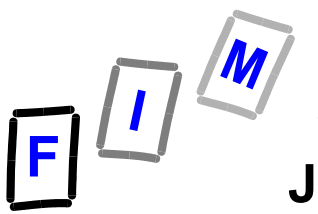
Secure WAN communication for teleworkers. A case study.

Presentation at the ICETA 2001, Kosice, Slovak Republic

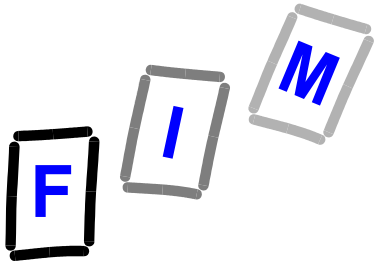
(http://www.fim.uni-linz.ac.at/iceta2001)

o. Univ.-Prof. Dr. Jörg R. Mühlbacher

Dipl.-Ing. Rudolf Hörmanseder

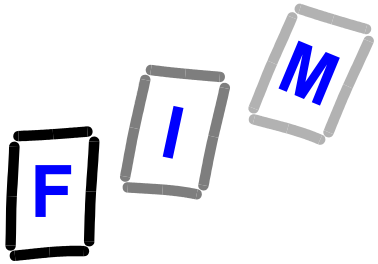


Institute for Information Processing and Microprocessor Technology (FIM), Johannes Kepler University Linz, Austria



abstract (the situation)

- typical situation:
  - ➡ tele-workers and freelancers
  - ➡ often / sometimes work for several companies from their
  - ➡ private home office (SOHO).
- main emphasis:
  - ➡ low cost
  - ➡ sufficient security level
  - ➡ acceptable for both tele-workers / freelancers and contracting companies



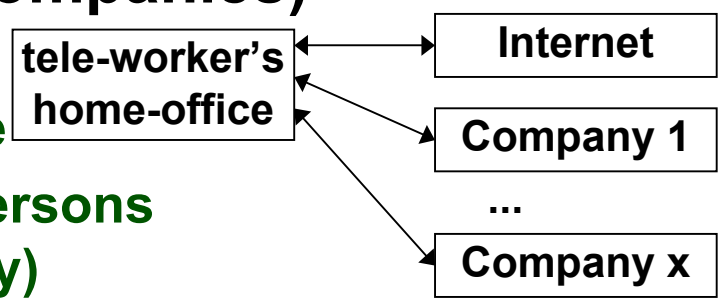
introduction (permanent change)

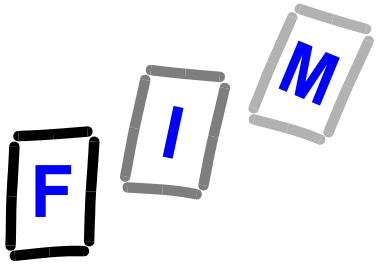
- premise of a social change:
  - ➡ new forms of labour
  - ➡ more flexible contracts of employment
  - ➡ flexible working conditions and flexible working hours
  - ➡ short-time employment
  - ➡ working for different companies simultaneously
  - ➡ self-employment
  - ➡ job and private life merge more and more
- IT structure has to deal with these changes ...
  - ➡ tele-offices
  - ➡ online all the day

general requirements for tele-workers [1]

- reuse of resources and scalability
  - ➡ buy (only) on demand
  - ➡ do not follow IT-configuration of contracting company / companies
  - ➡ use older equipment because of low utilisation rate

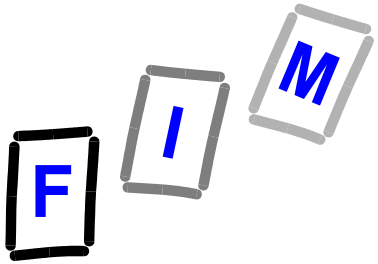
- interleaved work (tele-office ➔ companies)
  - ➡ working on contracts with more than one company at the same time
  - ➡ especially true for self-employed persons (because they act like/as a company)
  - ➡ online connection to every contractor
  - ➡ connection must be independent of IT platforms (-> open standards)





general requirements for tele-workers [2]

- access from company to home-office (tele-office ← company)
  - ➡ tele-workers sometimes work - “physically” - at a company’s premises.
  - ➡ (at least) limited access to their resources at home (e.g. for downloading files, ...)
  - ➡ trusted access from company to tele-office (to some extent)
- general Internet access
  - ➡ self-advertising
  - ➡ information search
  - ➡ e-mail
  - ➡ ...

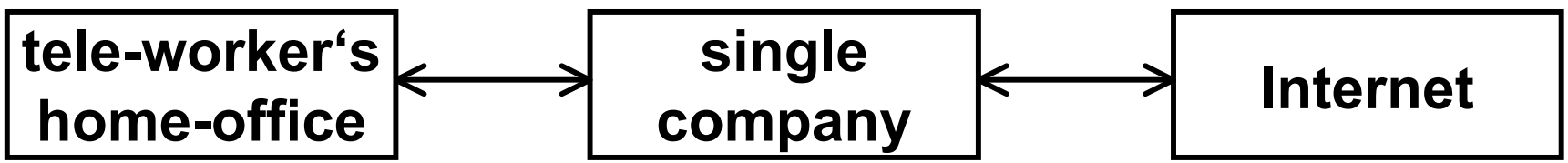


general requirements for tele-workers [3]

- personal security issues
  - ➡ tele-offices mostly are online all the day
  - ➡ sensible company data
  - ➡ tele-workers (especially self-contractors) have to protect her/his intellectual work against general espionage
  - ➡ limit access from company to SOHO network (according to agreement)
- we recognise the different security needs
  - ➡ high: self-employed persons
  - ➡ not so high: employees of a company

general requirements for tele-workers [4]

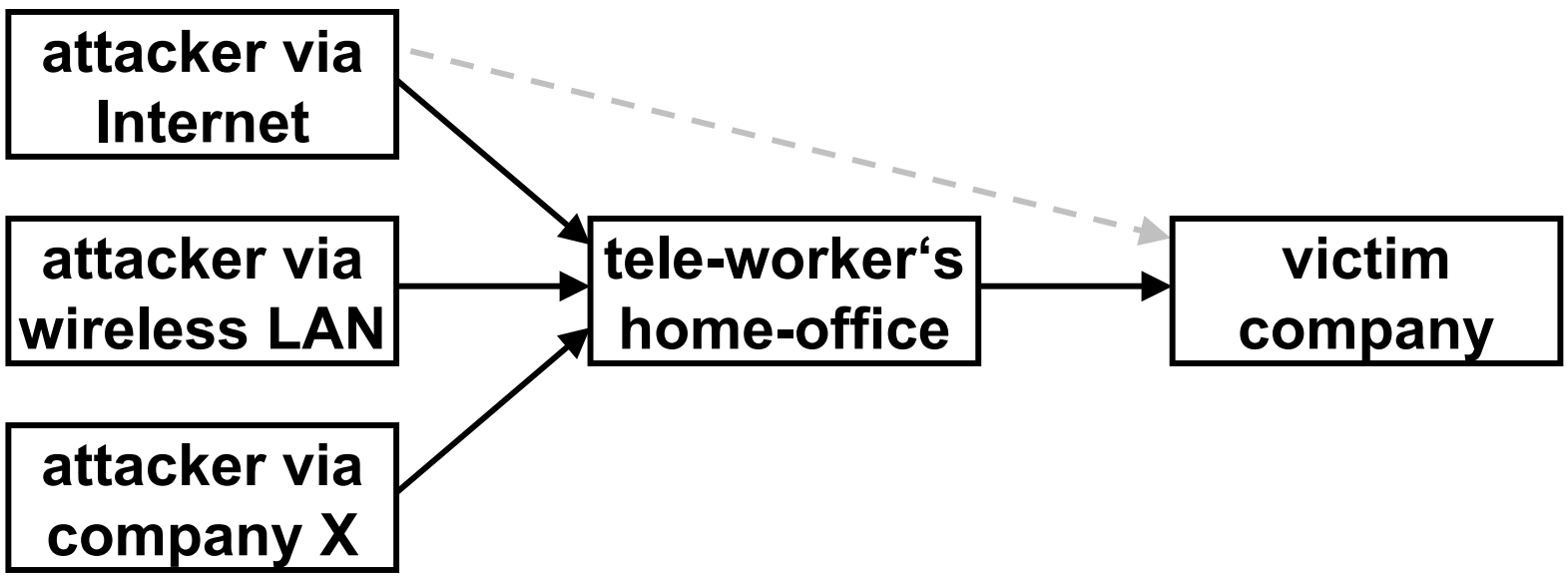
- employers / contractors security issues
  - ➡ same as any sub-network at the companies premises
  - \+ connection to sub-network
  - \+ no direct physical access to the sub-network
  - \+ no direct logical access to parts of the sub-network
  - \+ physical security of sub-network
  - \+ additional access lines to other companies
  - \+ access to Internet not controlled by company‘s security policy

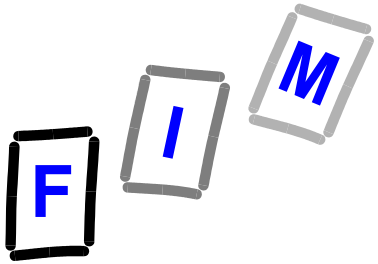


?????

general requirements for tele-workers [5]

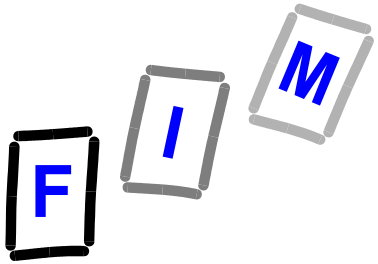
- employers / contractors security issues
  - ➡ possible indirect hacking attacks because of trusts between „tele-office“ and „victim company“





steps towards a stable solution [1]

- LAN at the home office
  - ➡ small
  - ➡ secret business data
  - ➡ physical security (+ e.g. WLANs)
  - ➡ workstations and servers at the home office: the trend is more workstations, fewer servers (office is online all the day)
- choosing the Internet Service Provider (ISP)
  - ➡ SOHO is in some part equal to private use, BUT
  - ➡ different contracts
  - ➡ services (out-sourcing of servers for Web, Mail, ...??)
  - ➡ bandwidth (download and upload)
  - ➡ availability (quality of service)

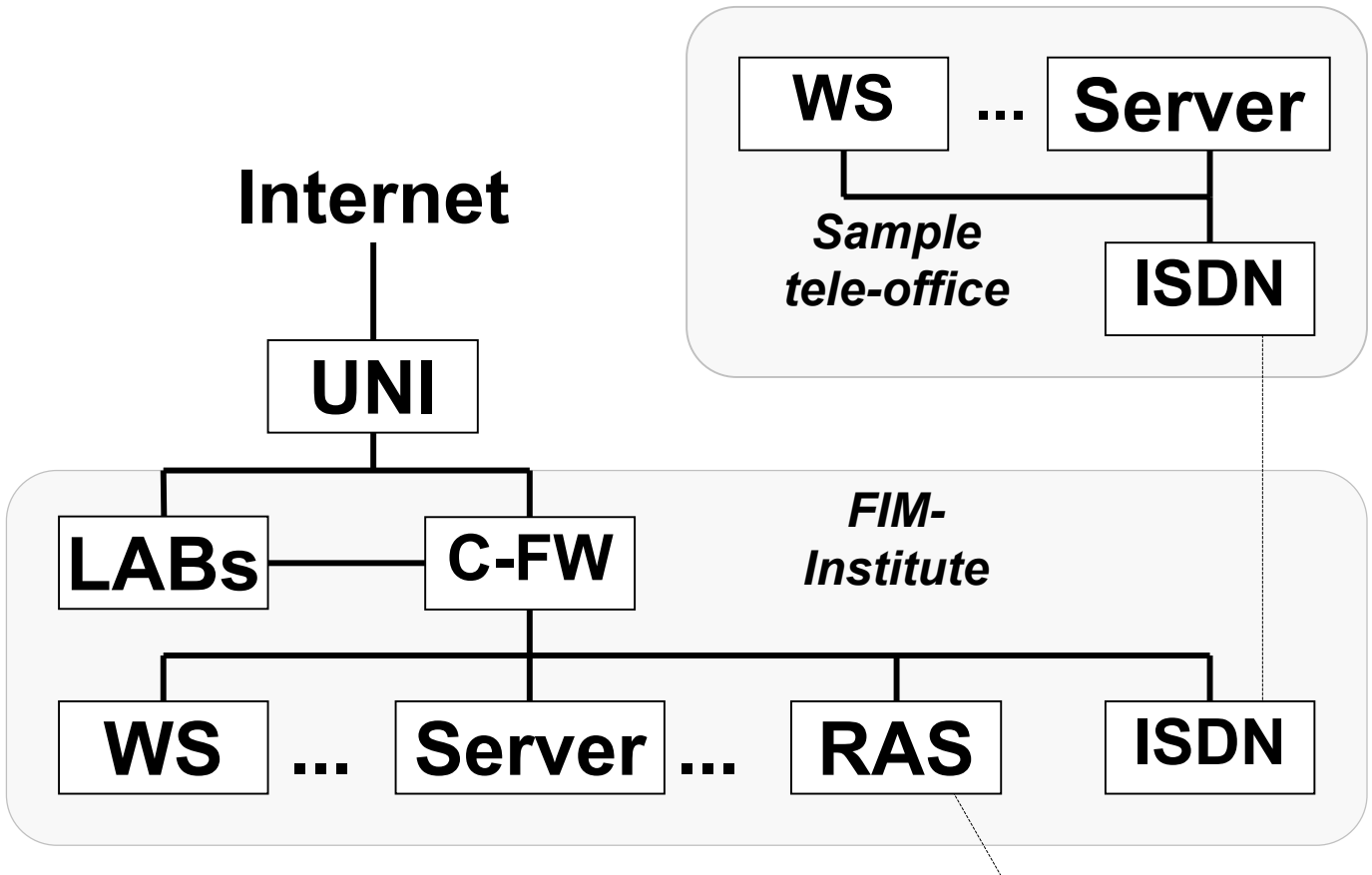


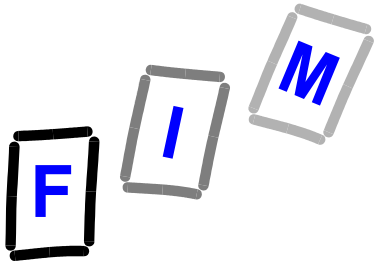
steps towards a stable solution [2]

- standard PTT-services to increase availability
  - ➡ using older equipment (ISDN telephone, ISDN-adapter, ...)
  - ➡ simple and cheap backup line
- firewall
  - ➡ dedicated special system “appliance” as firewall.
  - ➡ real bastion station
  - ➡ not used as general / generic computer
  - ➡ we do not prefer “Personal Firewalls” for ensuring these functions
- encryption issues (VPN)
  - ➡ all communication to company should be encrypted
  - ➡ usage of firewall as VPN endpoint
  - ➡ independent of current OS and hardware: IPSec, IKE, ...

case study in detail [1]

- history of the network at FIM



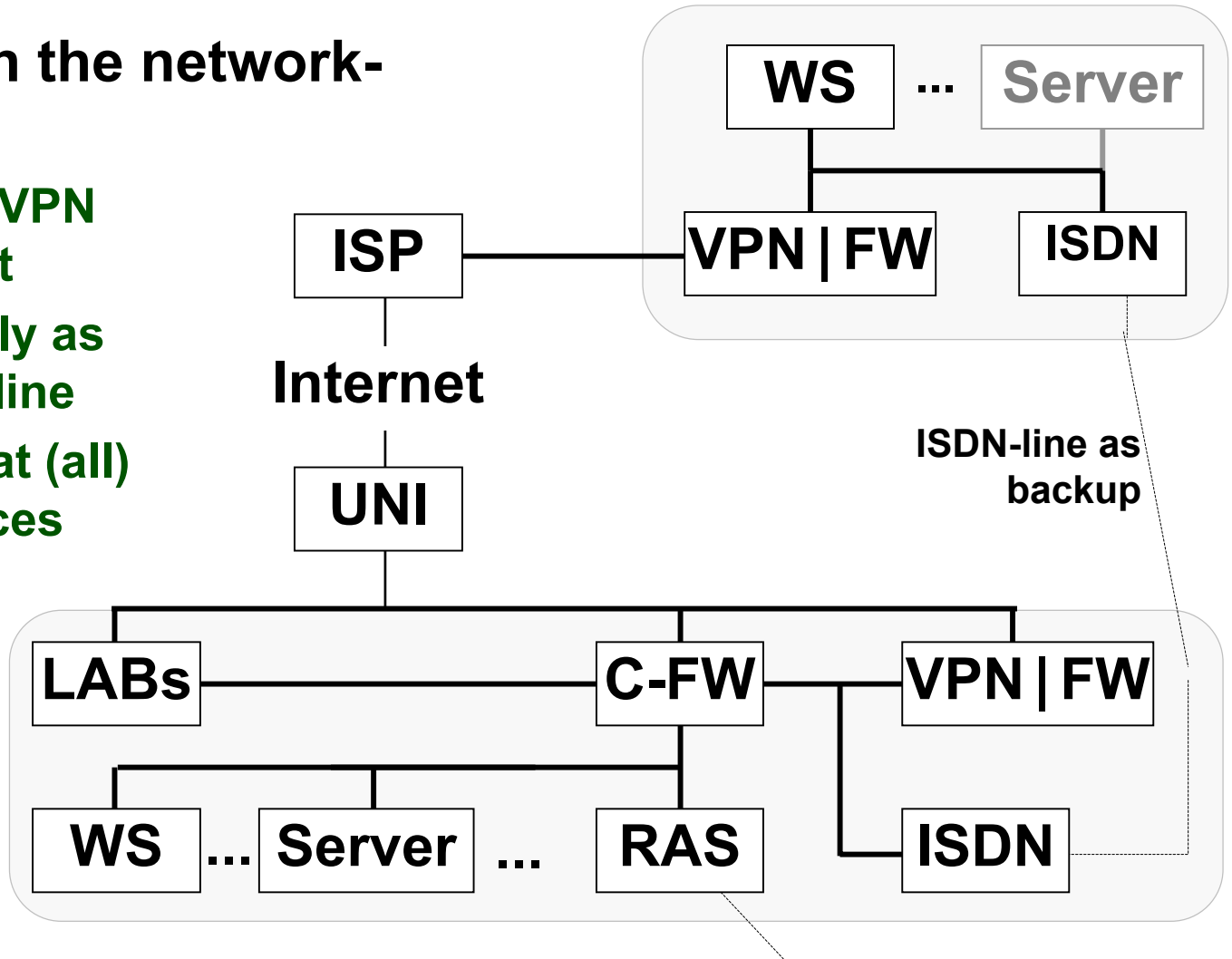


case study in detail [2]

- selecting the Internet Service Provider
  - ➡ cheap business solution
  - ➡ multiple fixed IP addresses
  - ➡ contract permits servers
  - ➡ ...
- additional hardware and software
  - ➡ firewall „appliance“
  - ➡ SonicWall
  - ➡ favourable price (especially for university education)
  - ➡ previous good experiences
  - ➡ SonicWall „Tele“ and/or „Tele2“
  - ➡ web-based administration
  - ➡ “Stateful Inspection” and NAT or VPN (until September 2001)

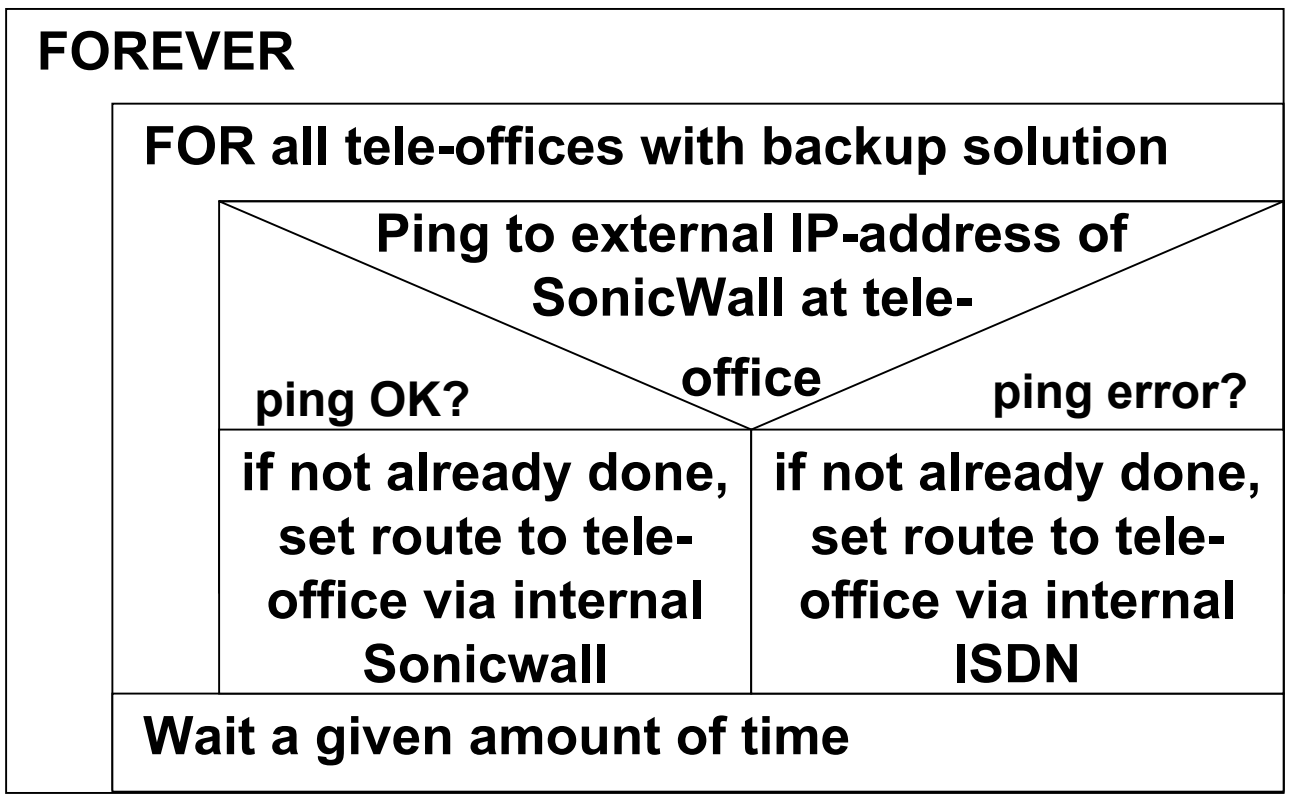
case study in detail [3]

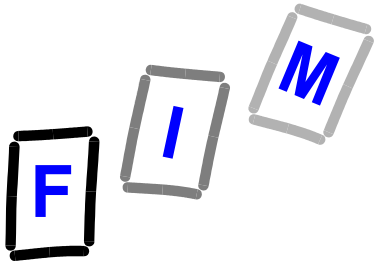
- changes in the network-structure
  - ➡ internal VPN endpoint
  - ➡ ISDN only as backup line
  - ➡ firewall at (all) tele-offices
  - ➡ routing issues
  - ➡ ...



case study in detail [4]

- routing issues
  - ➡ very simple „active routing“ via ping
  - ➡ see http://www.fim.uni-linz.ac.at/iceta2001 for details





conclusion and summary

- **security:**
  - ➡ **SOHO without firewall = nightmare**
  - ➡ **VPN encryption („privacy“) is very important**
  - ➡ **„firewall appliance“ has many benefits but also some drawbacks**
- **backup line**
  - ➡ **existence of backup line via ISDN is reassuring**
- **different security requirements:**
  - ➡ **tele-workers who are employees of a company versus self-employed contractors**
  - ➡ **Security range from employee doing tele-work to full B2B solution. (flexibility – security - ...???)**

future steps

- latest software release for Tele2 supports Firewall+NAT-functionality and VPN together
- additional security functions to protect tele-offices „against“ the network of the institute / company

→upgrade stations to SonicWall Tele2

→also routing has to be changed (will be simpler)