Sichere Einbindung von WLAN-Netzen in eine Forschungsumgebung

Ralph Niederberger
Egon Grünter
Forschungszentrum Jülich GmbH
Zentralinstitut für angewandte Mathematik
John von Neumann Institut für Computing
R.Niederberger@fz-juelich.de
E.Gruenter@fz-juelich.de

Inhalt

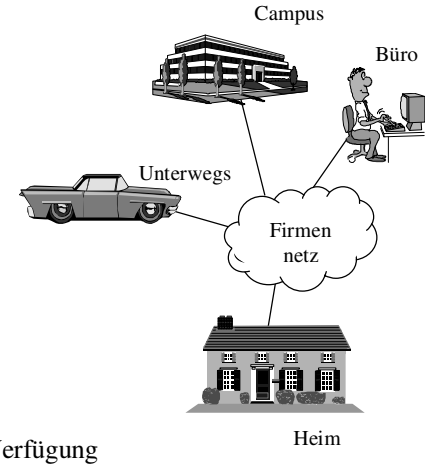
- WLAN Motivation
- Wireless LAN Grundlagen
- Probleme und Besonderheiten in Forschungsnetzen
- Allgemeine Sicherheitsgefahren und Lösungen
- Sicherheitsfeatures in 802.11b Netzen
- WLAN Konzept des Forschungszentrums Jülich
- Zusammenfassung

WLAN-Motivation

WLAN-Motivation

- Informationszeitalter ➔
  Information, Kommunikation, Mobilität besonders wichtig
- Task-Force orientiertes Arbeiten ➔
  wechselnde Gesprächspartner und Orte.
- Mitarbeiter oft in
  - Besprechungen und Vorträgen,
  - im Netzwerk- und Rechnerraum
- Abgeschnitten von Informationen,
  aber aktuelle Informationen notwendig

Ziel muss sein,
an beliebigem Ort steht gleiche technologische Umgebung zur Verfügung



WLAN-Grundlagen

Vor- und Nachteile

Besonderheiten

Unterschiede zu kabelgebundenen Netzen

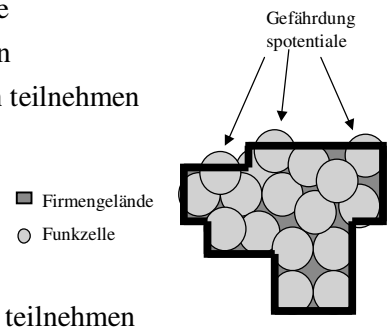
Wireless LAN

Drahtlose Netze nach IEEE Standard 802.11b werden als **Wireless Local Area Networks** bezeichnet

- Funktechnik im 2,4 GHz Frequenzbereich
- Weltweit eingesetzte Lösung
- Übertragungsrate 11 Mb/s (shared medium)
- Genehmigungsfrei, daher aber auch störanfällig
- Abhören derzeit noch straffrei
- Anbindung an kabelgebundenes Netz über Access Points

Vor-/Nachteile von Wireless LANs

+ inzwischen Plug & Play Technologie
+ ad hoc Netze z.B. bei Besprechungen
+ jeder kann leicht an Kommunikation teilnehmen



Positiv

Negativ

– jeder kann leicht an Kommunikation teilnehmen
– nicht mehr kontrollierbar, wo genau kommuniziert wird
– bei Bereichsüberschreitung auch externe Teilnehmer
– bei Gatewaykonfiguration Nebenpfade zum Firewall möglich
– Performance-Engpässe (11 Mb/s shared, effektiv 5,7 Mb/s)

Besonderheiten von WLANs

- Benutzer versuchen unangemeldet das Netz zu benutzen (Konnektivität)
- sie können auch ohne zugewiesenen Anschlussport teilnehmen / stören,
- sie können untereinander auch ohne Access Point kommunizieren (Ad Hoc)
- sie kennen meist nicht die Randbedingungen für Wireless LANs
- nicht WLAN Geräte können die Kommunikation stören,
  ohne dass dies den Betreibern der Geräte bekannt ist (Mikrowelle,...)
- es ist nicht bekannt, wieviele Teilnehmer gleichzeitig das WLAN benutzen wollen (Mengenproblem)

Unterschiede WLAN und kabelgebundenes Netz

Kabelgebundene Netze

- meist geswitchte Infrastruktur
- An jeder Anschlussdose ein Teilnehmer
- Remote-Netzmanagement-System kann Störungsquelle lokalisieren und sperren

Funknetze

- „Busstruktur“ in der Funkzelle
- Viele Teilnehmer je Funkzelle
- Teilnehmer lokalisierbar auf Funkzellenbasis (Ortung nur mit Spezialgeräten)
- Sperrung auf Funkzellenbasis möglich, Störsignale können allerdings nicht herausgefiltert werden

Probleme / Besonderheiten in Forschungsumgebungen

Forschungsnetze ...

- nutzen häufig neuartige Techniken
- haben oft leistungsstarke Rechner
- betreiben teure Ressourcen

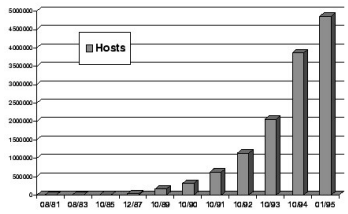
➔ **attraktives Ziel für Hacker**

- Netze notwendig offen für Kooperationen + externe Partner
- hohe Anzahl von „Nichtmitarbeitern“ im Netz
  - Partnerfirmen, Gastwissenschaftlern
  - Gastvorträge, Aus- und Weiterbildung auch externer
- Nutzung neuer Medien
  - Multimedia, Web, E-Mail, Präsentationen (auch remote oder interaktiv)

➔ Offenes Netz ➔ **erhöhtes Gefährdungspotential**

Allgemeine Sicherheitsgefahren und Lösungen

Gefahren aus dem Internet



Internet worm

virus

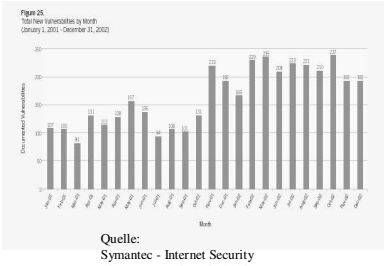
Schäden pro Jahr über 12 Mrd. US $

sendmail

Bot Killer 2000

Netbus

ping of death



Quelle:
Symantec - Internet Security
Threat Report 3, Feb. 2003

Antwort der Unternehmen

grosse Investitionen in

- Firewalls, Packet-Filter, Personal Firewalls
- Intrusion Detection Systeme
  - Network based IDS
  - Host based IDS
  - Vulnerablity Assessment - + Penetration Testing Systems
  - lokale und zentrale Virenfilter
- Aufwendungen für Sicherheit in Hard/Software- und Personal

Das heisst aber ....

auch neue Komponenten müssen

- einen ausreichenden Sicherheitsstandard besitzen
- bestehende Sicherheits-Policies respektieren
- so installiert werden, dass keine neuen Gefahren entstehen

Im Mittelpunkt dieser Überlegungen steht i.A. das kabelgebundene Netz

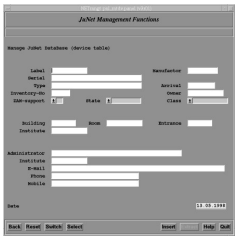
- am Netz angeschlossene Rechner müssen sicher sein
- die Administratoren angeschlossener Rechner sind bekannt
  (und !! ?? vertrauenswürdig ?? !!)

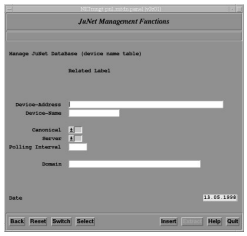
Sicherheitsgrundprinzipien in Rechnernetzen

Auch in sich häufig ändernden Umgebungen ...

- sollte zu jedem angeschlossenen IT-System ein Standort und ein Ansprechpartner sowie Vertreter benannt sein
- Kontaktinformationen, wie E-Mail und Tel.-Nr., dieser Personen bekannt sein

Realisierung durch IP-Verwaltungstool





Realisierung für WLAN recht aufwendig,

➔ **daher vereinfachtes Vorgehen notwendig**

Sicherheitsfeatures in IEEE 802.11b

Sicherheitsfeatures in IEEE 802.11b

IEEE 802.11b bietet verschiedene Sicherheits-Features

- Service Set Identifier (SSID)
- Open und Shared- Key Authentication
- Wired Equivalent Privacy (WEP) Protocol

Jedes dieser Features bietet unterschiedliche Sicherheitslevel

Sicherheitsfeatures in IEEE 802.11b

- **Service Set Identifier (SSID)**
- Open und Shared- Key Authentication
- Wired Equivalent Privacy (WEP) Protocol

Service Set Identifier SSID

Service Set Identifier ist ein „Dienst“-Bezeichner

Zwei Betriebsmodi möglich

Als Netzwerk-Name:

- Access-Point „broadcasted“ SSID
- Client verbindet sich nur mit Access-Points mit übereinstimmender SSID

Als Preshared-Key:

- Access-Point „broadcasted“ SSID nicht
- Client verbindet sich mit Access-Point und weist sich mit SSID aus

! Da die Management-Frames nicht verschlüsselt übertragen werden, ist dies kein Sicherheitsfeature

➔ Software zum Mitlesen frei verfügbar !

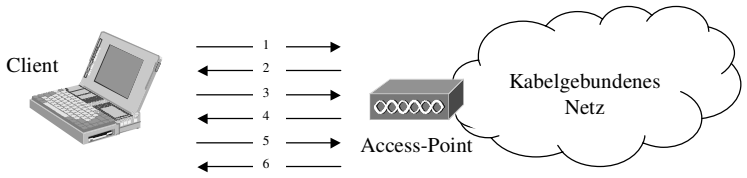
Sicherheitsfeatures in IEEE 802.11b

- Service Set Identifier (SSID)
- **Open und Shared- Key Authentication**
- Wired Equivalent Privacy (WEP) Protocol

Open und Shared-Key Authentication (1)

Client Authentication besteht aus den folgenden Aktionen:

1. Client „broadcasted“ einen „Probe-Request“ auf jedem Kanal
2. Erreichbare Access-Points antworten mit einem „Probe-Response“
3. Client sendet dem best-erreichbaren AP (Signalstärke) Authentication Request
4. Der Access-Point antwortet mit einem Authentication-Response
5. Bei erfolgreicher Antwort sendet Client einen Association-Request
6. Access-Point antwortet mit Association-Response



Open und Shared-Key Authentication (2)

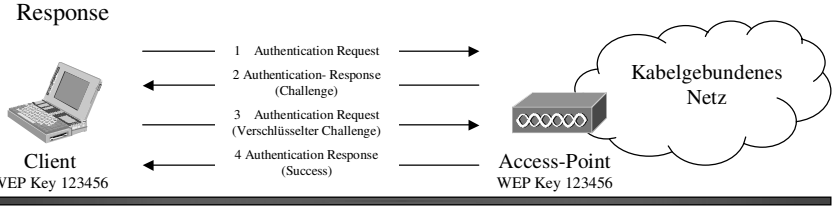
Open-Key-Authentication

Als Key wird eine Station-Id oder z.B. Hardware-Adresse gesendet

Shared-Key-Authentication

Client muss einen statischen WEP Key konfigurieren

1. Client sendet Authentication-Request an Access Point und fordert Shared-Key-Authentication an
2. Access-Point antwortet mit Authentication-Response und zufälligem Challenge Text
3. Client verschlüsselt Challenge Text mit WEP Key und sendet Ergebnis mit dem Authentication-Request mit
4. Access-Point entschlüsselt Request und sendet, falls erfolgreich, Authentication-Response



Open und Shared-Key Authentication (3)

Shared-Key-Authentication Probleme

Client muss einen statischen WEP Key konfigurieren, d.h. ...

- jeder Teilnehmer muss diesen kennen
- jeder Gast muss diesen kennen
- ständige Änderung sehr aufwendig
- Spricht sich schnell herum
- Viele Attacken basieren auf Möglichkeit der Ermittlung eines Schlüssels durch Mitschneiden eines verschlüsselten Textes bei bekanntem Ursprungstext
- WEP-Algorithmus bereits öfters geknackt

Sicherheitsfeatures in IEEE 802.11b

- Service Set Identifier (SSID)
- Open und Shared- Key Authentication
- **Wired Equivalent Privacy (WEP) Protocol**

Wired Equivalent Privacy (WEP) Algorithmus

- WEP wird benutzt um Verkehr zu verschlüsseln (eavesdropping)
- WEP wird benutzt um unauthorisierten Zugriff zum WLAN zu verhindern (nicht Ziel von 802.11)
- WEP nutzt shared secret key zwischen WLAN-Client und Access Point
- Standard legt nicht fest wie Key vereinbart wird (meist einer-für-alle)
- WEP benutzt RC4 Verschlüsselungs-Algorithmus
- Generierung eines Key-Streams aufgrund shared secret key (mittels 24-bit-Initialisierungsvector)
- Sender XOR's einen Text mit Key-Stream, Empfänger macht Vorgang rückgängig
- Dieses Verfahren erlaubt verschiedene Angriffsarten

WEP Angriffsattacken

Angriffsattacken, welche die Sicherheit von Systemen in WLANs unterlaufen

- Passive Attacken zur Verkehrsentschlüsselung auf Basis statistischer Analyse
- Aktive Attacken durch Einfügen neuen unauthorisiertem Verkehrs mobiler Stationen aufgrund bekannten Ursprungstextes
- Aktive Attacken zur Verkehrsentschlüsselung durch Täuschung des Access Points
- Dictionary-Attacken, die Realtime Entschlüsselung des Verkehrs zulassen, nach 24-Stunden Analyse des Verkehrs

Analysen bestätigen, dass dies mit kostengünstigem Off-The-Shelf-Equipment möglich ist.

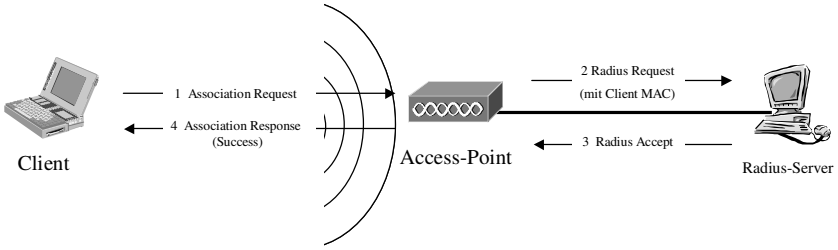
Empfehlung: Sicherheit darf nicht alleine auf WEP basieren.

Aus: N.Borisov, I.Goldberg, D.Wagner, http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html

MAC Address Authentication

- MAC Address Authentication nicht standardisiert in IEEE 802.11b, aber vielfach unterstützt (z.B. Cisco)
- Hardware-Adresse des Clienten wird überprüft (z.B. RADIUS-Server)
- Ergänzt Open /Shared-Key-Authentication
- Verhindert Zugriff auf WLAN für unauthorisierte

Sicherheit nicht gänzlich gewährleistet (MAC-Adress-Fälschung möglich)



WLAN Konzept des Forschungszentrums Jülich

WLAN Konzept des Forschungszentrums Jülich

- weitgehend Switch-basierte Infrastruktur im FZJ
- VLANs unterteilen physikalische Struktur in mehrere logisch getrennte Netze
- VLAN-Aufteilung bietet Trennung zwischen kabelgebundenem und funkbasiertem Netz
- WLAN ist eines dieser Netze (Ethernet-Seite der Access-Points)

➔ Institute ohne Switch-basierte Infrastruktur können nicht am WLAN teilnehmen

WLAN Konzept des FZ-Jülich (2)

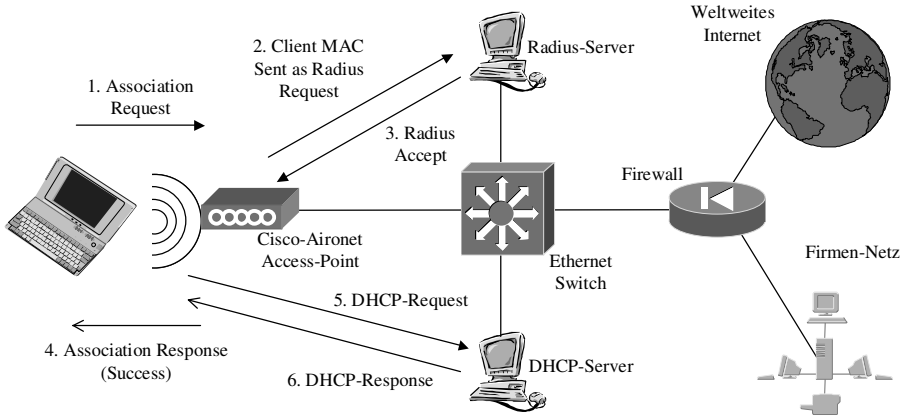
- Anschluss der WLAN Teilnehmer über zentral beschaffte, installierte und verwaltete Access-Points
- nur Geräte der Cisco Aironet Serie, weil ...
  - gut funktionierend und kompatibel zu LAN-Adaptern anderer Hersteller
  - passend zu bisheriger Infrastrukur
  - Unterstützung von MAC-Address-Authentication
- WLAN als Ergänzung, **nicht Ersatz**, der bestehenden Infrastruktur
- alle Regelungen des kabelgebundenen Netzes auch für WLAN gültig
  - Sysadmin, aktuelle Patches, Virenfilter, Personal Firewall, nichtbenötigte Dienste deaktiviert, etc. ...
- kein Routing erlaubt, d.h. gleichzeitig installierte Eth-Adapter deaktiviert
- WLAN als externes Netz definiert und konfiguriert (VLAN, Firewall)

WLAN Konzept des FZ-Jülich (3)

- WLAN Teilnehmer erhalten private IP-Adressen gemäß RFC1918
- dadurch disjunkter Adressbereich zwischen kabelgebundenem und funkbasiertem Netz
- erleichtert Sicherheitskonfiguration des Firewalls und der Endsysteme (lokales Netz sicher - andere unsicher)
- dynamische Adresszuweisung (DHCP)
  - Name, Domain, Netzmaske, Gateway, Name- / NTP-Server
- Mitarbeiter und Gäste (über betreuenden Mitarbeiter) stellen elektronischen Antrag auf Zugang (MAC-Adresse und E-Mail)
  - schnell, weitgehend automatisch, einfach, Sysadmin bekannt
- Zugang Unbefugter wird dadurch erschwert (MAC-Address-Authentication)
- Logging von Radius-Server-Info, Zugriffszeit und vergebene IP-Adresse ermöglicht Sysadmin-Identifikation

WLAN-Registrierung

WLAN-Netzwerkanmeldung



WLAN-Zugriff auf FZJ-interne Ressourcen

- Firewall des FZJ schützt vor Angriffen von externen Rechnern aus

➔ Firewall des FZJ schützt vor WLAN

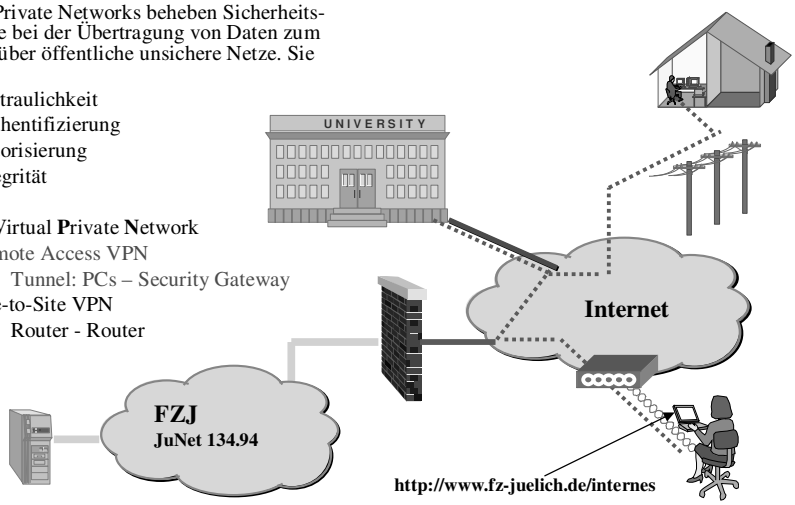
➔ WLAN-Teilnehmer können nicht auf interne Ressourcen, wie Drucker, Mail- und Fileserver, Computeserver etc., zugreifen

Zur Behebung der Problematik werden VPNs genutzt

- VPNs nutzen kryptographische Verfahren zum Aufbau sicherer Verbindungen

Definition von Virtual Private Networks

- Virtual Private Networks beheben Sicherheits-probleme bei der Übertragung von Daten zum Intranet über öffentliche unsichere Netze. Sie bieten
  - Vertraulichkeit
  - Authentifizierung
  - Autorisierung
  - Integrität
- VPN = **V**irtual **P**rivate **N**etwork
  - Remote Access VPN
    - Tunnel: PCs – Security Gateway
  - Site-to-Site VPN
    - Router - Router



VPN Protokolle - Überblick

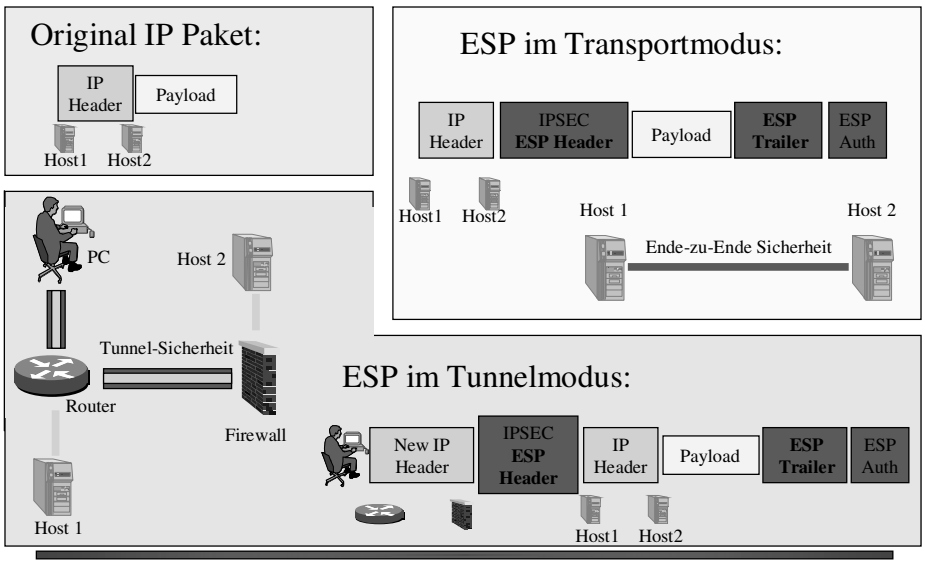
OSI-Layer:	Protokolle:	Plattformen:	Geräte:
Application	ssh (scp, sftp), https, s/mime	*UNIX,Windows*	
Presentation			
Session			
Transport	Secure socket layer (TCP)	*UNIX, Windows*	
Network	~~PPTP~~, L2TP, **IPSEC**	*UNIX, Windows 2000/XP*	
Data Link	~~MPPE~~, ~~WEP~~	*LINUX-, Windows-PPP*	
Physical			

WEP	=	Wired Equivalent Privacy
MPPE	=	Microsoft Point-to-Point Encryption
PPTP	=	Point to Point Tunneling Prototocol
L2TP	=	Layer 2 Tunneling Protocol (over IPSEC)
IPSEC	=	**Internet Protocol Security**

VPN-Protokoll IPSEC

- **IPSEC** = Internet Protocol Security
- unterstützt in IPv6 und IPv4
  - Windows 2000, AIX, Solaris, Tru64 UNIX, LINUX, u.a.
  - CISCO VPN Lösungen, z.B. VPN 3000 Client
- Internet-Standard RFC 2401-2412, RFC 2451
- IPSEC-Protokolle
  - IKE = Internet Key Exchange
  - AH = Authentication Header (Protocol Number 51)
  - **ESP = Encapsulating Security Payload (Protocol Number 50)**

IPSEC ESP



WLAN-Zugriff auf FZJ-interne Ressourcen (2)

Wichtige Eigenschaft von VPNs

➔ Zuordnung einer IP-Adresse im geschützten IP-Tunnel

➔ hier wird eine „offizielle“ IP-Adresse des FZJ zugewiesen

Damit sind VPN-Benutzer beim Zugriff auf zentrale Server internen Benutzern gleichgestellt.

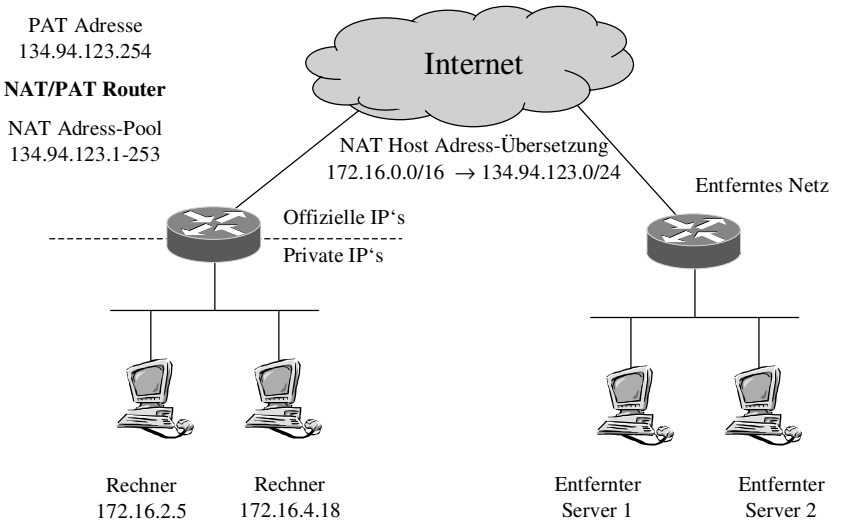
Cisco VPN-Client-Software derzeit verfügbar für

- Windows 95 / 98 / Me / NT / 2000 /XP
- Linux (x86) mit Kernelversion 2.2-2.4
- Solaris OS Vers. 2.6+
- Macintosh OS X Version 10.1.0+

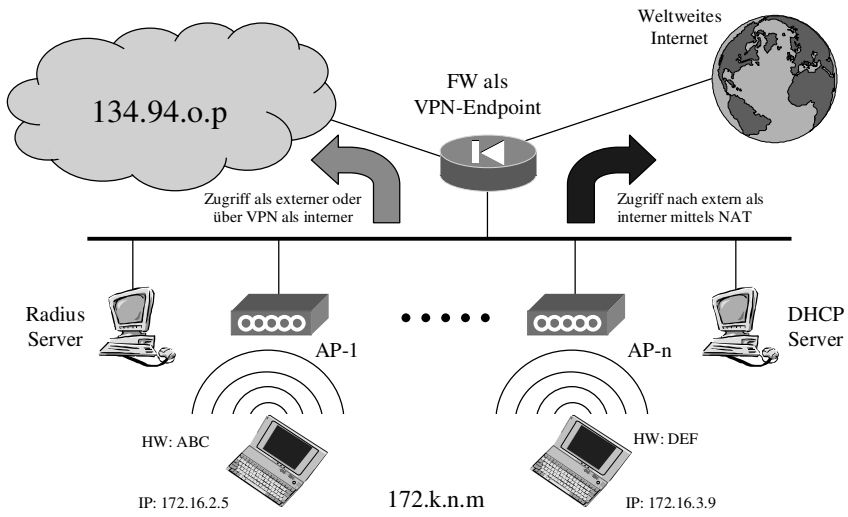
WLAN-Zugriff auf weltweites Internet

- Problematisch beim bisherigen Ansatz sind die privaten Adressen nach RFC1918
- IP-Pakete mit privaten Adressen werden im Internet nicht weitergeleitet
- Adressübersetzung notwendig
  - Network Address Translation
  - Port Address Translation
- Bei jedem Zugriff auf externe Ressourcen wird eine dynamische Adressübersetzung gestartet, daher nur wenige „offizielle“ Adressen notwendig

NAT / PAT - Adressübersetzung



Allgemeine Übersicht WLAN-Einbindung



Sicherheitsgrundprinzipien im WLAN

WLAN Komponenten

- respektieren die bestehenden Sicherheits-Policies
- sind so integriert, dass keine neuen Gefahren entstehen
- bieten mit der zusätzlichen VPN Kommunikation einen ausreichenden Sicherheitsstandard

Systemadministrator aufgrund der Hardware-Adress-Registrierung bekannt

➔ bei Kommunikationsstörungen „Verursacher“ schnell benachrichtigt

Bei Sicherheitsproblemen kann „Verursacher“ auch später ermittelt werden

➔ Logging Infos von

Radius- + DHCP-Server, VPN-Concentrator + Firewall

Zusammenfassung

Die vorgestellte Integration eines WLAN in eine Forschungsumgebung

- stellt weitgehend sichere und flexible Lösung dar
- Konzeption als externes Netz bietet Schutz vor unberechtigtem Zugriff
- Nutzung privater Adressen erhöht Sicherheit und spart Adressraum
- MAC-Address-Authentifizierung erschwert Zugang Unberechtigter
- elektronische Registrierung erlaubt AdHoc-Nutzung 24 h / 7 d / w
- VPN erlaubt den Zugriff Berechtigter auf das lokale Netz
- NAT / PAT- Adress- Übersetzung ermöglicht externe Kommunikation

Sichere kostensparende und weitgehend uneingeschränkte Nutzung der Unternehmensressourcen durch berechtigte Personen aus dem WLAN gewährleistet.

Fragen

? ? ?