NAC at a Campus University

UTwente key figures

- Campus university, 146 ha (~ 200 soccer fields)
- 12k students, 3800 FTE
- IT dept serves:
  - Research
  - Education
  - Campus life
    - Sports & culture
    - 2500 dorm rooms

UT network key figures

- 2x 100G IP uplink SURF, 4x 10G IP + Services
- 2 data centers on Campus
- 500+ access switches (23k access ports)
- 2200+ WiFi APs

UT network preferences

- Open standards
- Multi vendor network
  - Datacenter: Cisco → Arista
  - Firewalls: Cisco → Fortinet
  - Routers: Cisco → Juniper MX
  - WiFi: Cisco → Juniper MIST
  - Access: HP (ProCurve) → Arista? Cisco?

NAC products used by UTwente

- WiFi: Radiator (802.1X and MAC auth)
  - Proxying AuthN to NPS for @utwente.nl identities
  - Proxying AuthN to SURF for other identities
  - Authorization on Radiator itself
- LAN: Tesorion Immunity (Port security)
  - Dutch solution, managed “black box” appliances
  - Relatively powerful wrt policies
  - ...but we use them with Port Security only, no RADIUS

Why use NAC

- Perimeter security is not enough
- Avoid lateral movement
- Separate unrelated groups of client systems
  - The whole network is distributed “policy enforcement point”
    - Security features on switches, ACLs on routers, using VRFs, stateful firewalls in traffic path, etc etc
  - NAC is the “policy decision point”

Types of network clients

- ~ 70 distinct groups of clients / network devices
- Largest group is “mobile LAN hosts” (registered, known owner): 32k registrations
- Workstations (staff & student) with fixed IP: 2600
- Infrastructure: 1760 regular APs, 870 hospitality AP
- Generic IoT devices on LAN: 160
- Building automation: 660
- Building security: 300 cameras, 90 access control
- AV over IP: 440
- Video studio: 40
- Hotel equipment: 75 IPTV, 80 IP phones
- 130 printers, 75 people counters, 133 narrowcasting screens
- Cleanrooms & 20+ labs with dedicated equipment VLANs (some labs 40+ devices)
- Etc, etc, etc

What are we looking for

- Preferably open source NAC
- Client isolation for certain client types
  - Printers, vending machines, locker banks etc
- Flexible limiting # clients/port
  - Generally one client / port
  - Exceptions for AV equipment and building automation

Cooperation

- Exchange experiences about NAC on Campus
- Potentially develop a more powerful system together?