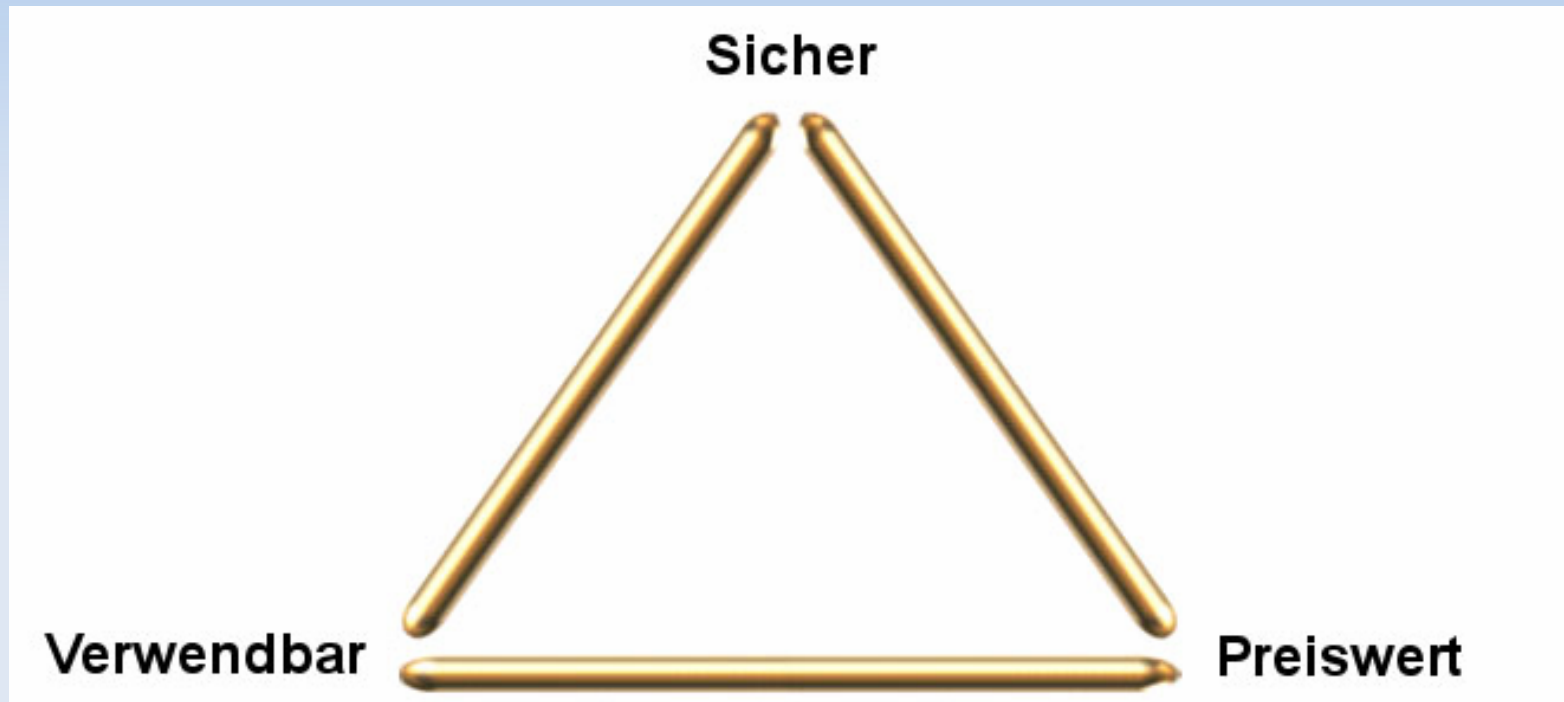


Fachbereich Medienproduktion

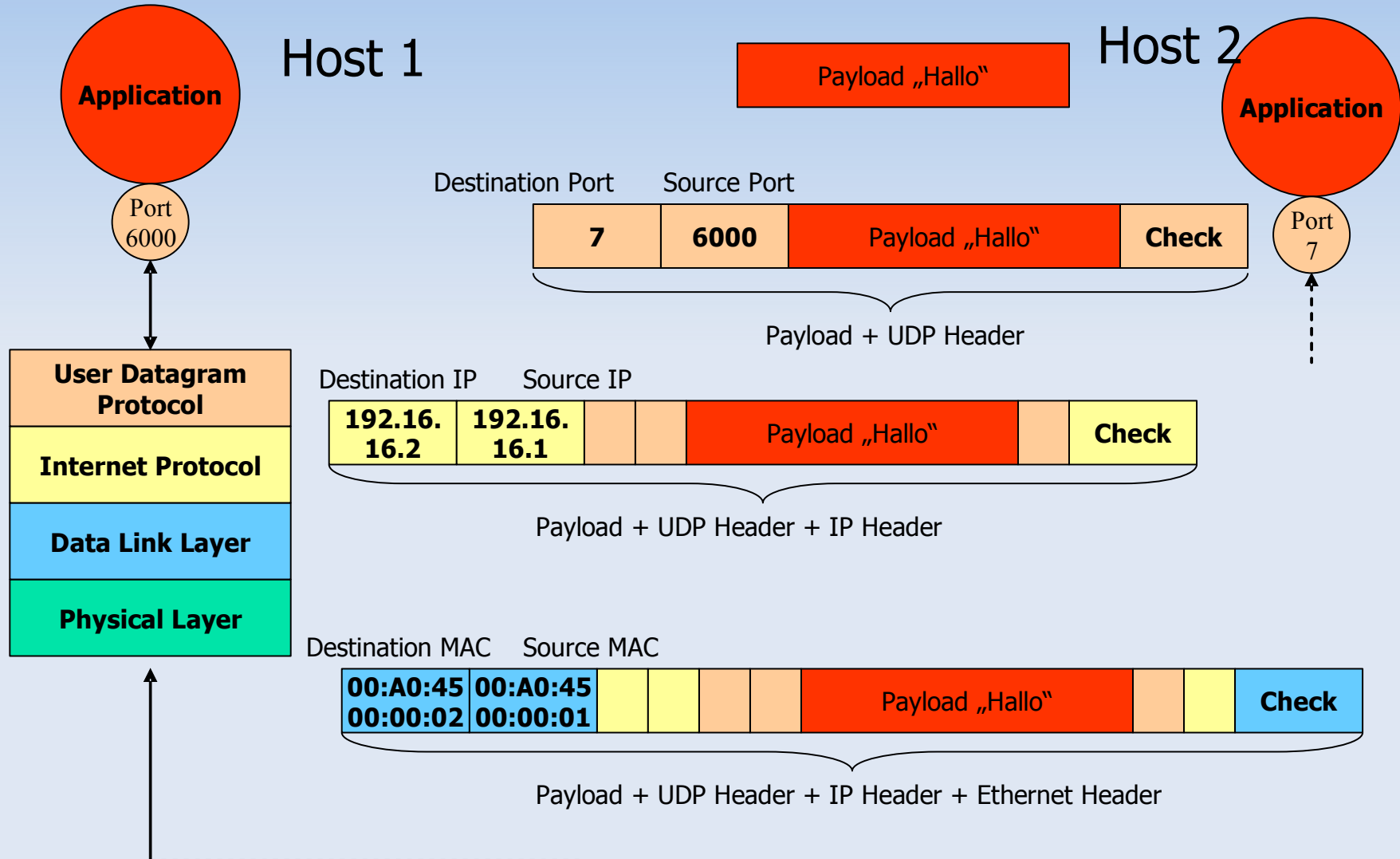
Herzlich willkommen zur Vorlesung im
Studienfach:

Grundlagen der Informatik I

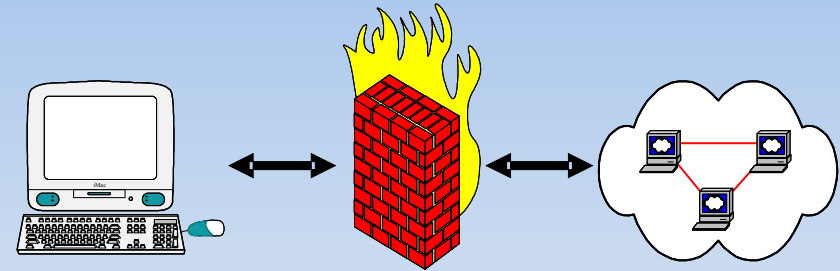
Security



Paketaufbau



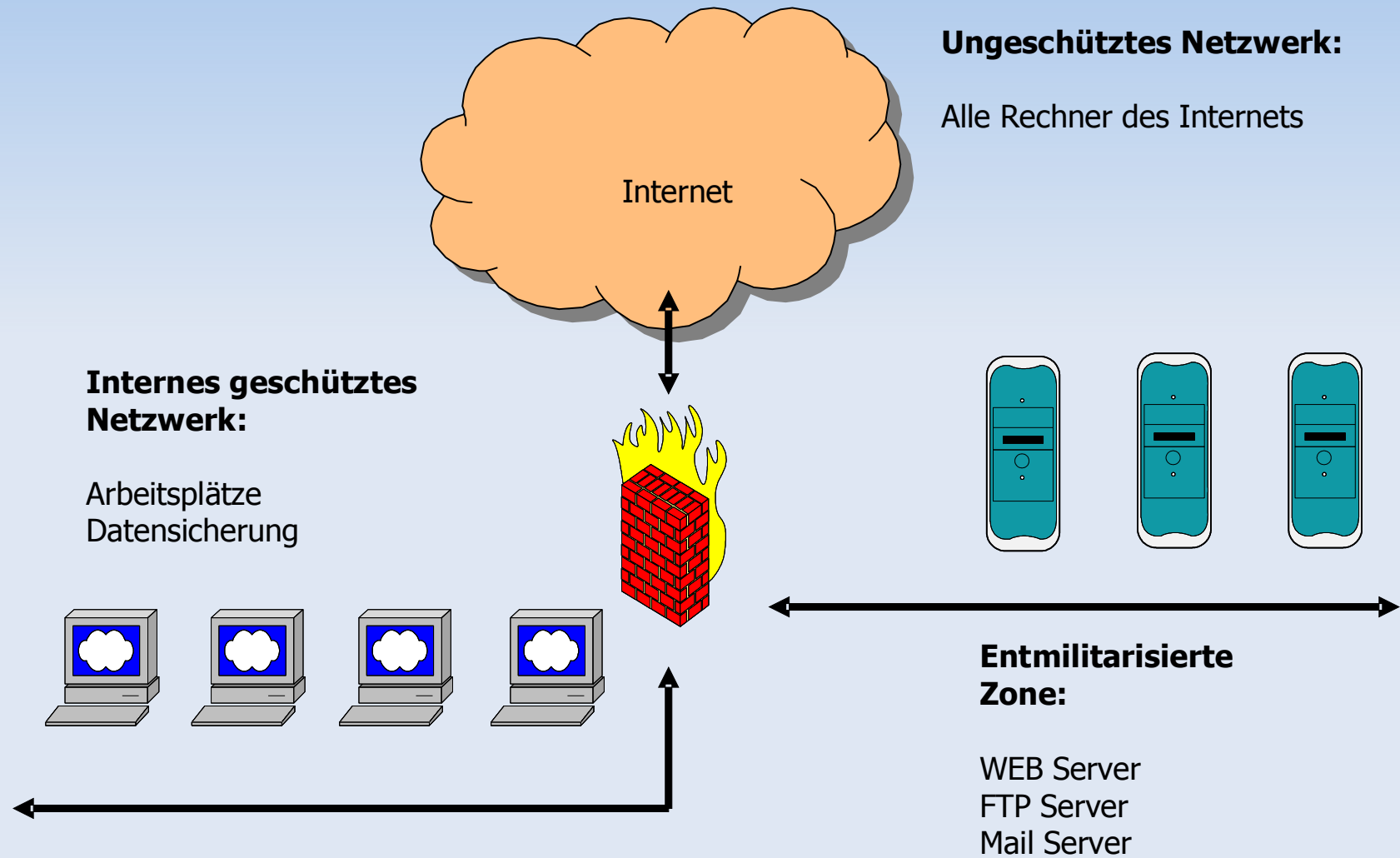
Firewalls



- Paketfilter, die Computer bzw. Netzwerke logisch voneinander trennen
- Regeln bestimmen die Pakete, die eine Firewall passieren dürfen bzw. geblockt werden sollen
- Default Regel sollte „Deny All“ sein
- Stateful Inspection
- Application Layer Gateways können auf Schicht 7 Entscheidungen über den Weitertransport von Paketen treffen

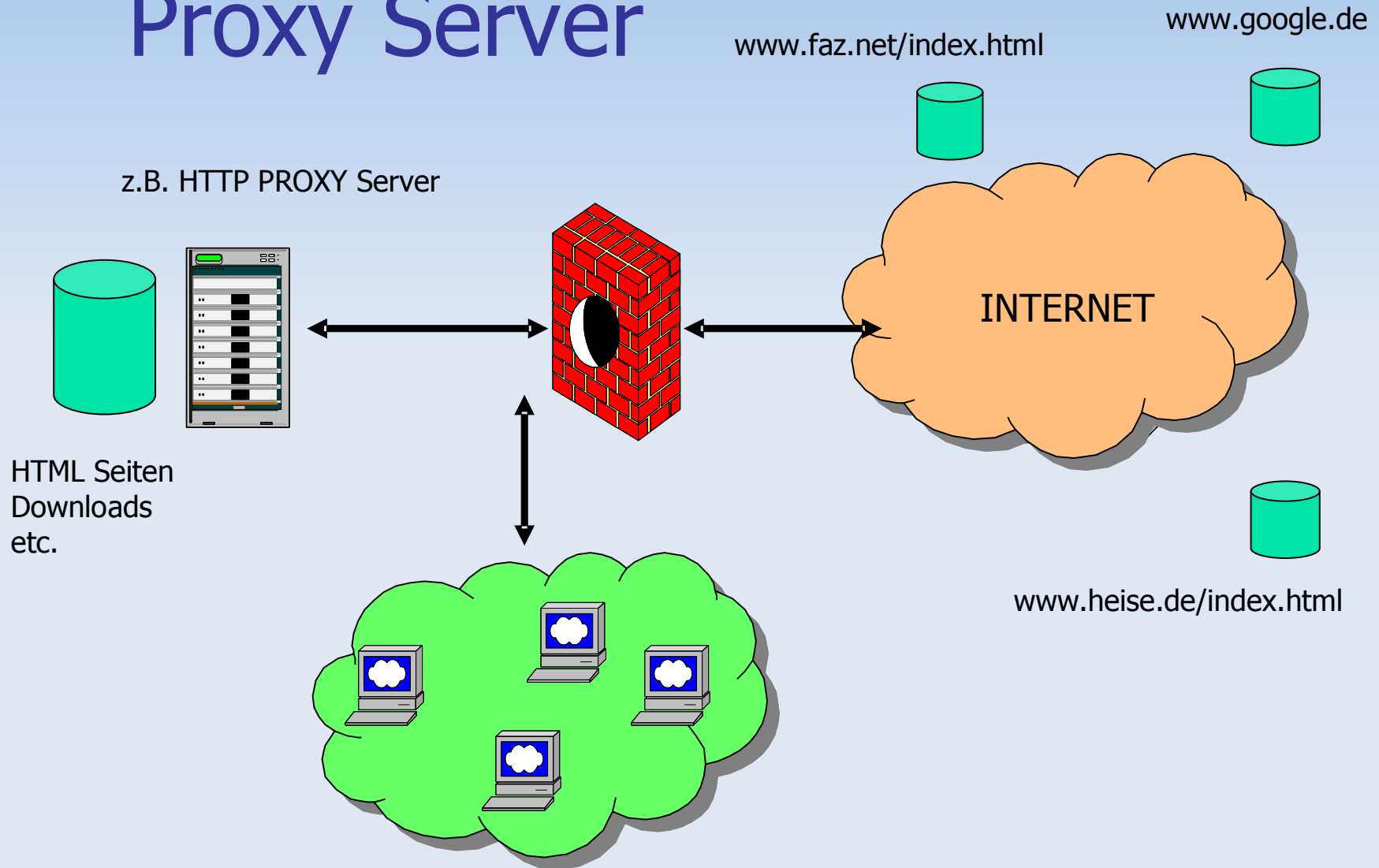
DMZ

„Entmilitarisierte Zone“



Application Layer Gateways

Proxy Server



Service Level Agreements

- Vertragspartner
- Reviews
- Zweck
- Standards
- Änderungshistorie
- Leistungsbeschreibung
- Verfügbarkeit des Service
- Service Level Kennzahlen
- Job-Planung/-Wartung
- Monitoring & Reporting
- Verantwortung Leitungserbringer
- Verantwortung Leistungsempfänger
- Externe Verträge
- Eskalationsmanagement
- Preisgestaltung
- Vertragslaufzeit
- Unterschriften

Fragen



WLAN Standards

- 802.11
 - 1997 festgelegter (historischer) Standard mit 2 Mbit/s Bandbreite
 - 2.4 GHz Band
- 802.11b
 - Erweiterung des 802.11 Standard für Bandbreite bis zu 11 MBit/s
 - 2,4 GHz Band
- 802.11a
 - Bandbreite bis 54 MBit/s
 - 5 GHz Band
 - Geringere Reichweite als im 2,4 GHz Band
- 802.11g
 - Bandbreite bis 54 MBit/s
 - 2,4 GHz Band
- 802.11n
 - Bandbreite über 100 MBit/s (300 MBit/s)
 - MIMO Technology
 - Hohe Reichweite und Rückwärtskompatibel zu 802.11g (2,4 GHz Band)

WLAN Security allgemein

- Zugangsberechtigung am Wireless Access Point (WLAN Router) ändern

Benutzernamen und Passwörter der „gängigen“ WLAN Router sind vielen Angreifern bekannt.

Vermeiden Sie nach Möglichkeit die Verwendung der bekannten Usernamen „root“ oder „admin“.

Verwenden Sie „sichere“ Passwörter.

WLAN Security allgemein

- Aktuelle Gerätefirmware verwenden

Viele Hersteller passen die Gerätefirmware den neuen Sicherheitsstandards an.

Überprüfen Sie regelmäßig ob Sie eine aktuelle Gerätefirmware verwenden.

WLAN Security Verschlüsselung

- Verschlüsselung der Daten auf der Funkstrecke aktivieren

Falls möglich aktivieren Sie die WPA (oder WPA-II) Verschlüsselung.

Verwenden Sie „sichere“ Pre-Shared Keys.

Müssen Sie WEP verwenden, so stellen Sie sicher, dass die Schlüssellänge mind. 128 Bit und ein „sicheres“, mindestens 13 Zeichen langes Passwort eingestellt ist. Ändern Sie dieses Passwort regelmäßig. WEP Passwörter sind mit einfachen Tools aus dem Internet bestimmbar.

WLAN Security 802.1x

- 802.1x ausschalten

Diese Funktion versorgt unter Umständen angeschlossene Clients automatisch mit WEP Schlüsseln.

Betrieb macht ohne RADIUS Server in der Regel keinen Sinn.

WLAN Security MAC Filter

- MAC Filter einschalten

Nur eingetragene MAC Adressen können auf den Access Point zugreifen.

Nicht sicher, da Tools die vom Hersteller einprogrammierte MAC Adresse einer WLAN Karte manipulieren können.

WLAN Security Remote Access

- Remote Zugriff unterbinden

Alle nicht benötigten Dienste des WLAN Routers sollten abgeschaltet werden (.z.B. WEB Interface, Telnet etc.)

WLAN Security IP Konfiguration

- Feste IP Konfiguration verwenden

Individuelle Subnetz IP Adressbereiche verwenden.

Werden keine Adressen per DHCP an „unbekannte“ Clients verteilt, können Angreifer nicht (so leicht) auf den Router zugreifen.

WLAN Security Konfiguration

- Konfiguration des Access Points über sichere Schnittstelle vornehmen

Die Einstellungen z.B. über eine Kabelverbindung zwischen Client und Access Point vornehmen.

Fragen

