FORSCHUNGSZENTRUM JÜLICH GmbH
Zentralinstitut für Angewandte Mathematik
D-52425 Jülich, Tel. (02461) 61-6402

Interner Bericht

Sichere Einbindung von WLAN-Netzen in eine Forschungsumgebung

Ralph Niederberger, Egon Grünter

FZJ-ZAM-IB-2003-01

Februar 2003

(letzte Änderung: 04.03.2003)

Preprint: DFN-CERT publications, Hrsg.: Rolf Schaumburg, Marco Thorbrügge
10. DFN-CERT/PCA Workshop „Sicherheit in vernetzten Systemen“,
ISBN 3-8330-0097-X

Sichere Einbindung von WLAN-Netzen in eine Forschungsumgebung

Ralph Niederberger
Egon Grünter
Forschungszentrum Jülich GmbH
Postfach
52425 Jülich
R.Niederberger@fz-juelich.de
E.Gruenter@fz-juelich.de

1 Einführung

Rechner, Daten und Datennetze stellen in einem Unternehmen einen großen Wert dar, dessen Schutz besonderer Aufmerksamkeit bedarf. Hierzu investieren diese Unternehmen große Geldbeträge in Firewalls, Intrusion-Detection-Systeme, Viren-Filter und weitere Sicherheitssoft- und Hardwaresysteme, um die Gefahr eines unberechtigten Zugriffs auf diese Ressourcen und des Einschleusens von Viren, Würmern und Trojanischen Pferden zu verhindern.

Alle Nutzer und Betreiber von Rechnern und Datennetzen müssen sich dieser Gefahren bewusst sein und entsprechend verantwortungsvoll verhalten. Es müssen Vorkehrungen getroffen werden, dass alle am Netzbetrieb beteiligten Komponenten entsprechend ihres Bedarfs abgesichert werden.

In den meisten Fällen steht im Mittelpunkt dieser Schutzbemühungen das kabelgebundene Firmennetzwerk. Die mobile Kommunikation, insbesondere Wireless Local Area Networks (WLANs) deren Bedeutung in allen Bereichen des öffentlichen Lebens zunimmt, nutzt nicht nur eine gesonderte Infrastruktur, sondern bedient sich der Luft als Übertragunsmedium. Dies erfordert besondere Vorkehrungen, damit alle am Netzbetrieb beteiligten Komponenten entsprechend ihres Bedarfs gesichert werden können.

Der vorliegende Bericht beschreibt die Einbindung eines Wireless LAN in die bestehende Netzwerkarchitektur des Forschungszentrums Jülich unter besonderer Berücksichtigung der IT-Sicherheit.

2 Generelle Probleme von WLANs

Mobile Kommunikation ist in der Informationstechnik von großer Bedeutung. Der IEEE 802.11b Standard, der im September 1999 vom Institute of Electrical and Electronic Engineers verabschiedet wurde, beschreibt die Grundlagen eines drahtlosen lokalen Netzes. Drahtlose Netze nach dem IEEE 802.11b Standard werden auch als Wireless Local Area Networks (WLANs) bezeichnet, welche auf Funktechniken basieren, die im genehmigungsfreien 2,4-GHz-Bereich Übertragungsraten von 11 Megabit pro Sekunde erreichen.

Daraus ergeben sich erste Einschränkungen für den Betrieb: Im genannten Frequenzbereich dürfen Funknetze ohne Genehmigung betrieben werden, so dass sich benachbarte Netze

grundsätzlich gegenseitig stören können. Ein daraus resultierendes "Abhören" des benachbarten Netzes zieht derzeit keine strafrechtlichen Konsequenzen nach sich [1].

Aus sicherheits-technischer Sicht stellt eher das Kommunikationsmedium Luft ein Problem dar. Die Frequenzen des 2,4-GHz-Bandes sind nur mit großem Aufwand räumlich zu kontrollieren, so dass Funkzellen auch über das eigene Firmengelände hinaus den Zugang zu einem WLAN ermöglichen {Abbildung 1}.

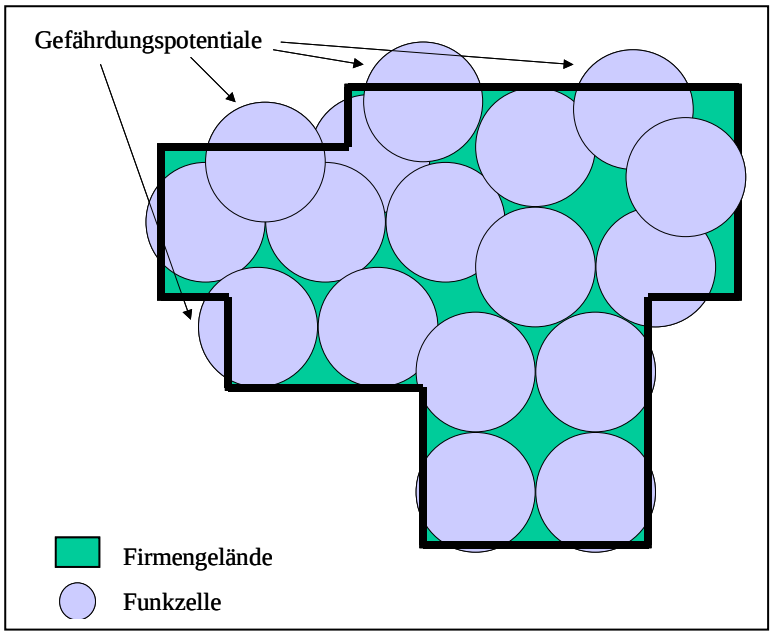

Abbildung 1: Beispielhafte funktechnische Ausleuchtung eines Firmengeländes

Mit der heute üblichen Plug and Play-Technologie können Rechner sehr leicht in Funknetze eingebunden werden. Die Einfachheit der Einbindung in diese Netze birgt jedoch auch ein inhärentes Problem in sich.

Eine externe Person kann so mit der entsprechenden Ausrüstung unberechtigt Zugang in das Firmennetz erlangen und als interner Benutzer arbeiten [2]. Ebenso können Personen, die sich auf dem Firmengelände befinden, unbemerkt am Funknetz teilnehmen und im schlimmsten Fall ihren Rechner als Gateway installieren, so dass von überall her unkontrollierter Zugriff auf das Unternehmensnetz besteht. Nebenpfade, wie oben beschrieben, ins firmeneigene Kommunikationsnetz werden von Hackern gerne genutzt. Dieses Szenario gilt es zu verhindern.

Aus sicherheitstechnischer Sicht sollte in einem Unternehmen die Verbindung interner Datennetze mit den externen Datennetzen (z.B. weltweites Internet, Telefonnetz) nur an einer zentralen Stelle erfolgen. Hier sind alle notwendigen Sicherheitsmaßnahmen (Logging, Routing, Firewalling, Authentication und Authorization usw.) implementiert und werden von geschultem Fachpersonal betrieben und überwacht.

Bedingt durch die Eigenschaften der Funkübertragung kann nicht die gleiche Konnektivität und Performance wie im leitungsgebundenen Netz garantiert werden. So bringen es die technischen Besonderheiten des WLANs mit sich, dass Funk-LANs mit 11 Mbit/s als "shared medium" betrieben werden. Das bedeutet, dass sich die Benutzer eine effektive Bandbreite von etwa 5,7 Mbit/s teilen müssen. Es kann hier sehr schnell zu Engpässen kommen, da eine unkontrollierte Nutzung stattfinden kann (Adhoc-Nutzung z.B. bei Besprechungen). Eine Planung des Netzes ist für das Netzmanagement wesentlich schwieriger.

Um gegenseitige Störungen (Bandbreitenengpässe) zu vermeiden, sollten die Benutzer des WLAN auch gebeten werden, keine großen Datenmengen zu übertragen, da das WLAN dafür ungeeignet ist.

Bei auftretenden Netzproblemen kann in kabelgebundenen geswichten Netzen schnell der Verursacher ermittelt werden. Die heutigen modernen Netzprotokolle ermöglichen über ein Remote Management die Konfiguration und Überwachung der Netzkomponenten von einer zentralen Managementworkstation aus. Hierdurch sind die Kommunikation störende Geräte leicht ermittelbar. Switch und Switchport, an den das Gerät angeschlossen ist, können prozedural ausgelesen werden. Das störende Gerät kann umgehend am Switch gesperrt und eine störungsfreie Kommunikation wieder hergestellt werden. Anders ist dies bei Funknetzen. Auch hier kann das verursachende Gerät anhand der Hardware-Adresse ermittelt und der zugehörige Access Point, der diesem Gerät Zugriff gewährt hat, ermittelt werden. Allerdings führt eine Sperrung des Problemverursachers nicht automatisch zur Lösung des Netzproblems. Der Verursacher stört weiterhin die Funkzelle, in der er tätig ist. Die hier angemeldeten Geräte können erst wieder störungsfrei arbeiten, wenn die defekte Komponente lokalisiert und abgeschaltet wurde. Dies kann eine langwierige Suche nach der Komponente im Bereich der Funkzelle bedeuten.

Alle diese Probleme machen somit eines unabdingbar. Voraussetzung für die Lösung ist der direkte und möglichst umgehende Kontakt mit dem Systemverantwortlichen. Es muss also auch in Funknetzen gelten: „Erst anmelden, dann surfen."

3 Probleme/Besonderheiten in Forschungsumgebungen

In Forschungsumgebungen werden häufig neuartige Techniken mit leistungsstarken Rechnern und Netzen hoher Bandbreite genutzt. Diese bieten daher ein attraktives Ziel für Attacken. Es gilt somit diese meist auch teuren Ressourcen ausreichend zu schützen. Eine straffe zentrale Organisation, wie in Wirtschaftsunternehmen, lässt sich in Forschungsumgebungen aber nicht leicht durchsetzen.

Aufgrund der weitreichenden Kooperationen eines Forschungszentrums mit externen Partnern aus Industrie, Forschung und Lehre sind ständig eine große Anzahl von Mitarbeitern dieser Partner vor Ort und benötigen Zugang zur Netzinfrastruktur. Charakteristisch für Forschungsumgebungen ist auch die hohe Anzahl von Praktikanten, Diplomanden und Doktoranden, die sich für kurze Zeit im Forschungszentrum aufhalten und für ihre Arbeit Zugriff auf interne Ressourcen wie Supercomputer, Drucker und Online-Bibliothekskataloge benötigen.

Ferner werden in den verschiedenen Teilinstituten Vortragsveranstaltungen organisiert, Ausbildungen durchgeführt und Adhoc-Besprechungen einberufen. Auch hier müssen Vortragsfolien heruntergeladen, Präsentationen über Kommunikationsnetze hinweg vorgeführt, Webinformationen geladen und E-Mails gelesen werden. Temporärer Kommunikationsbedarf ist hier ebenfalls vorhanden.

Grundprinzip sollte in derartigen sich häufig ändernden Umgebungen sein, dass jedes IT-System, das ans Rechnernetz angeschlossen wird, einen benannten Betreuer (Systemadministrator) hat, der sich beim Netzanschluss verpflichtet, für einen störungsfreien und sicheren Betrieb am Netz zu sorgen und alle Konfigurations- und Standortänderungen dem zentralen Netz-Management zu melden. Um kurzfristig am System auftretende Probleme des Netzwerkbetriebs und der IT-Sicherheit bearbeiten zu können, sollte auch bei Abwesenheit des Systemadministrators eine Vertretung ansprechbar sein. Im Forschungszentrum Jülich werden diese Informationen nicht nur für IT-Sicherheitsbelange sondern auch für das tägliche Netzmanagement ständig benötigt und sind hier mittels eines

selbsterstellten Netzverwaltungstool realisiert. Diese Informationen sind auch für ein sich ständig änderndes Wireless LAN und eine Anmeldung dieser Systeme unverzichtbar.

4 Sicherheitsfeatures im IEEE 802.11b Standard

Der IEEE 802.11 Standard bietet verschiedene Sicherheits-Features. Hierzu gehören Open- und Shared-Key-Authentisierung, der Service Set Identifier (SSID) und das Wired Equivalent Privacy (WEP) Protokoll. Jede dieser Features bietet unterschiedliche Level von Sicherheit.

Bei der SSID gibt es zwei unterschiedliche Nutzungsmodelle. Der SSID kann als Netzwerkname genutzt werden, über den sich ein Rechner an einen Access Point assoziieren kann. Werden für unterschiedliche Access Points verschiedene SSID's genutzt, so können hierdurch getrennte Zugriffsbereiche definiert werden. In diesem Modus wird der Access Point so konfiguriert, dass er seinen SSID broadcastet. Somit kann ein WLAN-Rechner über diesen SSID den Access Point finden, mit dem er sich verbinden möchte (das für ihn vorgesehene Netz).

Im zweiten Modus wird der SSID nicht vom Access Point bekannt gegeben. Der WLAN-Rechner kann sich durch Kenntnis des SSID ausweisen und somit Zugriff auf das Netz erlangen (preshared key).

Leider bietet dieser Zugriffsmodus keine ausreichende Sicherheit, da Management-Frames in 802.11 WLANs unverschlüsselt übertragen werden. Mit entsprechender Softwareausstattung kann eine unberechtigte Person den SSID mitlesen. Diese Software (z.B. AirSnort) ist vielfach im Internet frei verfügbar.

Der Zugriff eines Endgerätes auf das WLAN geschieht in mehreren Phasen. Nach einem Probe-Request und -Response wird mittels eines Authentication-Request eine Authentifizierung durchgeführt. Ist diese erfolgreich abgelaufen, so erhält der Rechner eine Authentication-Response Nachricht. Diese Authentifizierung kann im einfachsten Fall aus einem Authentication Request (z.B. mit Angabe der Station ID oder Hardware-Adresse) und dem Authentication-Response („Success" oder „Failure") bestehen. In diesem Fall handelt es sich um eine Open- oder Null-Authentication.

Bei der Shared-Key-Authentication sendet der Access Point nach dem Authentication-Request des Clients einen per Zufallsgenerator erzeugten Challenge-Text. Der Client verschlüsselt diesen Text mit dem shared-key und sendet das Ergebnis zurück an den Access Point. Dieser entschlüsselt die empfangene Nachricht wiederum mit dem Shared-Key. Ergibt sich der Ursprungstext, so war die Authentifizierung korrekt und ein Authentication-Response mit „Success" wird gesendet. Um gegenseitige Authentifizierung zu erlangen wird der Prozess ebenso in umgekehrter Richtung durchgeführt. Viele bekannte Attacken basieren darauf, dass durch Mitschneiden eines verschlüsselten Textes bei bekanntem Ursprungstext (Challenge-text) der Shared Key ermittelt werden kann. Eine Sicherheit auf der Basis dieser Shared-Key-Authentication ist somit nicht gewährleistet. Ein weiteres Problem ist, dass alle WLAN-Teilnehmer diesen Key kennen müssen, was sich einerseits leicht herumspricht, auch Gäste müssen diesen Key wissen, und andererseits bedeutet, dass ein derartiger Shared-Key nicht einfach änderbar ist, da alle WLAN-Teilnehmer informiert werden müssen.

Das Wired Equivalent Privacy (WEP) Protokoll wurde entwickelt, um das einfache Mitlesen am Netz zu verhindern. Die Sicherheit vergrößert sich mit der Länge des verwendeten Schlüssels. Der WEP-Algorithmus basiert auf dem RC4 Algorithmus und benutzt nur einen 40-Bit Secret Key in Verbindung mit einem 24 Bit Initialisierungsvektor. Hierdurch kann keine ausreichende Verschlüsselung gewährleistet werden. Das WEP-Protokoll bietet somit keinen ausreichenden Schutz gegen Mithören [3, 4]. Zur Zeit bietet also keines der im Standard spezifizierten Verfahren ausreichende Sicherheit. In der Entwicklung sind derzeit

neue Standards, die dieses Manko aufgreifen. Eine sichere Kommunikation bedarf daher momentan weitergehender Sicherungsmaßnahmen, auf die weiter unten eingegangen wird.

5 Das WLAN Konzept des Forschungszentrums Jülich

5.1 Allgemeines

Das WLAN muss in die bestehende Netzwerk-Infrastruktur integriert werden. Moderne Technologien erlauben in kabelgebundenen Netzen eine hierarchische Strukturierung (Baumstruktur), so dass jedes Endgerät einen dedizierten Anschluss besitzt. Hierdurch kann jedes Endgerät (Port am Switch) einem oder mehreren VLANs (Virtual LAN) zugeordnet werden. Durch diese, auf den Switches konfigurierten, VLANs lässt sich eine Trennung der Maschinen unterschiedlicher Netze realisieren, also auch zwischen kabel- und funkgebundenem Netz. Im Forschungszentrum Jülich können nur die Institute am WLAN teilnehmen, die an die switch-basierte Infrastruktur angeschlossen sind. Die über die VLANs realisierte Trennung zwischen kabelgebundenem und funkbasiertem Netz liefert nicht nur Sicherheit, sondern erspart auch zusätzliche Kosten für eine parallele Infrastruktur. Netzbereiche, die noch über Busstrukturen angebunden sind, können somit am WLAN-Betrieb nicht teilnehmen.

Der Anschluss der WLAN-Teilnehmer ans kabelgebundene Netz wird mittels sogenannter Access Points (APs) realisiert. Diese verfügen über einen Ethernet-Anschluss. Im Forschungszentrum Jülich werden diese Access Points und die zugehörigen Antennen zentral beschafft, installiert und administriert, um einen reibungslosen Betrieb zu gewährleisten. Es werden hier Produkte aus der "Cisco Aironet Serie" der Firma Cisco Systems eingesetzt. Diese Geräte garantieren auch eine sehr gute Kompatibilität mit Funk-LAN-Adaptern anderer Hersteller in den Endgeräten. Da diese Hardware-Komponenten, die für den Zugang eingesetzt werden, Produkte eines Herstellers sind, wird die Kompatibilität der Geräte untereinander und mit dem kabelgebundenen Netz sichergestellt, eine leichtere Administrierbarkeit wird erreicht. WLANs, welche diesen Bedingungen nicht entsprechen, dürfen im Forschungszentrum Jülich nicht installiert und betrieben werden.

Mobile Computer sowie stationäre Endgeräte können durch den Einbau eines speziellen WLAN-Adapters (Funk-LAN-Karte) ohne großen Aufwand in das Funknetz integriert werden.

Das WLAN wird als Ergänzung zum bestehenden kabelgebundenen Netz angeboten. Es ist auf dem Campus nicht flächendeckend verfügbar und nur dort nutzbar, wo entsprechende Hardware-Komponenten installiert worden sind. Für Gäste und Mitarbeiter des Unternehmens ist es wichtig, dass über das WLAN eine rasche und einfach zu handhabende Konnektivität ins lokale und weltweite Internet ermöglicht wird.

Alle Regelungen des kabelgebundenen Netzes gelten auch entsprechend für das WLAN. Das System muss beim Netzmanagement angemeldet sein. Der verantwortliche Systemadministrator muss dafür Sorge tragen, dass die aktuellen Betriebssystem- und Software-Patches installiert werden, alle nicht benötigten Dienste deaktiviert sind und Virenfilter mit den aktuellsten Virenmustern und eine Personal Firewall die Sicherheit des Systems ergänzen.

Des weiteren ist zu beachten, dass die Anschlüsse an das kabelgebundene Netz und an das WLAN (Funknetz) nicht gleichzeitig aktiv sein dürfen, da hierdurch einerseits Routingprobleme auftreten können und zum anderen parallele Übergänge zum zentralen Eingangsrouter (Firewall) implementiert werden könnten (vgl. Abbildung 2), die der

Sicherheitsphilosophie der Einrichtung widersprächen. Also müssen mögliche weitere Netzwerkadapter entfernt oder deaktiviert werden.

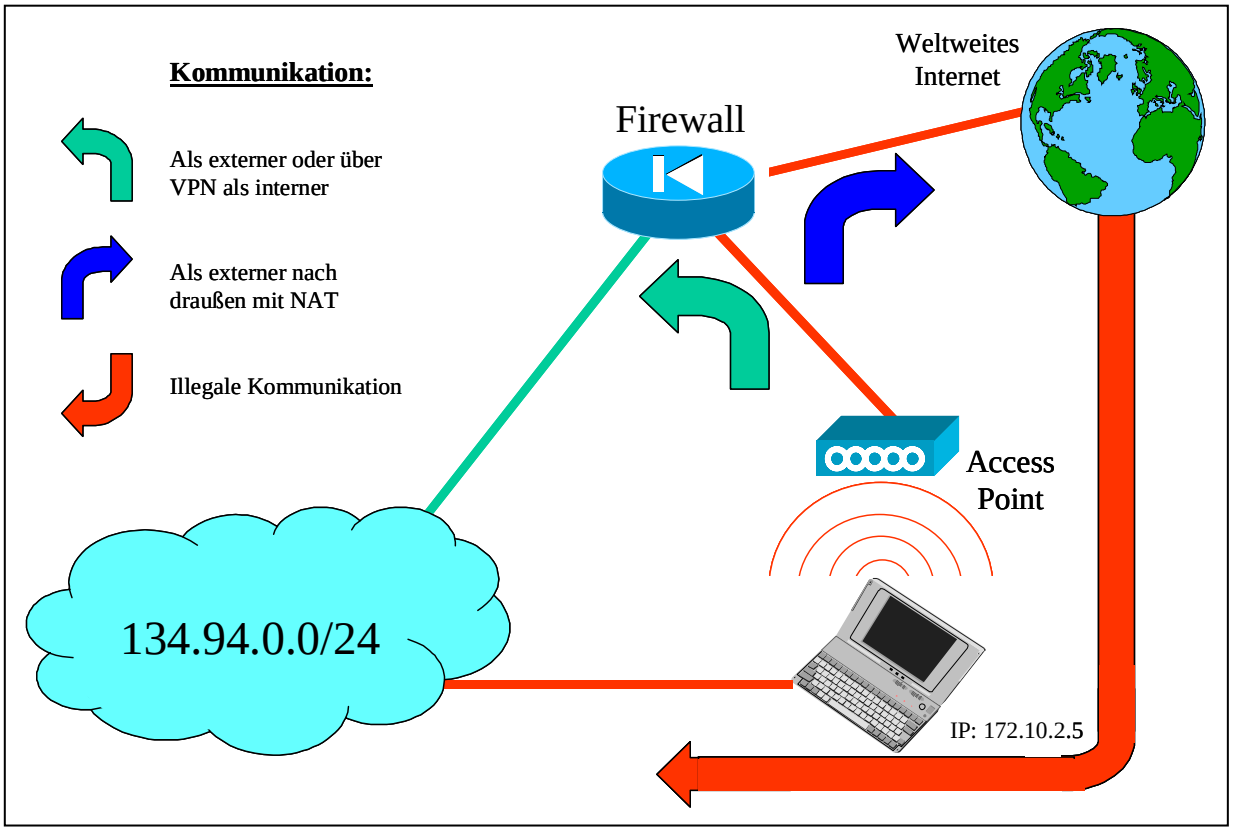

Abbildung 2: Illegale Konfiguration WLAN-Rechner als Gateway

5.2 Integration des WLAN mit MAC-Authentication

Dem WLAN wird ein privater IP-Adressbereich nach RFC1918 zugewiesen, der sicherheitstechnisch als externes Netz zu betrachten ist. Hieraus resultiert ein disjunkter Adressbereich zwischen kabelgebundenem und funkbasiertem Netz. Diese privaten Adressen müssen nicht bei der zentralen Adressvergabestelle (Internet Assigned Numbers Authority, IANA) beantragt werden. Sie erweitern somit den von der IANA zugewiesenen Adressbereich. Ein Firewall-System filtert die Zugriffe vom WLAN ins kabelgebundene Netz gemäß der Unternehmens-Sicherheitsphilosophie.

Mitarbeiter und Gäste, die ihren Rechner an das WLAN anschließen möchten, müssen hierzu einen Antrag stellen. Antragsteller und MAC-Adresse der Funk-Karte des Rechners werden hierbei gespeichert. Die Möglichkeit einer elektronischen Beantragung mit Antragstelleridentifikation erlaubt eine schnelle, automatische Bearbeitung des Antrages. Der Antragsteller übernimmt hierdurch die Verantwortung für die Kommunikation mit diesem Funk-LAN-Adapter. Die Konnektivität kann so innerhalb weniger Minuten hergestellt werden.

Die Access Points bieten eine Zugangskontrolle (MAC-Address-Authentication [5]), die es ermöglicht, den Zugang Unbefugter (nicht registrierter Netzwerkkarten) auf Netzwerkebene zu unterbinden. Diese MAC-Address-Authentication, welche die Open- und Shared-Key Authentication gemäß Standard 802.11b erweitert, ist zwar nicht im Standard vorgesehen,

aber von vielen Herstellern implementiert worden. Jedem Netzwerkadapter ist eine eindeutige Hardware-Adresse zugeordnet, so dass der Zugang zum WLAN auf bekannte Hardware-Adressen beschränkt werden kann. Diese bei der Authentication mitgesandte MAC-Adresse wird auf einem Radius-Server verifiziert. Logging dieser Adress-Vergabe (Antragsteller, Mac-Adresse, vergebene IP-Adresse, Start- und Endzeit der Komunikation) ermöglicht im Problemfall eine zeitlich korrelierte Identifikation der Nutzer des WLAN.

Die Zulassung zum Wireless LAN hat zunächst eine begrenzte Gültigkeit. Mitarbeiter des Forschungszentrums können eine dauerhafte Zulassung beantragen. Dazu muss der User das Formular, das bei der Registrierung im Web ausgedruckt werden kann, unterschrieben bei der Netzwerk-Benutzerberatung des Forschungszentrums abgeben.

Gastwissenschaftler sowie andere Gäste erhalten einen Zugang zum WLAN nur über ihren jeweiligen Betreuer im Forschungszentrum. Die Gültigkeit liegt wahlweise zwischen einer Woche und dauerhaftem Zugriff.

Konferenzteilnehmer können über das jeweilige Tagungsbüro einen Zugang zum WLAN erhalten. Die Konferenzteilnehmer sind keinem direkten Betreuer zugeordnet, so dass hier die Anmeldung für das WLAN durch das Konferenzbüro für diese Zeit (maximal eine Woche) vorgenommen wird. Konferenzlisten mit Konferenzteilnehmer und zugeordneter Hardware-Adresse seines Rechners geben im Problemfall Rückschluss auf den betroffenen Rechner.

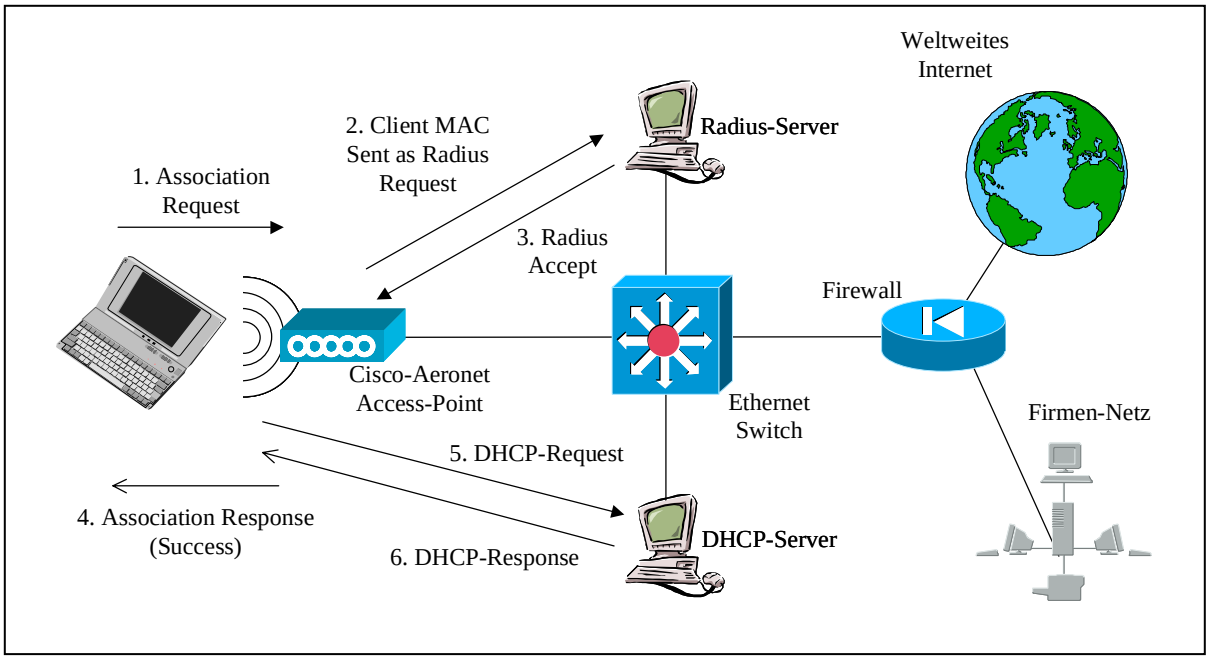

Abbildung 3: WLAN-Zugriff mittels MAC-Authentication

Die IP-Adressen der WLAN Teilnehmer werden automatisch per DHCP (Dynamic Host Configuration Protocol [6]) vergeben. Ein DHCP-Server versorgt dabei auf Anfrage die Stationen mit einer nur im WLAN gültigen IP-Adresse aus seinem Adress-Pool sowie Informationen über den eigenen Namen, Domain, Netzmaske, Nameserver, NTP-Server und Default-Gateway. Hierdurch ist die Kommunikation der registrierten WLAN-Teilnehmer untereinander sichergestellt.

Im Forschungszentrum Jülich werden im WLAN private IP-Adressen benutzt, um einerseits keinen Adressbereich des öffentlich bekannten Netzes des Forschungszentrums zu verbrauchen und andererseits eine klare Trennung zwischen internen und externen Netzteilnehmern zu gewährleisten. Viele Sicherheitsmechanismen beruhen auf der Aufteilung von lokalen und nicht-lokalen Netzen in unterschiedliche Sicherheitszonen, wobei die lokalen

Netze als sicher(er) angesehen werden. Die Unterscheidung zwischen lokal und nicht-lokal wird dabei oftmals aufgrund der IP-Adresse getroffen. Eine saubere Trennung dieser Bereiche ist daher von Vorteil.

Eine Kommunikation in das Firmennetz, bzw. in das weltweite Internet kann aufgrund der privaten Adressen nur stattfinden, wenn diese entweder geroutet werden oder aber andere Mechanismen in Anwendung kommen. Diese Mechanismen beschreiben die beiden folgenden Kapitel.

5.3 Zugriff in das Intranet (VPN, externe Mitarbeiter)

Bei der in das Forschungszentrum Jülich eingehenden Kommunikation werden über das lokale Firewall nur Dienste zugelassen, die der bestehenden Sicherheitsphilosophie entsprechen. Alle Aktivitäten der WLAN-Nutzer werden immer als externe Aktivitäten betrachtet. Es wird daher eine Funktion benötigt, die Mitarbeitern des Forschungszentrums Jülich, die über das WLAN kommunizieren, den internen Benutzern des kabelgebundenen Netzes gleichstellt. So kann auf interne Ressourcen wie Mail- und Druckserver, File- und Computeserver des Forschungszentrums Jülich zugegriffen werden. Zur Behebung dieser Problematik können Virtual Private Networks (VPN's) [7] eingesetzt werden. VPN's minimieren die Gefährdungspotentiale einer Datenübertragung durch unsichere nicht lokale Netze. Diese Technologie nutzt kryptographische Verfahren zum Aufbau eines sicheren Zugangs zu einem Firmennetz. Sie bieten Vertraulichkeit durch verschlüsselte Übertragung, Authentifizierung, Autorisierung und Integrität.

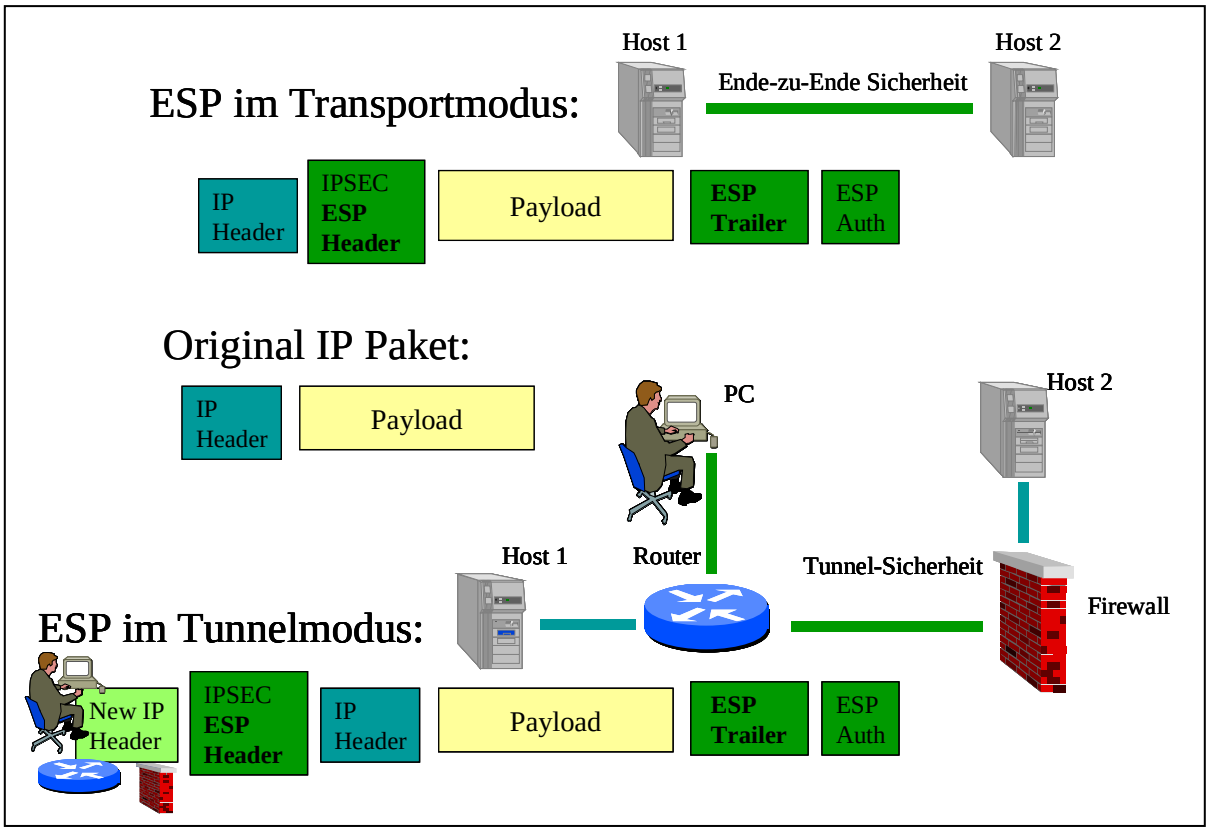

Abbildung 4: IPSEC- Tunnel-Techniken

Zur Realisierung eines VPN's werden die ursprünglichen IP-Pakete verschlüsselt und in einem neuen IP-Paket durch das INTERNET zu einem Security Gateway übertragen; diese Art der Übertragung ist eine spezielle Variante sogenannter IP-Tunnel. Im Forschungszentrum Jülich basiert die VPN-Lösung auf dem IPSEC-Protokoll. Das IPSEC-Protokoll ist integraler Bestandteil von IPv6 und kann in IPv4 optional genutzt werden. Hier wird das ursprüngliche IP-Paket in ein neues IPSEC-Paket eingepackt.
Das Security Gateway im Forschungszentrum Jülich ist ein Cisco VPN Concentrator. Die auf der Gegenseite (Client) genutzte VPN-Software ist die Cisco VPN Client Software [8, 9], die insbesondere auf Interoperabilität mit dem Cisco VPN Concentrator als Security Gateway optimiert ist.

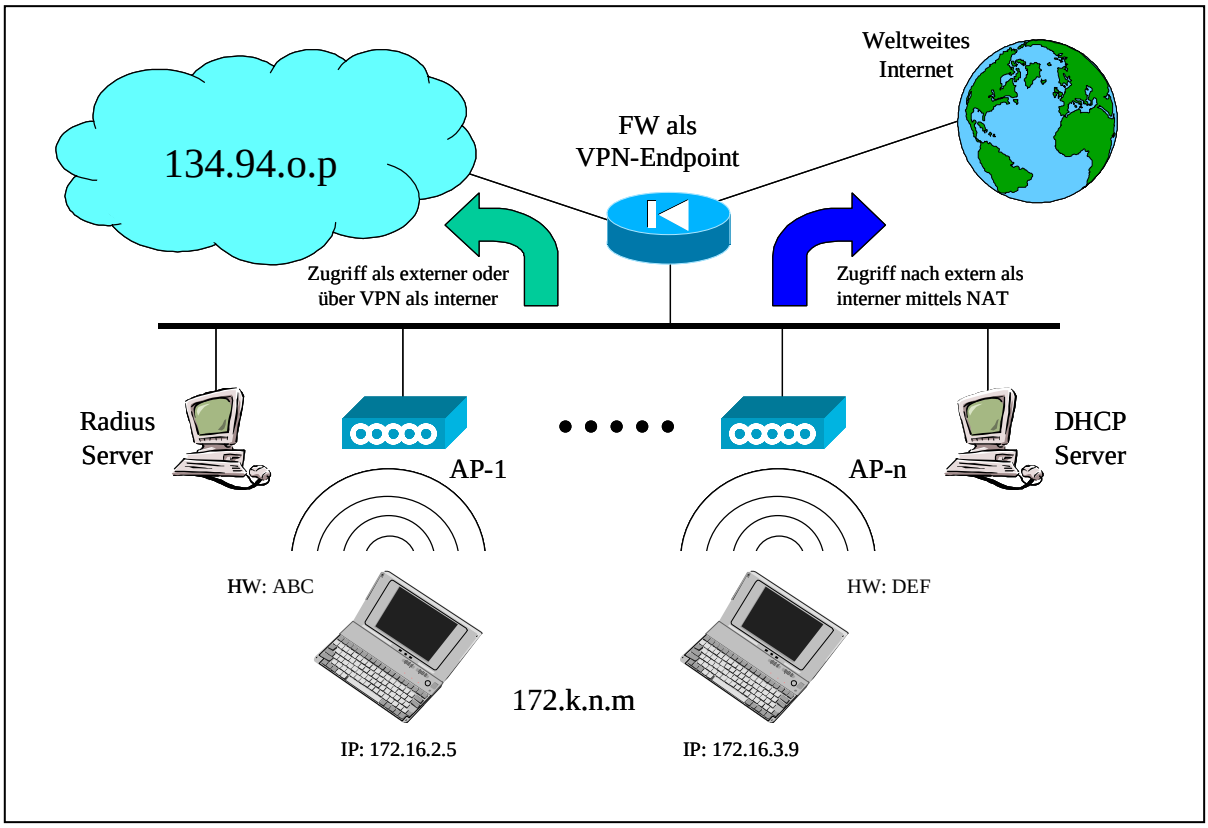

Abbildung 5: VPN-Zugriff (WLAN) auf interne Dienste des Forschungszentrums

Eine wichtige Eigenschaft dieser VPN-Software ist die Zuordnung einer eigenen IP-Adresse im geschützten IP-Tunnel, hier im konkreten Fall eine offizielle Internet-Adresse des Forschungszentrums Jülich. Damit sind VPN-Benutzer beim Zugriff auf zentrale Server wie WWW- und E-Mail-Server des Forschungszentrums internen Benutzern gleichgestellt. Derzeit ist die Software für die Windows-Varianten 95/98/Me/NT/2000/XP, LINUX (x86) mit Kernelversion 2.2 – 2.4, Solaris OS Vers. 2.6+ und Macintosh OS X Version 10.1.0+ verfügbar.

5.4 Zugriff auf das weltweite Internet (NAT/PAT)

Die WLAN-Teilnehmer benötigen Zugriff sowohl auf interne Ressourcen als auch auf externe Dienste. Insbesondere wollen Gäste auf Dienste ihres Firmennetzwerkes zugreifen.

Im Internet werden Pakete jedoch nur dann erfolgreich weitergeleitet, wenn das Netz, zu welchem ein Rechner gehört, in den weltweit installierten Routern bekannt ist oder aber eine

Default-Route existiert. Die nach RFC 1918 [10] definierten und im WLAN des Forschungszentrums Jülich benutzen privaten IP-Adressen werden jedoch von den meisten Providern nicht weitergeleitet, da diese Netze nicht eindeutig einer Installation zugewiesen sind. Eine eindeutige Weiterleitung solcher Adressen ist also nicht gewährleistet. Um nun den WLAN-Teilnehmer, die per DHCP-Server Adressen aus einem privaten Adressbereich erhalten haben, einen Zugriff auf Rechner im weltweiten Internet ermöglichen zu können, müssen diese Adressen eindeutig öffentlichen Adressen zugeordnet werden. Daher ist ein Mechanismus erforderlich, der bei einem Zugriff auf das Internet diese privaten Adressen in offizielle IP-Adressen aus dem Adressraum des Forschungszentrums umsetzt. Das geschieht mittels Network Address Translation (NAT) [11] bzw. Port Address Translation (PAT) an dafür geeigneten Geräten. Hier wird bei jedem Zugriff auf externe Ressourcen eine dynamische Adress-Übersetzung gestartet, die nur für einen begrenzten Zeitraum gültig ist. Es braucht daher nur ein eingeschränkter IP-Adress-Bereich der Einrichtung reserviert zu werden.

Bei der Port Address Translation wird ebenfalls eine Adress-Umsetzung durchgeführt. Allerdings wird hier nur eine offizielle Adresse benötigt. Zusätzlich muss hier zur Adressumsetzung auf diese eine Adresse auch noch eine Umsetzung der Source Ports durchgeführt werden, so dass das NAT-Device anhand der zurückkommenden Pakete erkennen kann, für welche Verbindung diese Pakete bestimmt sind. Aufgrund der großen Menge der Ports, mehr als 60000, kann hierdurch Adressraum eingespart werden, wenn nicht genügend offizielle lokale Adressen zur Verfügung stehen.

Logging der dynamischen Adress/Port-Vergabe gewährleistet auch hier eine Rechner-/Benutzeridentifikation im Problemfall. Werden von externen Stellen Zugriffe aus dem Forschungszentrum Jülich gemeldet, die einer Aufklärung bedürfen, so kann mittels der Logging-Dateien der zentralen Geräte die Hardware- Adresse des Urhebers zurückermittelt werden, wenn Informationen über den Zeitpunkt des illegalen Zugriffs bekannt sind. Aufgrund dieser Informationen kann nun im Anmeldeprotokoll der Hardware-Adressen (Benutzer, Hardware-Adresse) der Systemadministrator des Rechners (Beantrager) ermittelt werden. Dieser kann sich dann um das Problem kümmern.

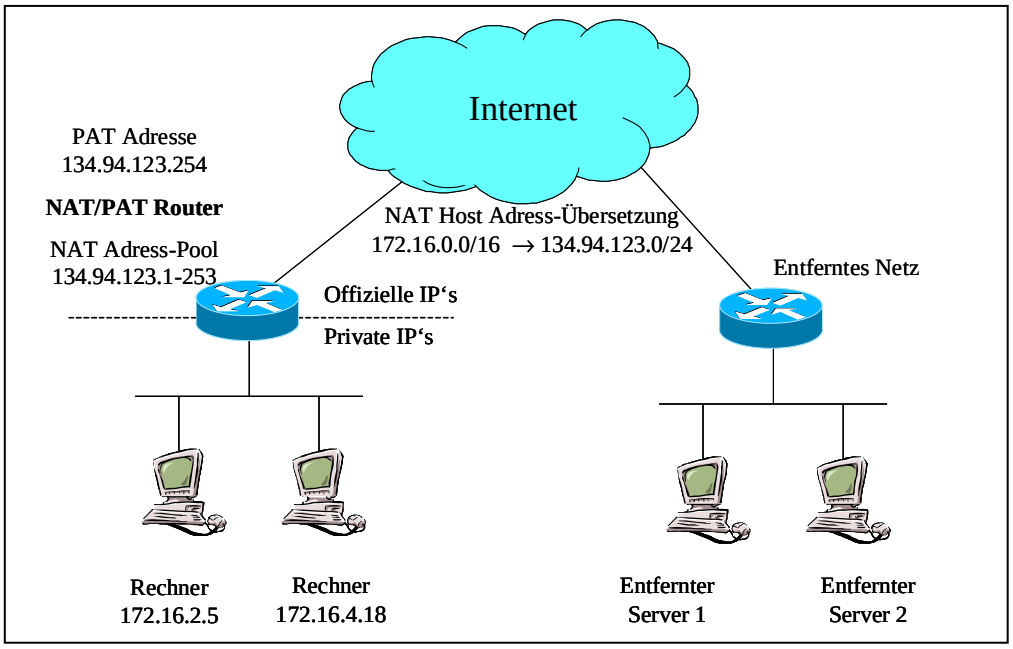

Abbildung 6: NAT/PAT Adress-Übersetzung für den Zugriff ins weltweite Internet

6 Zusammenfassung

Der hier aufgezeigte Weg der Integration eines Wireless-LAN in eine Forschungsumgebung stellt sich als sichere und weitgehend auch flexible Lösung dar. Die Realisierung des WLANs als externes Netz bietet sicherheitstechnisch gesehen Schutz vor dem Zugriff unberechtigter Personen in das kabelgebundene Rechnernetz. Die Mac-Adress-Authentifizierung macht es unberechtigten Personen schwierig, wenn auch nicht unmöglich, das WLAN mit seinen Access-Points zu nutzen. Der VPN-Zugriff ermöglicht es berechtigten Personen authentifiziert und vertraulich auf interne Ressourcen uneingeschränkt zuzugreifen. Die NAT/PAT-Übersetzung für die externe Kommunikation bietet zusätzlich die Möglichkeit externe Dienste, wie z.B. Mail- und Web-Server, zu erreichen, was z.B. für Gäste, die nur kurze Zeit in der Einrichtung tätig sind, zwingend notwendig erscheint. Durch die Implementierung einer elektronischen Registrierung der WLAN-Adapter ist eine AdHoc-Kommunikation gewährleistet. Eine sichere, kostensparende und weitgehend uneingeschränkte Nutzung der Unternehmensressourcen durch berechtigte Personen aus dem Wireless-LAN ist somit gewährleistet.

Literaturverzeichnis

[1] Heise-Online Meldung vom 25.04.2002 13:55: „Funknetz Hacken straffrei?“, http://www.heise.de/newsticker/data/pab-25.04.02-000/

[2] Heise-Online Meldung vom 13.03.2002 18:15: „FunkLAN im Überfluss“, http://www.heise.de/newsticker/data/ju-13.03.02-000/

[3] N.Borisov,I.Goldberg,D.Wagner – Intercepting Mobile Communications: The Insecurity of 802.11, ACM Press, Proceedings of the seventh annual international conference on Mobile computing and networking, pp. 180 189, New York 2001, ISBN 1-58113-422-3

[4] A. Stubblefield, et al – Using the Fluhrer, Mantin and Shamir Attack to break WEP (Rev. 2), AT&T Labs Tech. Report TD-4ZCPZZ, http://www.cs.rice.edu/~astubble/wep/, Aug. 2001

[5] Cisco Systems - 802.11 Wireless LAN Security White Paper, A Comprehensive Review of 802.11 WLAN Security and the Cisco Wireless Security Suite, http://ww.cisco.com

[6] P.Degotardi, et al - Beyond DHCP – Work Your TCP/IP Internetwork with Dynamic IP, IBM-Redbooks, SG24-5280-00, Aug. 1998

[7] Microsoft Windows 2000 Server - White Paper: Microsoft Privacy Protected Network Access:Virtual Private Networking and Intranet Security, 1999, http://www.microsoft.com/windows2000/docs/nwpriv.doc

[8] Cisco Systems – VPN Client Administrator Guide, Release 3.6, Aug. 2002, Customer Order number DOC-7814739-, Text Part Number: 78-14739-01, http://www.cisco.com

[9] Cisco Systems – VPN Client Users Guide, Release 3.6, August 2002, Customer Order Number DOC-7814738-, Text Part Number: 78-14738-01, http://www.cico.com

[10] Y. Rekhter, et al - Address Allocation for Private Internets, RFC 1918, Februar 1996, ftp://ftp.uni-stuttgart.de/pub/doc/standards/rfc/rfc1918.txt.gz

[11] K. Egevang, P. Francis - The IP Network Address Translator (NAT), RFC 1631, Mai 1994, ftp://ftp.uni-stuttgart.de/pub/doc/standards/rfc/rfc1631.txt.gz