Linux based Infrastructure

Developed by: Tomas B. Krag, wire.less.dk

Goals

- To be aware of the different roles of Linux computers in a (wireless) network
- To be able to set up a basic wireless infrastructure running Linux

Table of Contents

- Prerequisites
- Hardware and software requirements
- The role of Linux Infrastructure
- Scenario 1
- Scenario 2
- Scenario 3

Prerequisites

- To be familiar with Linux from a user's perspective
- To be capable of installing a GNU/Linux distribution of your choice
- To have a basic understanding of the command line interface (terminal) in Linux
- To have an understanding of TCP/IP networking
  - See “Advanced Networking”

Hardware Requirements

- A Linux computer is required with either
  - one Ethernet interface and one wireless interface
  - two wireless interfaces
- Scenario 3 requires some more hardware
  - will run on 500 MHz x86 with a 10 Gb hard disk (or even a 2 Gb Compact Flash Card), and 128 Mb RAM

Software Requirements

- Ubuntu Linux version 5.10 (Breezy Badger)
  - should work with other distributions
- Wireless card supported by hostap or madwifi drivers
  - Other drivers need to support Master mode (AP mode).
  - It is possible to do the setup in Ad-hoc mode which is broadly supported across all possible drivers

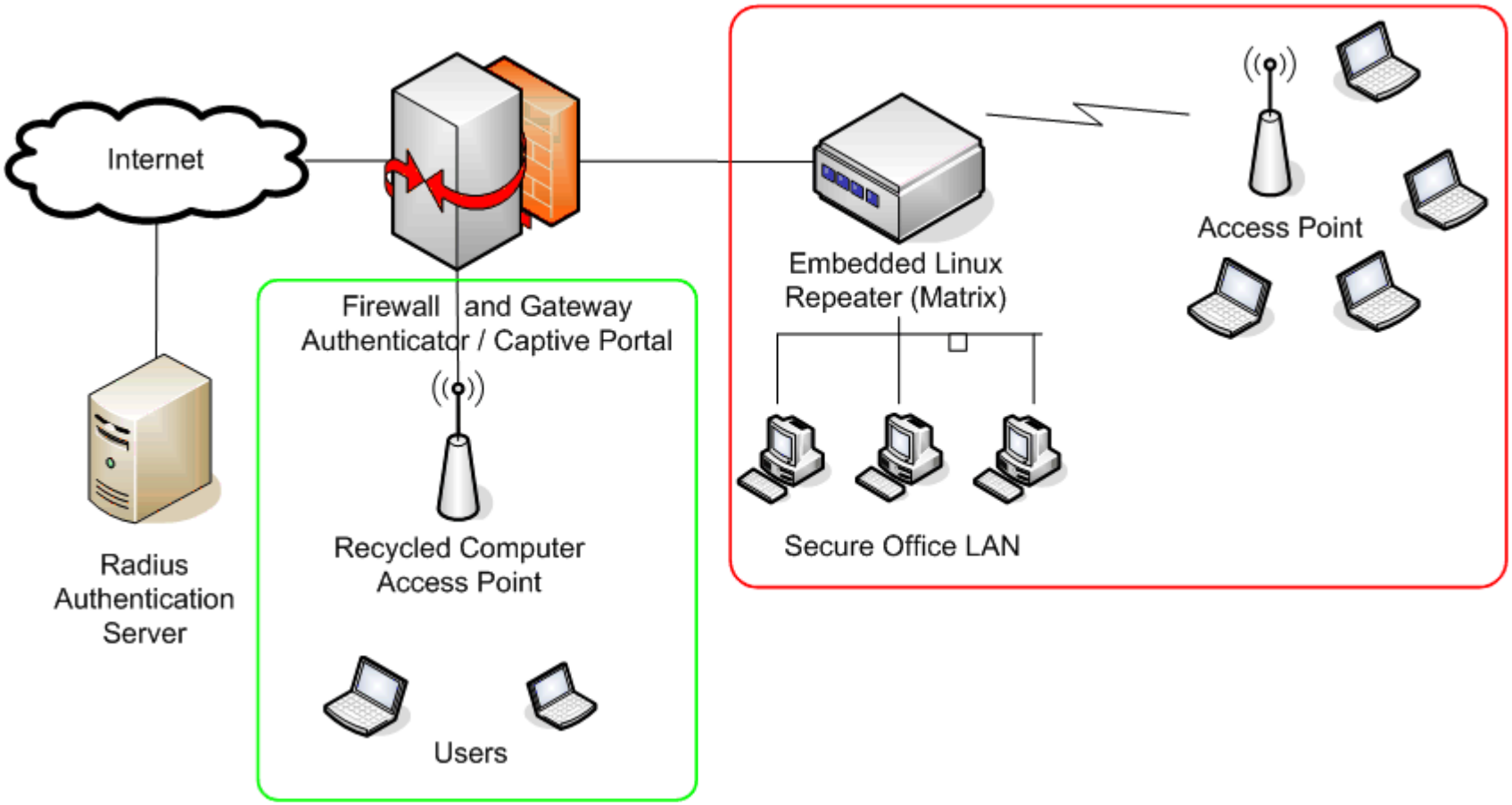
Software Requirements

- Software required to complete the three scenarios
  - wireless tools (iwconfig, iwlist commands)
  - iptables firewall
  - dnsmasq (caching DNS server, and DHCP server)

Introduction to Linux Infrastructure

- GNU/Linux Operating System (unlike Windows) gives the network administrator full access to the networking stack
  - Data Link, networking layer, application layer
- That makes GNU/Linux a powerful tool that can fill a broad variety of roles in a network infrastructure

Scenario 1-3


Internet
Firewall and Gateway
Authenticator / Captive Portal
Embedded Linux
Repeater (Matrix)
Access Point
Radius
Authentication
Server
Recycled Computer
Access Point
Secure Office LAN
Users

Scenario 1-3

- A LAN with 2 separate segments
  - open segment
  - closed system with authentication
- 3 different wireless infrastructure units
  - embedded unit like Linksys WRT54G
  - a dedicated Linux-based wireless device like Metrix MkII
  - a old recycled computer running Linux.

Scenario 1: Masquerading AP

- Especially useful in situations where you want a single access point for an office, and either
  - there is an existing dedicated firewall and gateway running Linux, and you just want to add a wireless interface
  - you have an old refurbished computer or laptop available, and prefer to use that as an access point
  - you would like a single machine to act as 2 access points (and firewall) so that you can offer both a secure network access to the intranet, as well as open access to guests

Scenario 2: Transparent bridging AP

- Can be used for either
  - a 2-radio repeater
  - an access point connected to an Ethernet, on which we want both sides of the access point to be on the same subnet

Scenario 3:
Central firewall with authentication

- Will force users to login via a captive portal web-page (user name/ password)
- The machine will have 2 network interfaces
  - connected to the Internet (eth0)
  - internal interface (eth1)

Conclusions

- After the exercise, summarize and conclude in groups what you have learn out of this unit