



# Sektornet security issues

[tommy.ravn.jensen@uni-c.dk](mailto:tommy.ravn.jensen@uni-c.dk)

# Sektornet ISP services in brief

- Internet access
  - "Closed user group" within TDC (Not MPLS VPN!)
- 
- Managed security: Security concepts, IOS firewall, CPE configuration (ACLs, NAT, policy maps, VLANs etc.), enrollment, Wireless LAN, IOS upgrades
  - Self-service: Toolbox (demo DNS, VPN)
  - Remote access: ipsec VPN gateway, certificates
  - DNS (resolver and hosting)
  - "all inclusive" help-desk, single point of contact
  - CPE service

## Major "revolutions" – last 5 years

- Real firewall: Improved security
- Leased lines -> ADSL
- Metropolitan area networks: Losing customers
- Self service
- Wireless LANs: Security
- Fibres to the home: New providers

# Security issues

- Management access
- Filtering
- Security model and group policies
- IOS vulnerabilities
- Wireless LAN
- Combining Sektornet managed security with Forskningsnettet access
- Abuse handling

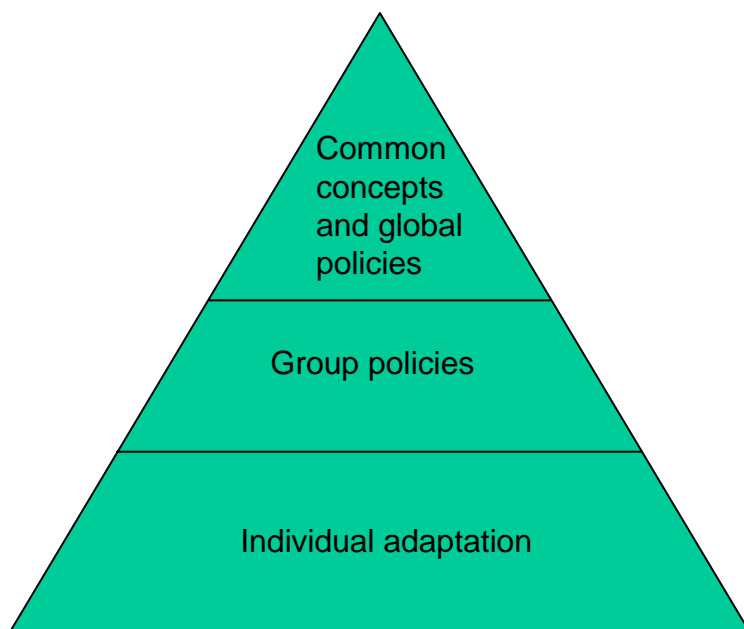
# Management access

- Shell/interactive setting and troubleshooting: Telnet (no ssh!), tacacs+
- Configuration update and IOS upgrade: SNMP, tftp
- Performance monitoring: SNMP
- Closed user group: Community strings etc. in clear text.
- ADSL: Management access tunneled via LAN: SecurID, fine grained authorisation, full command log

# Filtering

- Mainly layer 3-4 based on concepts
- Anti ip-spoofing
- Early days of P2P: Static “Kazaa filter”
- Now: P2P filtering (NBAR protocol detection and filtering)
- Simple filter settings based on concepts and groups: Toolbox (demo)
- Anti-spam (SkoleKom), Anti-virus (local)
- No content filtering

# Security models



- Management system developed from scratch: Full control. Data model fits conceptual model.
- Overall concept defines security levels: Adm, Paed, DMZs, Wireless
- Global filtering: Anti ip-spoofing, ICMP limitations.
- Groups: Schools with similar or identical security needs. Partly impl. in management system (demo)
- Individual adaptation: Toolbox

# IOS vulnerabilities

- Remote upgrade of different CPE platforms – risky business
  1. Risk assessment -> Threats and impact. Concerns? Plan! Inform!
  2. Workaround (safe)
  3. Upgrade (“unsafe”) – schools can block and upgrade themselves through the Toolbox. CPE service provider in alert.

# Wireless LAN

- Easy to get up and running **without** security config.
- Virus
- Unauthorized access
- Bypasses firewall
- Sniffing (??)
- Solution 1: Web-based authentication (CPE based hotspot)  
Restricted access until auth. Works for all accesspoints - i.e. for existing wireless networks as well. Local/central radius
- Solution 2: “Integrated wireless security“, management and helpdesk. Only Cisco APs, WPA integrated with Windows AD and all security zones. VLAN.

# Sektornet managed security and Forskningsnettet access

- All aspects of managed security
- No closed user group: Protect (encrypt) confidential data
- Protected management access
- Ipv4 tunnelling of secure Sektornet subnets
- Support interface

# Abuse handling

- Service-minded approach
- Aim to handle **all** complaints
- Tailored ticketing system (based on RT) => Links related cases and combines incident reports with management data