



Institut für Telematik
unter Betreuung der
Fraunhofer Gesellschaft

 Preprint 01-10

**Anforderungsprofil für
den „sicheren“ Betrieb
eines WLAN**

Uwe Roth
Frank Losemann
Thomas Engel
Christoph Meinel



Authors	Dipl. Inform. Uwe Roth Dipl. Inform Frank Losemann Dr. Thomas Engel Prof. Dr. Christoph Meinel
Copyright	© 2001 Institut für Telematik e.V., Trier
Trademarks	Use of a term in this paper should not be regarded as affecting the validity of any trademark and service mark. The product or brand names are trademarks of their respective owners.
Printing	1/2002
Document status	Version 1.2a (14.01.2001)
	Printed in Germany All rights reserved
	<p>The documentation was accomplished through the Institut für Telematik.</p> <p>The information contained in this document represents the current view of the authors on the issues discussed as of the date of publication. Because the mentioned enterprises must respond to changing market conditions, the results of this paper should not be interpreted to be a commitment on the part of the authors. Any information presented after the date of publication are subject to change.</p> <p>The right to copy this documentation is limited by copyright law. Making unauthorised copies, adaptations or compilation works without permission of the authors or institutions mentioned above is prohibited and constitutes a punishable violation of the law.</p>



Im Gegensatz zu der aus der Werbung vertretenen Meinung ist die Einführung eines WLAN (Wireless LAN) nicht mit dem Aufbau einzelner Empfangsstationen (Access-Points) und der Installation der Funk-Karten (WLAN-Karten) in den Computern abgeschlossen. Die Gründe hierfür sind hauptsächlich Sicherheitsaspekte, da mit der Datenübertragung über Funk ein Zugang zu dem Intranet der Institution geschaffen wird, der bisher technisch nicht möglich war.

Mit dem Aufbau eines WLAN muss deshalb schon im Vorfeld die Frage geklärt werden, welche Services (Dienste, Leistungsmerkmale) von dem WLAN erwartet werden (QoS - Quality of Services). Auf Grundlage dieser Entscheidung kann anschließend eine Lösung entwickelt werden, die alle benötigten Sicherheitsaspekte berücksichtigt, um das WLAN zu betreiben und die QoS-Liste abdeckt. Da mit dem Aufbau der Lösung auch der Einsatz an zusätzlichen Komponenten notwendig ist, muss eine Priorisierung stattfinden, um einen Kompromiss zwischen dem finanziellen Rahmen, den gewünschten Services, sowie den notwendigen Sicherheitsanforderungen in Einklang zu bringen.

Dieses Dokument deckt im Wesentlichen den Entscheidungsprozess am Institut für Telematik ab. Bis zu einem gewissen Punkt sind die Fragestellungen und Lösungsansätze allgemeingültig. Ab dem Zeitpunkt der Konkretisierung der Lösung, hat natürlich unsere Prioritätsliste der QoS sowie die am Institut vorliegende Infrastruktur das Endergebnis stark beeinflusst.

Anforderungsprofil für den „sicheren“ Betrieb eines WLAN

Uwe Roth

Frank Losemann

Thomas Engel

Christoph Meinel

Sicherheit im WLAN?

Wireless LAN (WLAN) ist ein Funknetz, das auf dem Standard von IEEE 802.11b basiert. Dieser Standard garantiert eine Übertragungsrate bis maximal 11MBit/s. Der Standard definiert mit dem WEP-Protokoll (Wired Equivalent Privacy) eine Möglichkeit der verschlüsselten Kommunikation zwischen Funk-Karten und Basis-Station. Zur Zeit sind zwei Variationen des WEP-Protokolles üblich. WEP 40 basiert auf 64Bit von denen 24 Bit einen nicht zufälligen Initialisierungsvektor beinhalten. Die Zahl 40 definiert also die verbliebenen wirksamen Bit. Bei WEP 128 definiert 128 die Gesamtzahl der Bit. Auch hier sind nur die um 24 Bit reduzierten 104 Bit wirksam. Beide Verfahren leiden an dem prinzipiellen Problem, dass durch reines Mithören des Datenstromes der Schlüssel berechnet werden kann. Die zur Berechnung notwendigen belauschten Datenpakete steigt mit der Anzahl der Schlüssellänge nur linear an, womit eine Verdopplung der Schlüssellänge nur eine Verdopplung der notwendigen Zeit zum Entschlüsseln mit sich bringt. Inzwischen sind Tools im Internet erhältlich, die es auch technisch unversierten Personen ermöglichen, den Schlüssel zu knacken und damit den Datenverkehr abzu hören. Somit ist eine Absicherung allein durch WEP nicht geeignet.

Eine höhere Sicherheit ergibt sich durch die Verwendung von Virtual Private Network (VPN). VPN werden verwendet um in öffentlichen Netzen einen sicheren Tunnel zwischen zwei Kommunikationspartnern aufzubauen. Zur Zeit finden hauptsächlich zwei Protokolle Anwendung. PPTP (Point to Point Tunneling Protocol) ist eine Erweiterung des PPP Protokolls durch Microsoft. Damit ist dieses Protokoll schon Bestandteil der neueren Microsoft Betriebssysteme, der Konfigurationsaufwand somit überschaubar. PPTP ermöglicht das Tunneln von IP, IPX, SNA oder anderen Layer 3-Protokollen. Allerdings hat PPTP ein Design-Problem, so dass die Verbindungsdaten allein aus den ersten beiden übertragenen Datenpaketen berechnet werden können. Als sicher für VPN gilt derzeit IPsec, das auch bei der Verschlüsselung der IP-Pakete von IPv6 zum Einsatz kommt. Allerdings ist mit IPsec das Protokoll auf IP beschränkt. Ebenso definiert IPsec nicht das verwendete Verschlüsselungssystem. Es muss also darauf geachtet werden, dass die beiden Kommunikationspartner mindestens ein gemeinsames Verschlüsselungsverfahren unterstützen.

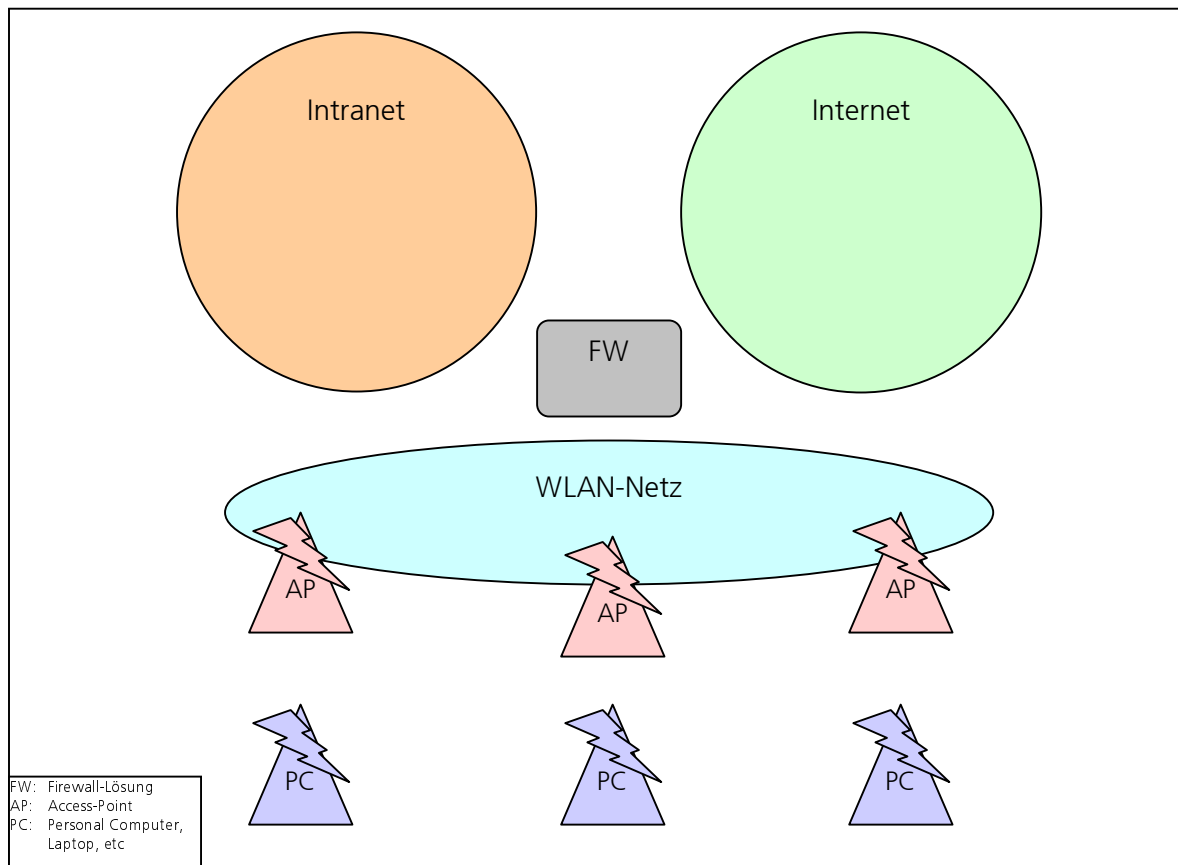
Ein weitere Möglichkeit, WLANs sicherer zu machen ist die Verwendung von Radius-Servern zur Autorisierung. Sie sichern zunächst den Zugang zu den Access-Points, bieten was die Abhörsicherheit angeht zunächst also keinen Vorteil. Unterstützen die Access-Points jedoch das EAP (Extensible authentication protocol) oder LEAP (Lightweight Extensible authentication protocol), kann der Radius-Server dazu beitragen, die bei der WEP-Kommunikation verwendeten Schlüssel zwischen Access-Point und WLAN-Karte auszuhandeln. Zur Berechnung des verwendeten WEP-Schlüssels wird eine bestimmte Anzahl von abgehörten Datenpaketen benötigt. Wird der Schlüssel jedoch öfters ausgetauscht, so erhöht das den Aufwand für einen potentiellen Angreifer erheblich und reduziert damit das Risiko.

Was sind mögliche Services?

Dieses Kapitel spezifiziert nicht die QoS, die das Institut von ein WLAN erwartet, sondern listet mögliche QoS auf. Alle im Folgenden entwickelten Szenarien müssen sich gegenüber dieser Liste positionieren. Es muss also klar sein, welche QoS von der Lösung abgedeckt werden, und welche nicht. Da die Lösungen auf verschiedenen Ebenen operieren, muss auch klar sein, welcher Beitrag die Teillösung zur Bereitstellung des Gesamt-QoS liefert. Es muss also deutlich werden, ob der Service ausschließlich von der Teillösung bereitgestellt wird oder dies möglicherweise schon von einer anderen Teillösung abgedeckt wird. Der Mehrwert muss sichtbar werden. Nach der Entwicklung möglicher Teillösung muss anschließend eine Priorisierung der Services stattfinden auf deren Grundlage anschließend die Zusammensetzung der WLAN-Lösung ermittelt werden kann.

Topologie

Die folgende Grafik soll die möglichen Beteiligten an der WLAN Lösung visualisieren. Sie dient als Grundlage zur grafischen Darstellung möglicher Lösungsszenarien. Der Detaillierungsgrad sowie die Position der einzelnen Komponenten ist dabei nicht auf die vorgegebene Grafik beschränkt. Vielmehr soll in der Diskussion um mögliche Lösung nur ein Hilfsmittel zur Verfügung gestellt werden, dass den Entscheidungsprozess unterstützt.



Quality of Services (QoS)

Bei der Definition möglicher Quality of Services sollte ein möglicher Lösungsansatz, sowie die daran beteiligten Komponenten, zunächst unberücksichtigt bleiben, um mögliche andere Lösungen nicht von vornherein zu benachteiligen. Aus diesem Grunde wurde versucht die Services aus Sicht der beteiligten Benutzergruppen oder Interessensvertreter auf einer höheren Ebene zu spezifizieren. So interessiert sich z.B. ein Benutzer des WLAN nur am Rande für die technische Gesamtkonzeption. Für ihn ist es von Interesse, mit dem WLAN die gleichen Dienste nutzen zu können wie stationär im LAN.

Die Liste der QoS ist so aufgebaut, dass sich alternative QoS unter Umständen widersprechen. So kann z.B. ein gewünschter QoS sein, einen bestimmten Service nicht nutzen zu können. Als Beispiel soll hier der Zugang von Gästen zum Intranet erwähnt sein.

Bei der Priorisierung muss somit nicht nur die Bedeutung eine QoS für die Gesamtlösung definiert, sondern auch die Alternative hierzu gewählt werden.

Aus der Sicht des Benutzers (Mitarbeiter)

Nr.	Alt.	Beschreibung	Erläuterung
1	a	Zugriff auf alle Services des Intranets .	Alle Rechner können auf allen Ports angesprochen werden: Umfassende Nutzung
	b	Zugriff auf einen Teil der Services des Intranets .	Ein Teil der Rechner kann auf bestimmten Ports angesprochen werden: Geschützte Nutzung
2	a	Zugriff auf alle Services des Internets .	Alle Rechner können auf allen Ports angesprochen werden.
	b	Zugriff auf einen Teil der Services des Internets .	Ein eingeschränkter Teil der Rechner kann auf bestimmten Ports angesprochen werden.
3	a	Zugriff auf alle Services des WLAN-Netzes.	Alle Rechner können auf allen Ports angesprochen werden.
	b	Zugriff auf einen Teil der Services des WLAN-Netzes:	Ein Teil der Rechner kann auf bestimmten Ports angesprochen werden.
	c	Zugriff auf keinen Service des WLAN-Netzes.	Kein Rechner des WLAN-Netzes kann angesprochen werden.
4	a	Roaming erlaubt/möglich. Wechsel des Access-Points, Übergabe der Verbindung	Der Benutzer kann sich bei bestehender Verbindung im Gebäude frei bewegen.
	b	Roaming nicht erlaubt/möglich.	Der Benutzer kann sich bei bestehender Verbindung im Gebäude nicht frei bewegen.

Aus der Sicht eines Gastes

Nr.	Alt.	Beschreibung	Erläuterung
5	a	Zugriff auf alle Services des Intranets.	Alle Rechner können auf allen Ports angesprochen werden.
	b	Zugriff auf einen Teil der Services des Intranets.	Ein Teil der Rechner kann auf bestimmten Ports angesprochen werden.
6	a	Zugriff auf alle Services des Internets.	Alle Rechner können auf allen Ports angesprochen werden.
	b	Zugriff auf einen Teil der Services des Internets.	Ein Teil der Rechner kann auf bestimmten Ports angesprochen werden.
7	a	Zugriff auf alle Services des WLAN-Netzes.	Alle Rechner können auf allen Ports angesprochen werden.
	b	Zugriff auf einen Teil der Services des WLAN-Netzes:	Ein Teil der Rechner kann auf bestimmten Ports angesprochen werden.
		Zugriff auf keinen Service des WLAN-Netzes.	Kein Rechner des WLAN-Netzes kann angesprochen werden.

8	a	Roaming erlaubt/möglich.	Der Benutzer kann sich bei bestehender Verbindung im Gebäude frei bewegen.
	b	Roaming nicht erlaubt/möglich.	Der Benutzer kann sich bei bestehender Verbindung im Gebäude nicht frei bewegen.

Kompatibilität Hardware

Nr.	Alt.	Beschreibung	Erläuterung
9		Access-Point: große Anzahl von PC-Karten möglich	Der Zugriff auf den Access-Point sollte auch von Karten anderer Hersteller möglich sein, wenn diese sich an allgemeingültige Standards halten.
10		PC-Karte: Windows	Für die eingesetzte Karte existieren Treiber für Windows.
11		PC-Karte: Linux	Für die eingesetzte Karte existieren Treiber für Linux.

Kompatibilität Software

Nr.	Alt.	Beschreibung	Erläuterung
12		Software: PC-Karte	Die notwendige Software auf dem PC läuft auch mit anderen PC-Karten.
13		Software: Access-Point	Die notwendige Software auf dem PC läuft auch mit anderen Access-Points.
14		Software: Fire-Wall (VPN-Module)	Die notwendige Software auf dem PC läuft auch mit anderen Firewalls/VPN-Moduln.
15		Software: Offenheit der Lösung	Die notwendige Software auf dem PC setzt keine Hardware eines bestimmten Herstellers ab Access-Point/WLAN voraus.
16		Software: Windows	Die notwendige Software auf dem PC läuft unter Windows.
17		Software: Linux	Die notwendige Software auf dem PC läuft unter Linux.

Sicherheit

Nr.	Alt.	Beschreibung	Erläuterung
18	a	Direkter Zugang zum Laptop (IEEE802.11-Ebene) möglich	Niemand kann über eine direkte Funkverbindung (ohne Access-Point) einen Kontakt zu einem Laptop herstellen (auf IEEE802.11-Ebene).
	b	Direkter Zugang zum Laptop (IEEE802.11-Ebene) nicht möglich	Über eine direkte Funkverbindung (ohne Access-Point) kann ein Kontakt zu einem Laptop hergestellt werden (auf IEEE802.11-Ebene).
19	a	Direkter Zugang zum Laptop (Protokoll-Ebene) möglich	Niemand kann über eine direkte Funkverbindung (ohne Access-Point) einen Kontakt zu einem Laptop herstellen und z.B. IP-Pakete übertragen.
	b	Direkter Zugang zum Laptop (Protokoll-Ebene) nicht möglich	Über eine direkte Funkverbindung (ohne Access-Point) kann ein Kontakt zu einem Laptop hergestellt werden und z.B. übertragen werden.
20		Zugang zum Laptop: Verschlüsselung	Alle Daten, die zum Laptop übertragen werden oder die den Laptop verlassen, sind verschlüsselt und können nur von bekannten Gegenstellen ver-/entschlüsselt werden.
21		Zugang zum Access-Point: PC-Karte	Nur autorisierte PC-Karten haben Zugriff zum Access-Point.
22		Zugang zum Access-Point: Person	Nur autorisierte Personen haben Zugang zum Access-Point.
23		Zugang zum Access-Point: Verschlüsselung (IEEE802.11)	Alle Daten die zum Access-Point übertragen werden sind verschlüsselt (IEEE802.11-Ebene).
24		Zugang zum Access-Point: Verschlüsselung (VPN)	Alle Daten die zum Access-Point übertragen werden sind verschlüsselt (VPN-Ebene).
24		Zugang zum WLAN: Person	Nur autorisierte Personen haben Zugang zum WLAN.
25		Zugang zum Intranet: Person	Nur autorisierte Personen haben Zugang zum Intranet.
26		Zugang zum Internet: Person	Nur autorisierte Personen haben Zugang zum Internet.

27	a	Diebstahl des Laptop: Keine Maßnahmen	Durch einen gestohlenen Laptop müssen keine Veränderungen an der bestehenden System-Konfiguration (Access-Points, Firewall, VPN) vorgenommen werden um die Sicherheit des Intranet/anderer WLAN-PC's zu gewährleisten.
	b	Diebstahl des Laptop: Verzögerte Maßnahmen	Durch einen gestohlenen Laptop müssen keine unmittelbaren Veränderungen an der bestehenden System-Konfiguration (Access-Points, Firewall, VPN) vorgenommen werden um die Sicherheit des Intranet/anderer WLAN-PC's zu gewährleisten. Um die Wahrscheinlichkeit einer erfolgreichen Offline-Attacke gegenüber den notwendigen Zugangsdaten auf dem Laptop auszuschließen, müssen trotzdem bei bekannt werden des Diebstahls Konfigurationsänderungen vorgenommen werden.
	c	Diebstahl des Laptop: Sofortige Maßnahmen	Durch ein gestohlenen Laptop müssen unmittelbare Veränderungen an der bestehenden System-Konfiguration vorgenommen werden um einen Zugang zum Intranet/anderen WLAN-PC's zu verhindern.

Priorisierung der QoS

Nach ausgiebigen Diskussionen über mögliche Teillösungen wurde die Notwendigkeit nach einer verbindlichen QoS-Liste deutlich, um die Lösungsvorschläge konkreter ausgestalten zu können. Die im vorangegangenen Kapitel aufgeführte Prioritätsliste unterscheidet die folgenden Prioritätsstufen (Auszug in Anlehnung an RFC2119):

- **MUST (2)**
This word, or the terms "REQUIRED" or "SHALL", mean that the definition is an absolute requirement of the specification.
- **SHOULD (1)**
This word, or the adjective "RECOMMENDED", mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
- **MAY (0)**
This word, or the adjective "OPTIONAL", mean that an item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor may omit the same item. An implementation which does not include a particular option **MUST** be prepared to interoperate with another implementation which does include the option, though perhaps with reduced functionality. In the same vein an implementation which does include a particular option **MUST** be prepared to interoperate with another implementation which does not include the option (except, of course, for the feature the option provides.)
- **SHOULD NOT (-1)**
This phrase, or the phrase "NOT RECOMMENDED" mean that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.
- **MUST NOT (-2)**
This phrase, or the phrase "SHALL NOT", mean that the definition is an absolute prohibition of the specification.

Geforderte QoS

Die im Folgenden dargelegte Priorisierung ist keine allgemeingültige Priorisierung. Sie wurde speziell auf die Bedürfnisse des Institutes ausgerichtet. Allerdings können technische Gründe immer noch dazu führen, dass gewünschte QoS in der umgesetzten Lösung nicht zur Verfügung stehen.

Aus der Sicht des Benutzers (Institutsmitarbeiter)

Nr.	Beschreibung	Erläuterung	Prio
1	Zugriff auf alle Services des Intranets.	Alle Rechner des Intranets können auf allen Ports angesprochen werden.	2
2	Zugriff auf alle Services des Internets.	Alle Rechner des Internets können auf allen Ports angesprochen werden, sofern sie auch aus dem Intranet aus angesprochen werden können.	2
3	Zugriff auf alle Services des WLAN-Netzes.	Alle Rechner des WLAN können auf allen Ports angesprochen werden.	2
4	Roaming erlaubt/möglich.	Der Benutzer kann sich bei bestehender Verbindung im Gebäude frei bewegen.	1
5	Wechsel zwischen WLAN und LAN ist Problemlos möglich.	Ein PC, der über eine Netzwerkkarte verfügt muss auch im LAN betrieben werden können. Der Wechsel zwischen WLAN- und LAN-Betrieb muss für den Benutzer einfach durchführbar sein.	2

Aus der Sicht eines Gastes

Nr.	Beschreibung	Erläuterung	Prio
6	Zugriff auf einen Teil der Services des Intranets.	Ein Teil der Rechner des Intranet kann auf bestimmten, definierbaren Ports angesprochen werden.	0
7	Zugriff auf einen Teil der Services des Internets.	Ein Teil der Rechner des Internet kann auf bestimmten, definierbaren Ports angesprochen werden.	1
8	Zugriff auf einen Teil der Services des WLAN-Netzes.	Ein Teil der Rechner des WLAN-Netzes kann auf bestimmten, definierbaren Ports angesprochen werden.	0
9	Roaming erlaubt/möglich.	Der Benutzer kann sich bei bestehender Verbindung im Gebäude frei bewegen.	0

Kompatibilität Hardware

Nr.	Beschreibung	Erläuterung	Prio
10	Access-Point: große Anzahl von PC-Karten möglich	Der Zugriff auf den Access-Point sollte auch von Karten anderer Hersteller möglich sein, wenn diese sich an allgemeingültige Standards halten (Wi-Fi, 802.11b).	2
11	PC-Karte: Windows	Für die eingesetzte Karte existieren Treiber für Windows 98, Windows NT 4.0, Windows 2000, Windows XP.	2
12	PC-Karte: Linux	Für die eingesetzte Karte existieren Treiber für Linux.	1

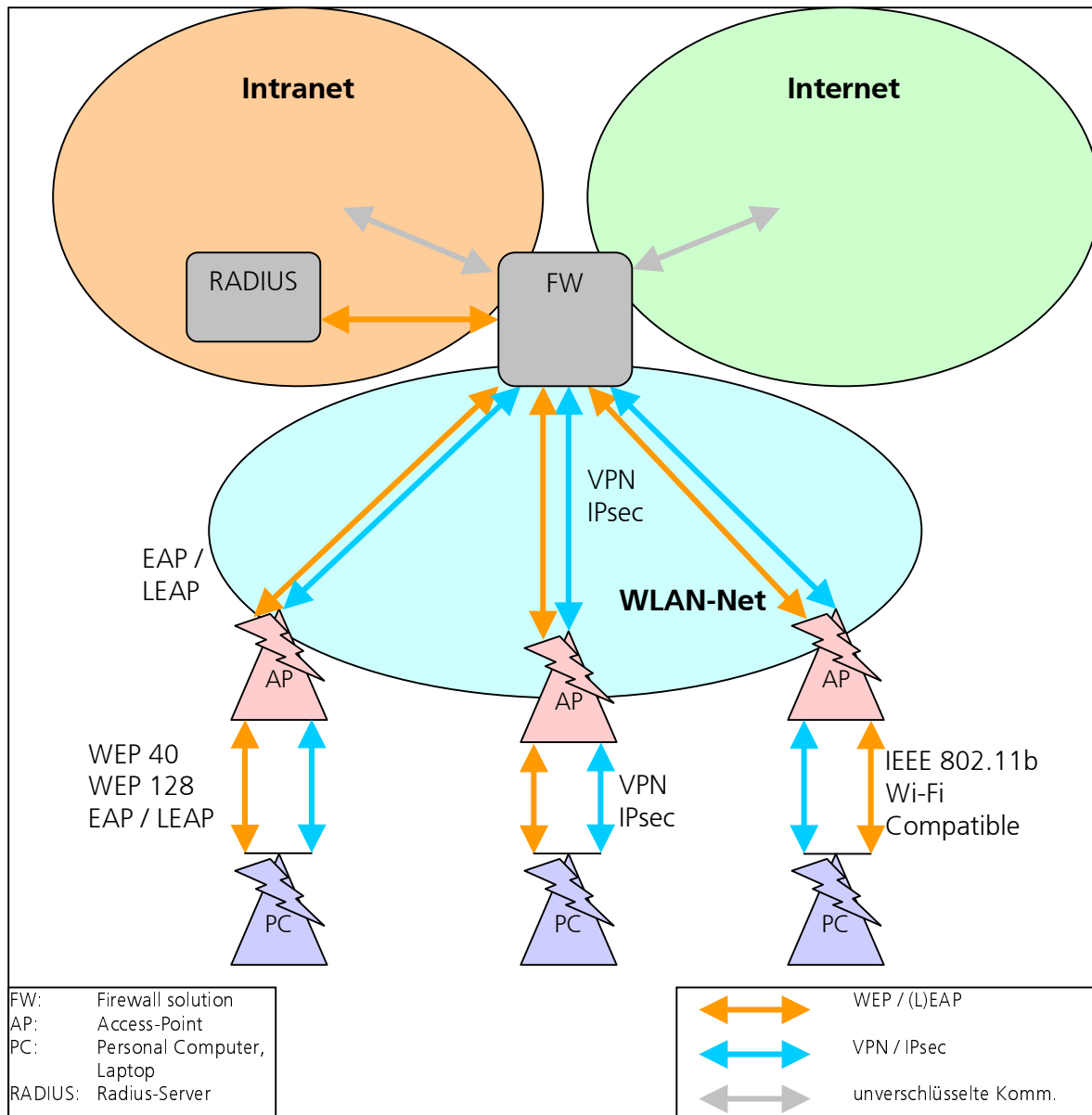
Kompatibilität Software

Nr.	Beschreibung	Erläuterung	Prio
13	Software: PC-Karte	Die notwendige Software auf dem PC läuft auch mit anderen PC-Karten, wenn diese sich an allgemeingültige Standards halten (Wi-Fi, 802.11b).	2
14	Software: Access-Point	Die notwendige Software auf dem PC läuft auch mit anderen Access-Points, wenn diese sich an allgemeingültige Standards halten.	1
15	Software: Fire-Wall (VPN-Module)	Die notwendige Software auf dem PC läuft auch mit anderen Firewalls/VPN-Moduln.	1
16	Software: Offenheit der Lösung	Die notwendige Software auf dem PC setzt keine Hardware eines bestimmten Herstellers ab Access-Point/WLAN voraus (z.B. Radius-Server, Firewall).	2
17	Software: Windows	Die notwendige Software auf dem PC läuft unter Windows 98, Windows NT 4.0, Windows 2000, Windows XP.	2
178	Software: Linux	Die notwendige Software auf dem PC läuft unter Linux.	1

Sicherheit

Nr.	Beschreibung	Erläuterung	Prio
19	Direkter Zugang zum PC (IEEE802.11-Ebene) möglich	Niemand kann über eine direkte Funkverbindung (ohne Access-Point) einen Kontakt zu einem anderen PC herstellen (auf IEEE802.11-Ebene).	0
20	Direkter Zugang zum PC (Protokoll-Ebene) möglich	Niemand kann über eine direkte Funkverbindung (ohne Access-Point) einen Kontakt zu einem PC herstellen und z.B. IP-Pakete übertragen.	1
21	Zugang zum PC: Verschlüsselung	Alle Daten, die zum PC übertragen werden oder die den PC verlassen, sind verschlüsselt und können nur von bekannten Gegenstellen ver-/entschlüsselt werden.	2
22	Zugang zum Access-Point: PC-Karte	Nur autorisierte PC-Karten haben Zugriff zum Access-Point.	1
23	Zugang zum Access-Point: Person	Nur autorisierte Personen haben Zugang zum Access-Point.	1
24	Zugang zum Access-Point: Verschlüsselung (IEEE802.11)	Alle Daten die zum Access-Point übertragen werden sind verschlüsselt (IEEE802.11-Ebene).	1
25	Zugang zum Access-Point: Verschlüsselung (VPN)	Alle Daten die zum Access-Point übertragen werden sind verschlüsselt (VPN-Ebene).	2
26	Zugang zum WLAN: Person	Nur autorisierte Personen haben Zugang zum WLAN.	1
27	Zugang zum Intranet: Person	Nur autorisierte Personen haben Zugang zum Intranet.	2
28	Zugang zum Internet: Person	Nur autorisierte Personen haben Zugang zum Internet.	1
29	Zugangsberechtigung konfigurierbar	Die Berechtigungshürden 22-28 können temporär und individuell gelockert oder verschärft werden.	1
30	Diebstahl des PC: Keine Maßnahmen	Durch einen gestohlenen PC müssen keine Veränderungen an der bestehenden System-Konfiguration (Access-Points, Firewall, VPN) vorgenommen werden um die Sicherheit des Intranet/anderer WLAN-PC's zu gewährleisten.	2

Geplante Infrastruktur



Die geplante Infrastruktur ist auf verschiedenen Ebenen gesichert. Zunächst befinden sich alle Access-Points in einem eigenen WLAN-Netz, das über eine Firewall vom Intranet getrennt ist. Der Zugang zu den Access-Points wird durch einen Radius-Server gesichert. Bei der Vertraulichkeit der Daten kommt zum einen der über den Radius-Server unter Verwendung des EAP ausgehandelte WEP-Schlüssel in Frage. Diese Art der Verschlüsselung soll allerdings nur eine Minimalsicherung für Gäste sein. Die Vertraulichkeit der Daten von Mitarbeitern wird durch einen VPN-Tunnel auf Basis von IPsec gewährleistet. Das Ende dieses Tunnels befindet sich in der Firewall.

Die aufgeführte Lösung ermöglicht die kontrollierten Abstufung von Sicherheitsaspekten. So kann für Gäste ein Zugang zum Internet geschaffen werden, der unbeschränkt und ggf. abhörbar ist, ohne die Sicherheitsanforderung von Mitarbeitern zu berühren.