SPATTI

Securing Public Access To The Internet

Marya Steenman - Carlos Groen - Harm-Jan Blok - Wouter Borremans

30 Mei 2005

This page is accidentally left blank. . .

Project

Vrij publiekelijk toegankelijk tot het Internet;

- **Voor de gebruiker:**
  - **Weinig configuratie instellingen**
- **Voor de aanbieder:**
  - **Inzicht in verkeer**
  - **Actieve monitoring**

Project

- **Wel of geen encryptie?**
- **Anonieme toegang of accounting?**
- **Volledig gebruik of alleen bepaalde diensten?**
- **Welke infrastructuur?**
- **Wat gaan we meten?**
- **Hoe reguleren we het netwerk verkeer?**
- **Wat te doen bij misbruik?**

Vooronderzoek

- **Services**
- **Bedreigingen**
- **Technische mogelijkheden**
- **Implementatieadvies**

Services

- **Web, Mail, filetransfer**
- ***Geen* encryptie**

Bedreigingen

- **Misbruik door de gebruiker**
- **Bedreiging voor de gebruiker (intern)**
- **Bedreiging voor de gebruiker (extern)**

Preventie

- **Limiting, content filtering**
- **Encryptie (VPN, 802.1x, WPA, WEP etc.)**
- **Firewalling,antivirus**

Onderzochte technieken

- **Honeywall (bridge)**
- **Proxy (NAT)**
- **Smart accesspoint**

Honeywall (bridge)

- **Transparant voor de gebruiker**
- **Relatief gemakkelijk beheer**
- **Actieve monitoring**

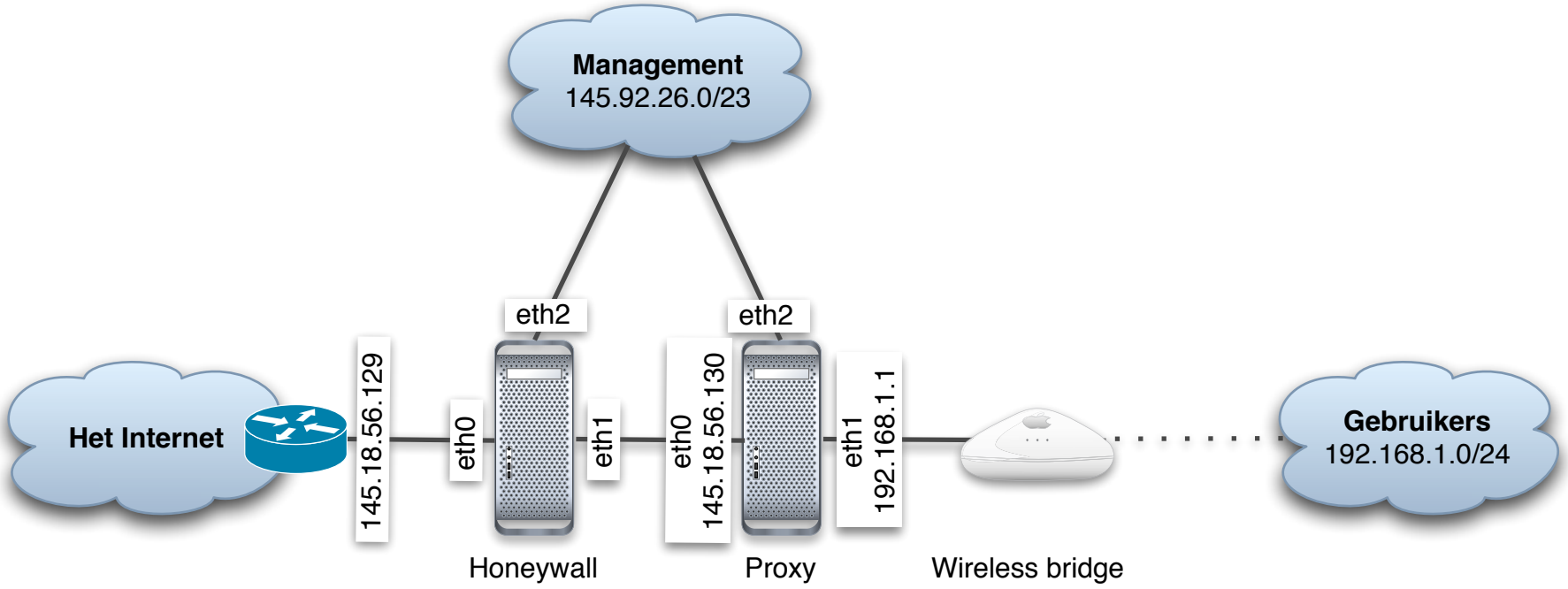
Proxy (NAT)

- **Al het verkeer via proxy**
- **Filtering van zowel in- als uitgaand verkeer (AV, Limiting)**
- **Hosts achter NAT zijn niet direct bereikbaar vanaf het Internet**

Smart accesspoint

- **Out of the box functionaliteit (firewalling, routing, NAT, etc.)**
- **Mogelijkheid tot firmware implementatie van derden (openWRT etc.)**

Test infrastructuur



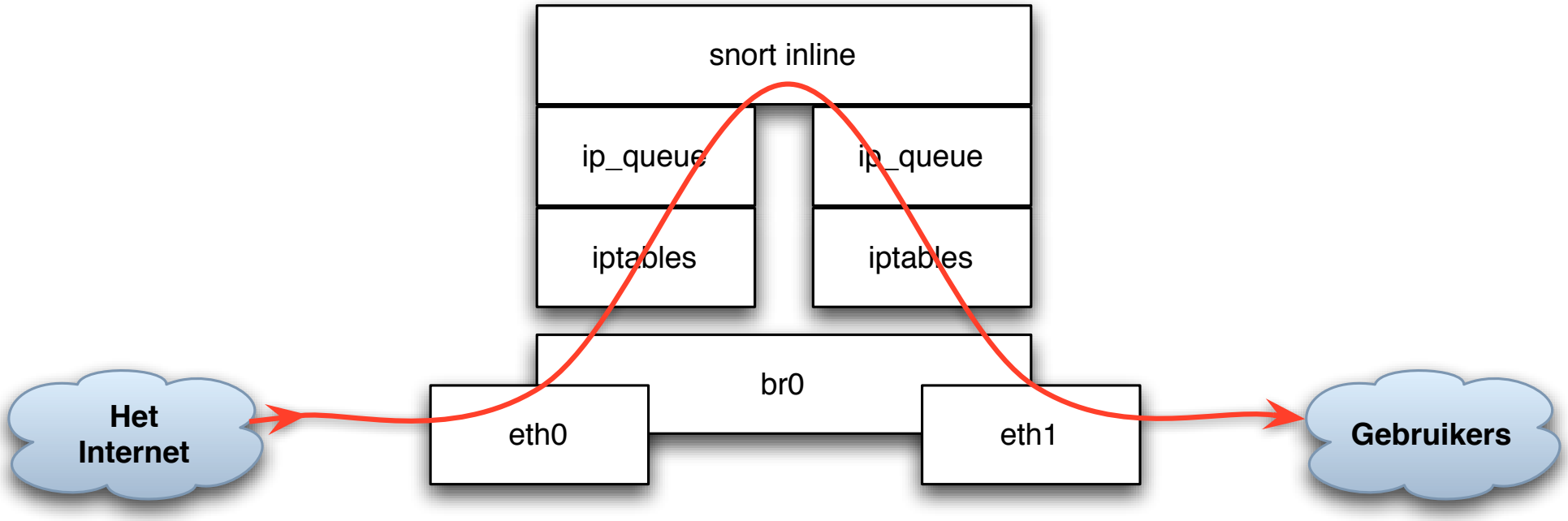
Belangrijkste componenten

- **Transparant bridge**
- **Firewall**
- **Packet inspectie**
- **Transparante proxy**

Firewall & Packet inspectie

- **Implementatie van Snort-inline en IPTables**
  - **Voordelen:**
    - **Monitoring node wordt niet gezien (bridge mode)**
    - **Realtime packet inspection**
    - **Directe samenwerking tussen IPTables & Snort**
  - **Nadelen:**
    - **Configuratie is gecompliceerd (eigen configuratie)**
    - **Afhankelijkheid van meerdere processen**

Transparante bridge



Transparante proxy

- **Implementatie van Bind 9**
  - **DNS forwarding**
- **Implementatie van Squid (HTTP)**
  - **Content filtering**
  - **Welkomspagina**
  - **Reguleren van downloads**
- **Implementatie van proxSMTP (SMTP)**
  - **Viruscheck**
  - **Limiting**

- **Implementatie van p3scan (POP)**
  - **Viruscheck**
  - **HTML Striping (web code bug)**
  - **Limiting connectie rates**

Conclusie

- **Haalbaar maar gecompliceerd**
- **Proxy en bridge mode conflicteren met elkaar**

Implementatieadvies

- 1 machine
  - NAT
  - Firewall
  - Honeywall (snort inline)
  - Proxy's

Overwegingen voor de toekomst

- **Accounting (SMS etc.)**
- **Encryptie (VPN)**
- **2e accesspoint (802.1x)**

The end

. . . of end 2 end?