Jonas Lippuner

Overview

- IPCop
  - Introduction
  - Network Structure
  - Services
  - Addons
- Installing IPCop on a SD card
  - Hardware
  - Installation

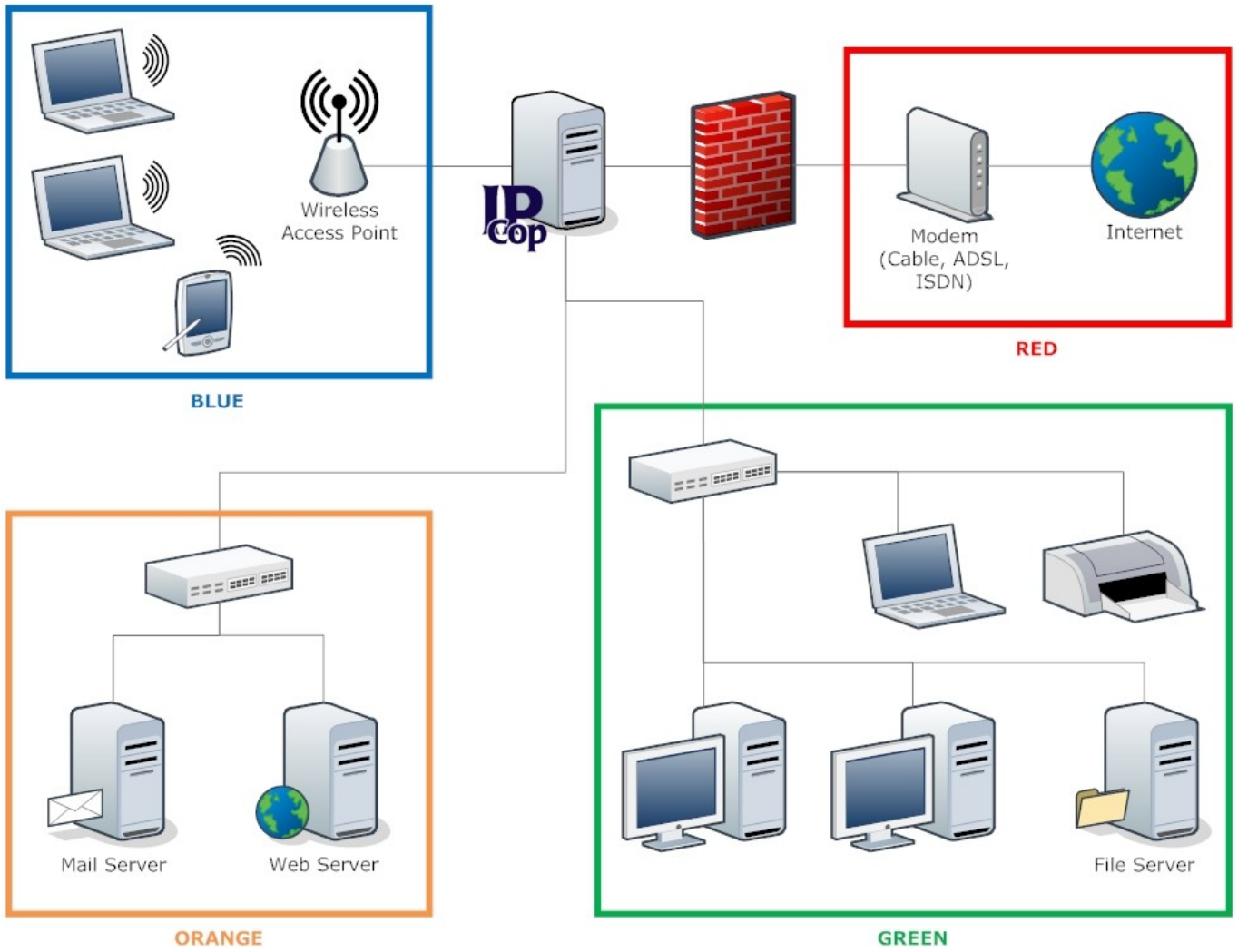
Introduction

- Linux firewall distribution
- the bad packets stop here
- SOHO users
- current 1.4.21 with kernel 2.4
- version 2.0 under development
- www.ipcop.org

Network Structure

- up to 4 physically separated networks
- RED: untrusted network, i.e. Internet
- GREEN: protected (local) network
- BLUE: optional network for wireless devices
- ORANGE: optional network for public servers (DMZ)

Network Structure



Network Structure

	IPCop	RED	GREEN	BLUE	ORANGE
RED	closed EA		closed PF, VPN	closed PF, VPN	closed PF
GREEN	open	open		open	open
BLUE	closed BA	closed BA	closed DP, VPN		closed BA
ORANGE	closed	open	closed DP	closed DP	

EA: External Access
BA: Blue Access

PF: Port Forwarding
DP: DMZ Pinholes

VPN: Virtual Private Network

Access Control

- External Access
  - allow access to IPCop from RED
- Port Forwarding
  - forward specific ports from RED to specific addresses in GREEN, BLUE or ORANGE
- Blue Access
  - list of trusted IP and/or MAC addresses in BLUE
- DMZ Pinholes
  - like port forwarding, but from ORANGE or BLUE to GREEN or BLUE

Connecting to the Internet

- Static IP
- DHCP, e.g. from a cable modem or DSL router
- PPPoE, e.g. over an DSL router configured as “bridge”
- PPTP
- USB modem
- ISDN card

Configuration

- easy-to-use web interface
- SSH access can be enabled
  - password based authentication
  - public key based authentication
- updates can be downloaded and installed through the web interface

Services

- Web proxy (squid)
  - for GREEN and BLUE
  - can be transparent for port 80
- DHCP server
  - for GREEN and BLUE
  - fixed and dynamic leases
- Dynamic DNS
  - updates RED IP to a dynamic DNS service

Services

- Host Names
  - host names can be assigned to IP addresses
- Time Server
  - IPCop retrieves time from public NTP servers and acts as NTP server for local network
- Traffic Shaping
  - assign priorities to traffic on different ports

Services

- Intrusion Detection System (Snort)
  - on GREEN, BLUE, ORANGE and/or RED
  - analyses packets for known signatures of malicious activity
  - passive protection, must be monitored by user
  - requires a lot of memory

Services

- VPN (IPSec)
  - access to GREEN and BLUE from RED and BLUE
  - secure and encrypted connection through an untrusted network
  - Net-to-net, Host-to-net (road warrior)
  - Authentication through pre-shared key or digital certificates

Addons

- new features and capabilities
- unofficial
- more than 120 addons
- www.ipcopaddons.org

Addons

- Advanced Proxy
  - extends the configuration options
  - adds user management
- BlockOutTraffic (BOT)
  - block access to RED by default and allow only according user-defined rules

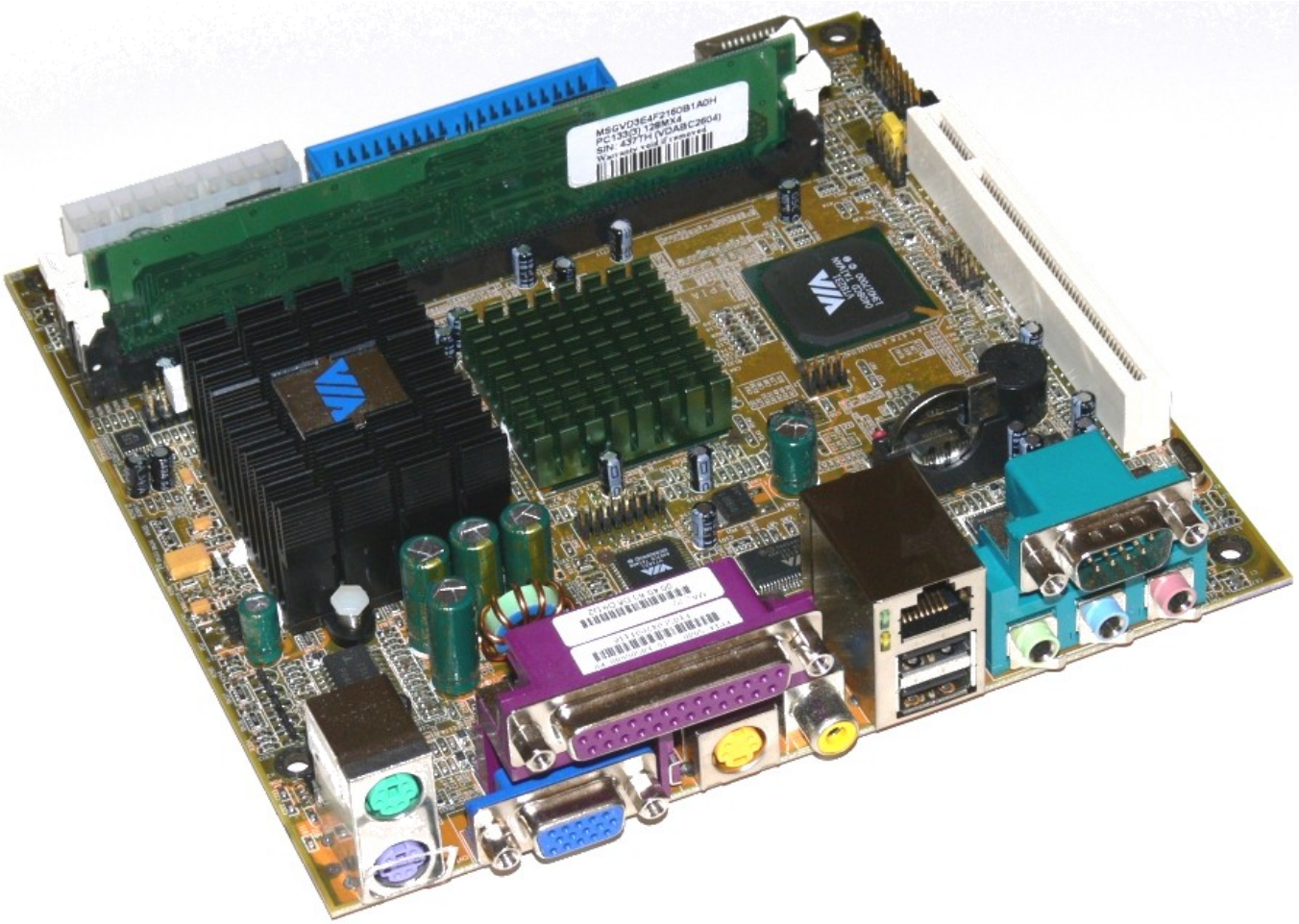
Addons

- Copfilter
  - scans email and web traffic for viruses and spam
- URL filter
  - blocks specific domains, URLs and/or files
  - includes time based access control
- WLAN-AP
  - turns IPCop into a wireless access point

Hardware Requirements

- minimal
- 32 MB RAM (more required for advanced features like IDS)
- 128 MB SD card is enough (more space required for extensive logging)
- Network adapters (number depends on network configuration)

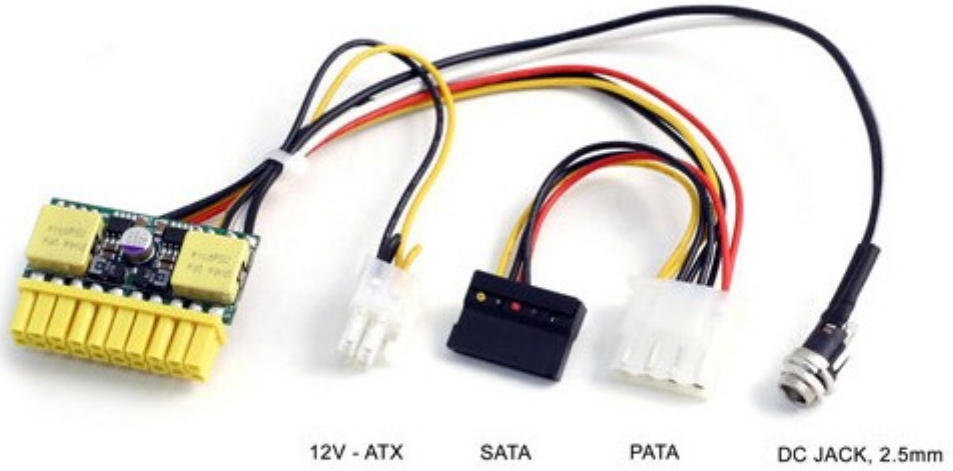
Motherboard



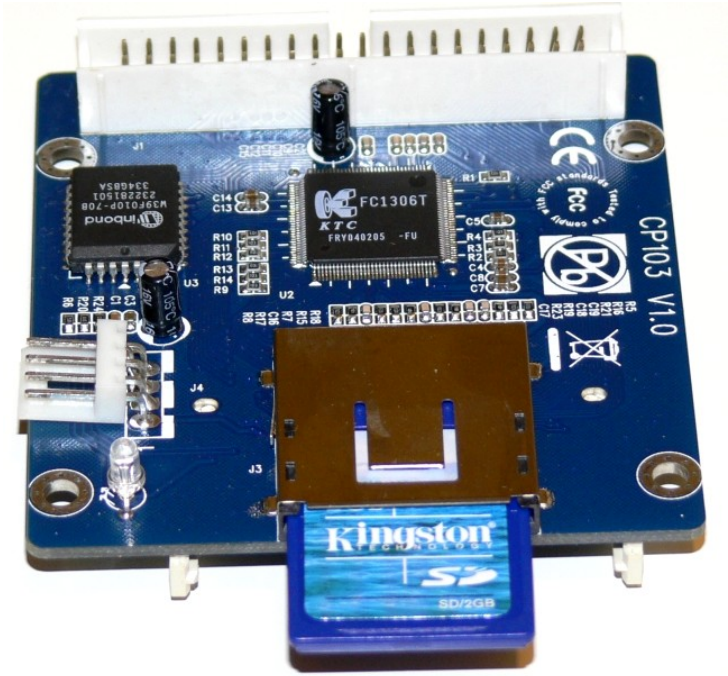
Motherboard

- Mini-ITX
- embedded CPU (533 MHz)
- 128 MB RAM
- integrated graphics chip
- 2x USB v1.1 ports
- 1x network adapter (10/100 Mbps)
- 1x PCI slot
- fanless

Power Supply



SD to IDE Adapter



Enclosure

Enclosure

- designed for Mini-ITX and PicoPSU
- up to two 2.5” drives
- 2x hidden USB ports
- wireless antenna hole
- no space for PCI card
- fanless

Network Card

Putting It Together