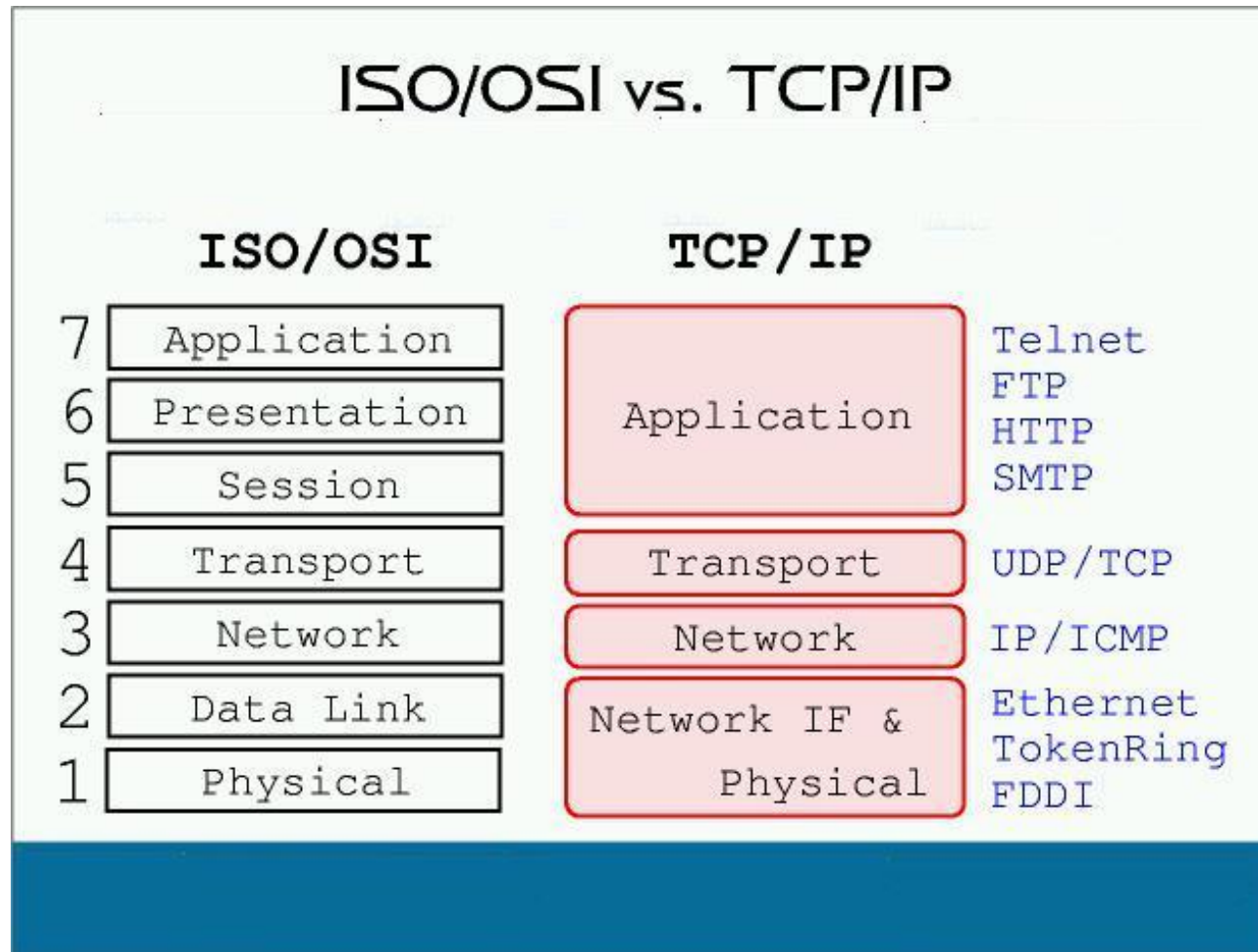


Anforderungen

- Nicht belauschbar (Selbstzweck)
- Vertraulichkeit: Angreifer darf Inhalt nicht erfahren
- Authentizität: keine Daten unter falschem Namen einschleusen
- Integritätssicherung: Nachricht nicht verändern, nichts wiederholen, nichts einfügen
- Verfügbarkeit: Robust gegen DoS Angriffe



TCP/IP



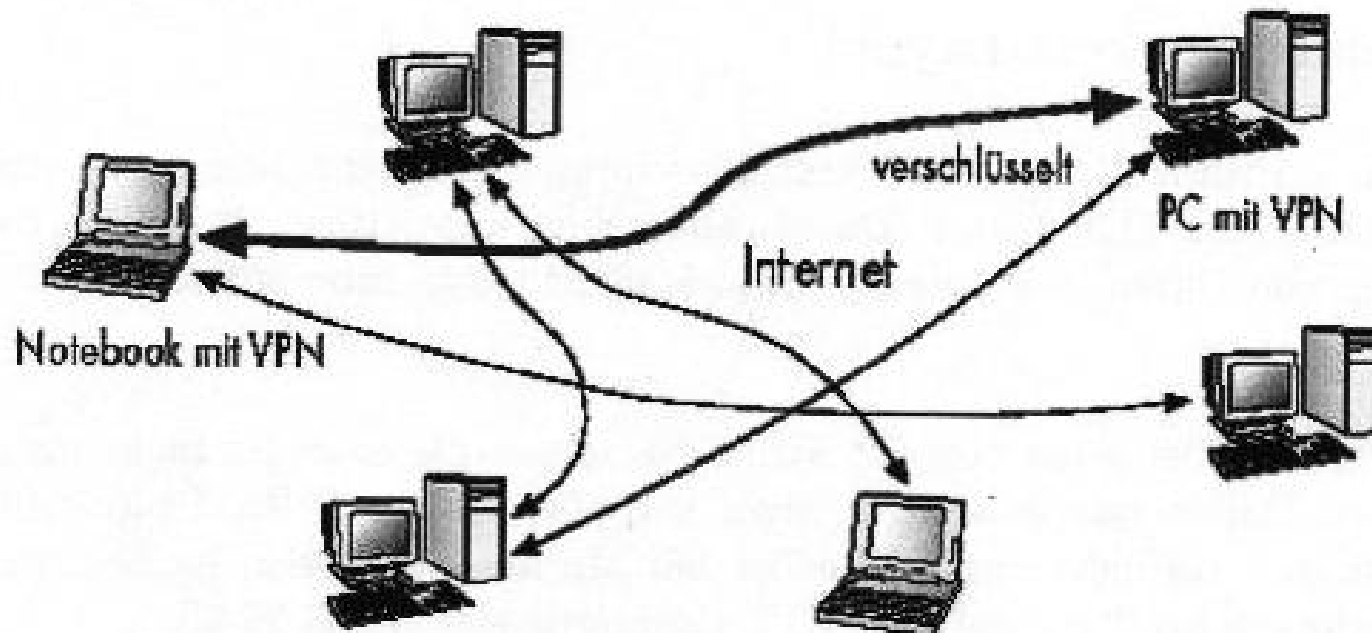
Methoden

- Tunnelbare Pakete
 - IP (TCP, UDP)
 - IPX
 - NetBUI
 - Etherframes
- Protokoll
 - UDP
 - TCP
 - GRE
- Kryptographische Verfahren
 - Stromchiffre (RC4)
 - Blockchiffre (3DES, IDEA)
 - symmetrische/asymmetrische Verfahren

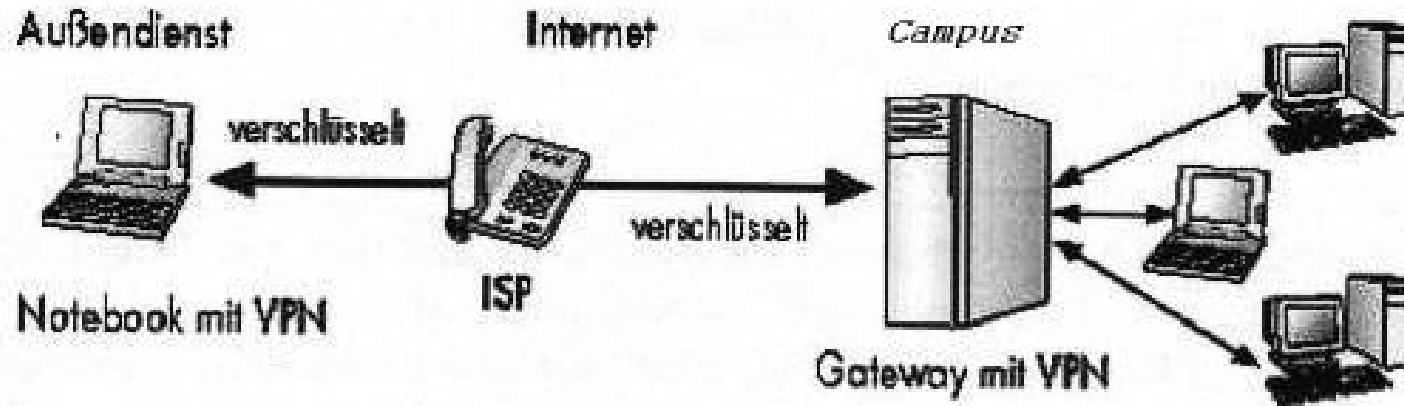


Topologien

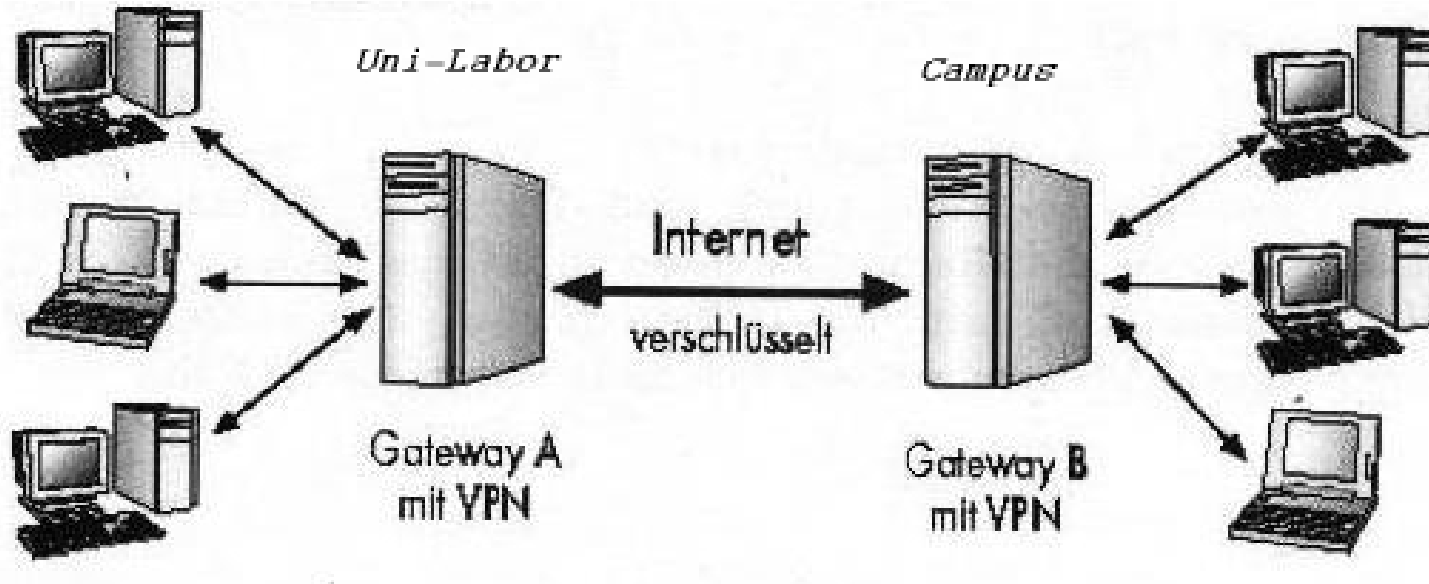
- Client to Client



- Client to Network



- Network to Network



kryptographische Verfahren

Name	Art	Schlüssellänge	Geschwindigkeit	Sicherheit	Anwendung
DES	Block	56Bit	Hardware:hoch Software:niedrig	Aufwändig angreifbar	früher verbreitet
3DES	Block	112Bit	Hardware:hoch Soft.:sehr niedrig	kein Angriff bekannt	verbreitet
IDEA	Block	128Bit	schneller als DES	sehr hoch	verbreitet
RC4	Strom	variabel	Software:hoch	-	z.B. SSL
A5	Strom	64Bit	Hard.:sehr hoch	gebrochen	GSM-Handys
Blowfish	Block	variabel	hoch	kein Angriff bekannt	OpenSource
Twofish	Block	variabel	hoch	kein Angriff bekannt	
RSA	-	1024/2048	niedrig	bisher sicher	PublicKey-Ver
Diffie-Hellmann	-	keine	sehr niedrig	bisher sicher	z.B. IPsec, ssh



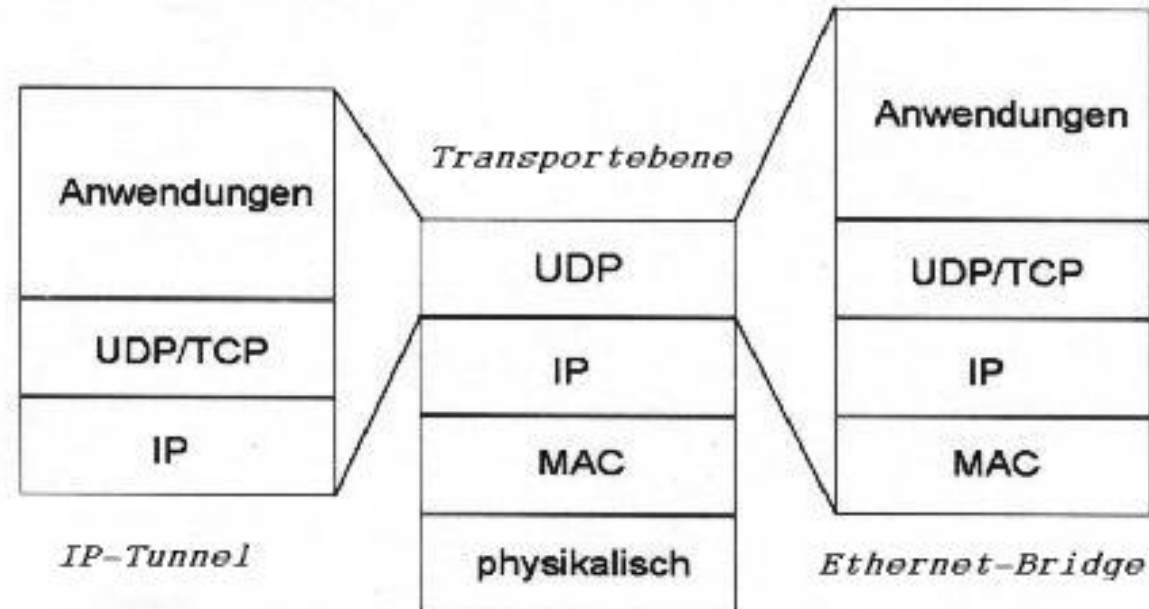
Applikationen

Applikation	Verschlüsselung	User/Kernelspace	Protokoll	OS
FreeS/WAN †	IPsec	Kernel (Patch)	AH, ESP, UDP	Linux, Windows*
OpenVPN	TLS	User (tun)	UDP (TCP)	alle ¹
tinc	Blowfish	User (tun)	UDP (+TCP)	Linux, Solaris, MacOS X
Cipe †	Blowfish/IDEA	Kernel (Modul)	UDP	Linux, Windows2000
PPTP	RC4	Kernel (Patch)	GRE	alle ¹
L2TP-VPN	IPsec	?	UDP	Linux, Windows*
pppssh	SSL	Userspace (ppp)	TCP	alle ¹
Cisco	IPsec/WebVPN	Kernel (Modul)	UDP	Linux, Solaris, MacOS X, Win
Netgear	3DES	Kernel (Modul)	UDP	alle ¹

¹Windows2000, WindowsXP, Linux, *BSD, MacOS X



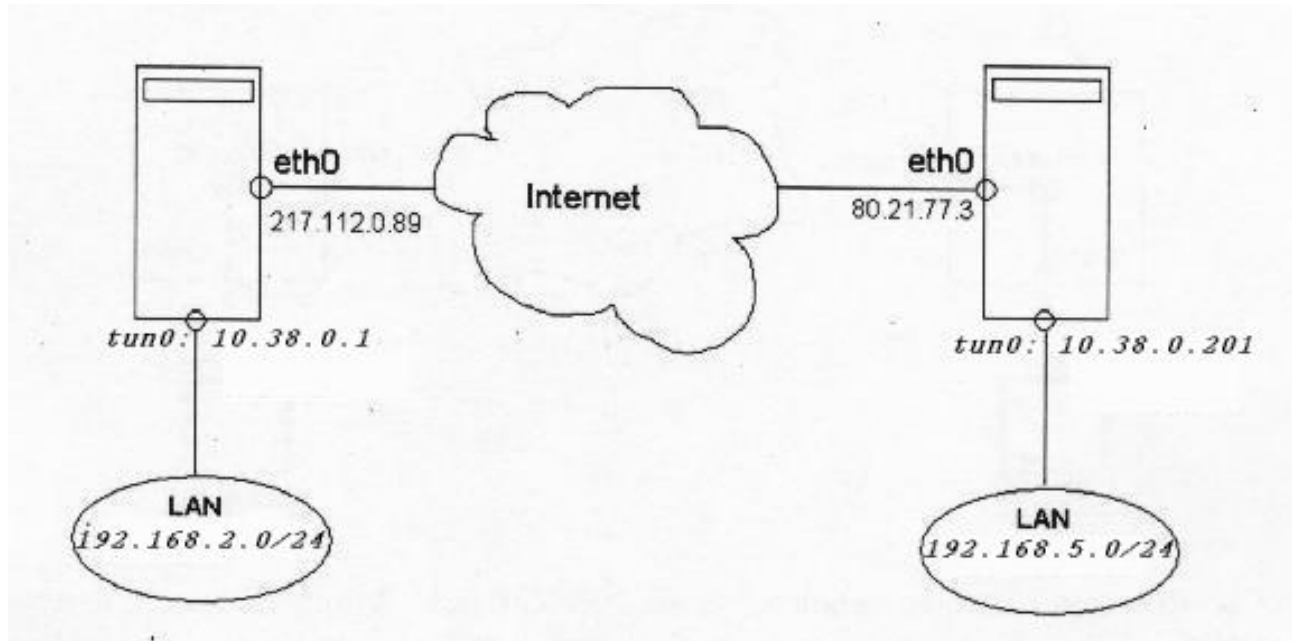
IP-Tunnel vs Ethernet-Bridging



Im IP-Tunnel nur IP-Pakete (TCP, UDP)
Durch die Etherbridge alle Etherframe Pakete (IP, IPX, NetBUI)



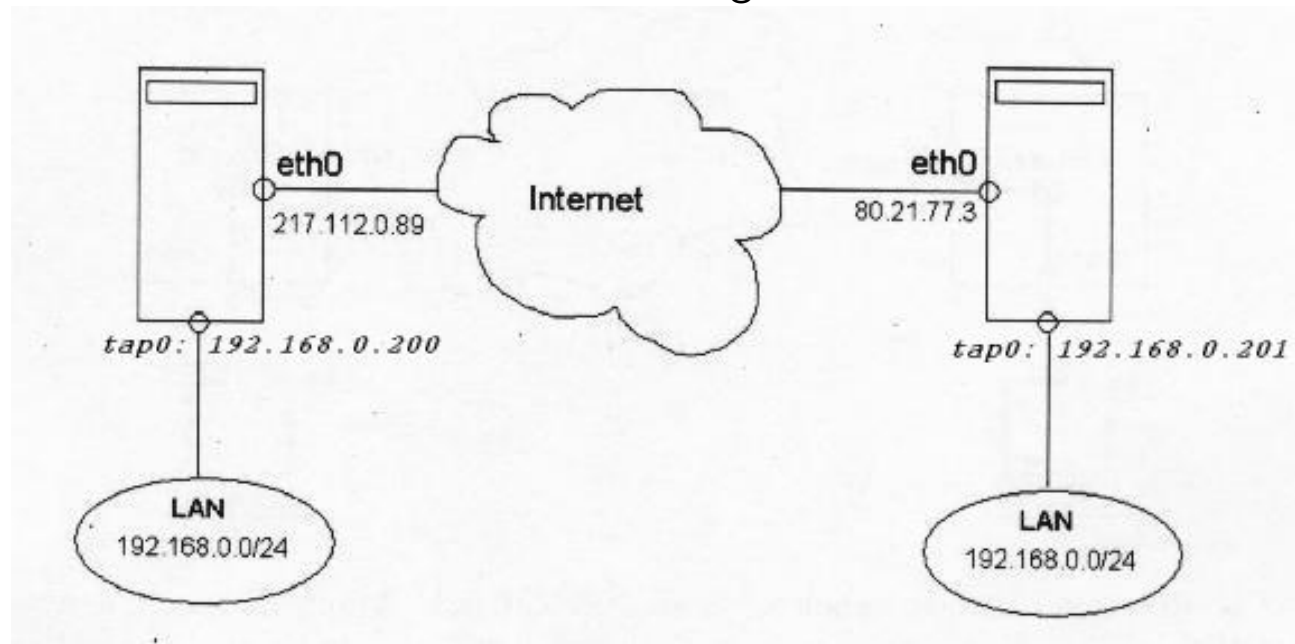
- IP-Tunnel



z.B. mit cipe, IPsec, pptp



• Etherbridge



z.B. mit OpenVPN, pptp, tinc

