Remote Access Services

Security Architecture Notes

Martin Fredriksson

m@crt.se

2001-10-17

Varför säkerhet? Vilken säkerhet?

- **Behov av säkerhet?**
  - Större beroende av (gamla och nya) tjänster ⇨ “inbyggda” / “automatiska” behov av högre säkerhet/kvalitet
  - Ex: IP-telefoni, styrning av värmepanna, lördagsfilmen, ...
- **Hotet?**
  - Antalet attacker ökar.
  - Verktyg för *script-kiddies*
  - Bredband: alltid på?
  - Det “uppkopplade hemmet”?

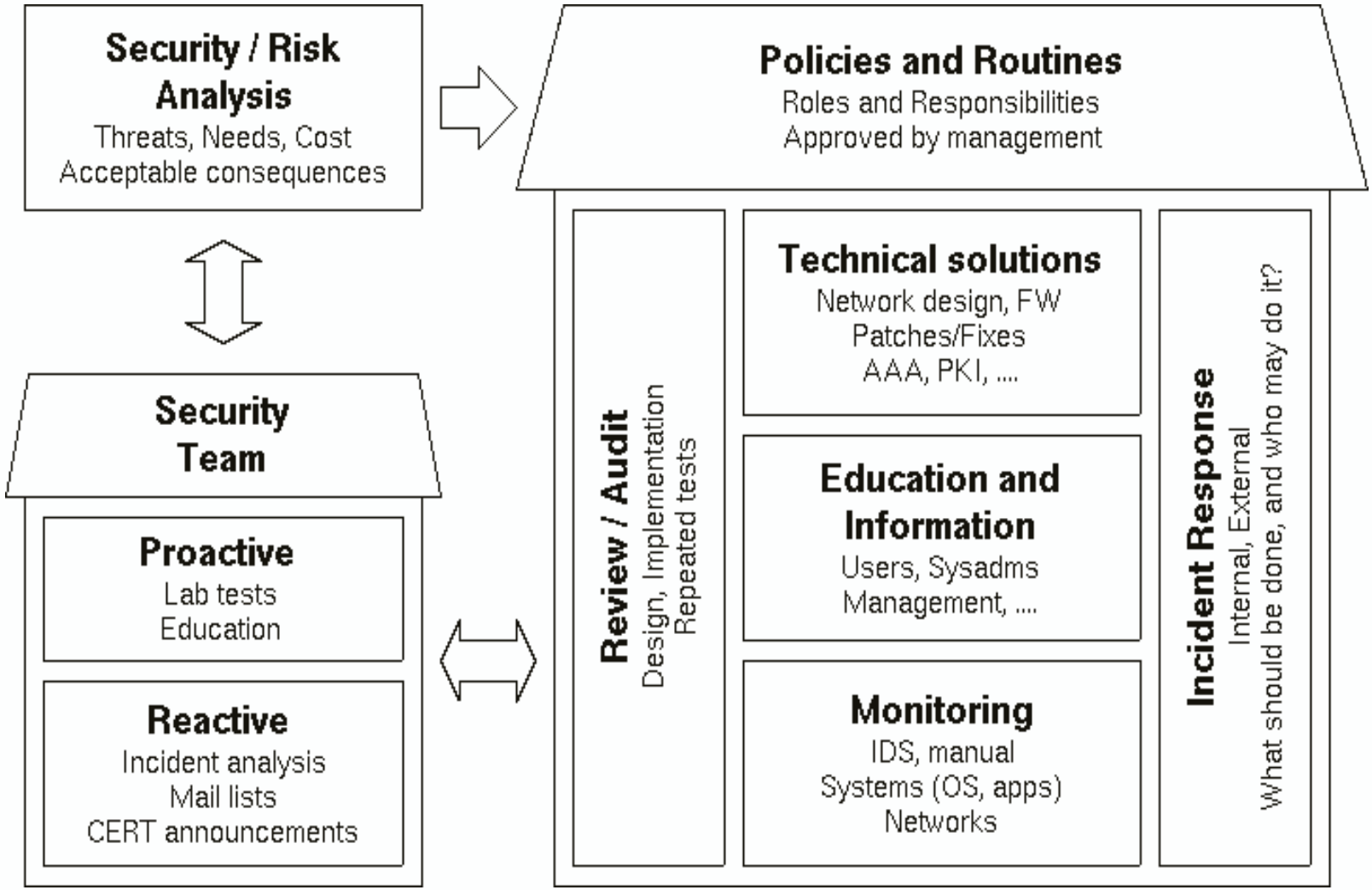
Fördubbling av säkerhetshot i år

(2001-10-16 08:13) Enligt statistik från Computer Emergency Response Team är vi på god väg mot en fördubbling av antalet attacker mot datorsystem jämfört med förra året.

Mats Lövgren, Computer Sweden

- **Vad kommer att styra?**
  - Behov av tjänster? Kvalitetskrav? Allmän teknik-fetischism?

Säkerhetsarbete



Nätverksnivå och teknik
Exempel: IPsec

IP Security Protocol

IPsec is designed to provide interoperable, high quality, cryptographically-based security for IPv4 and IPv6. The set of security services offered includes access control, connectionless integrity, data origin authentication, protection against replays (a form of partial sequence integrity), confidentiality (encryption), and limited traffic flow confidentiality. These services are provided at the IP layer, offering protection for IP and/or upper layer protocols.

These objectives are met through the use of two traffic security protocols, the Authentication Header (AH) and the Encapsulating Security Payload (ESP), and through the use of cryptographic key management procedures and protocols.

Security Architecture for the Internet Protocol

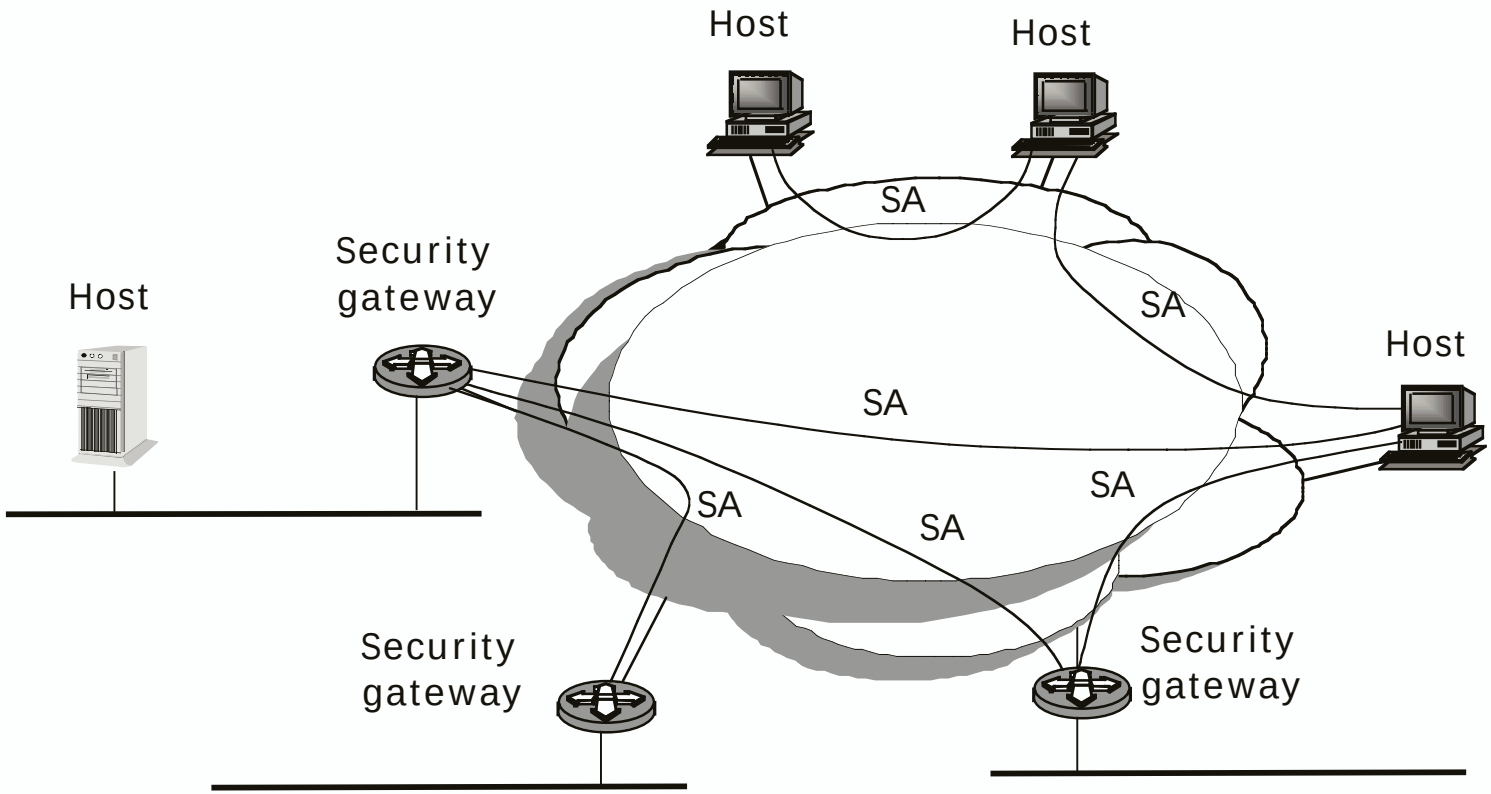
ftp://ftp.isi.edu/in-notes/rfc2401.txt

IPsec: AH och ESP

- **Authentication Header (AH):**
  - Authentication of sender (*data origin authentication*)
  - Data integrity
  - Protection agains replaying traffic (*anti-replay protection*)
  - HMAC-MD5, HMAC-SHA1

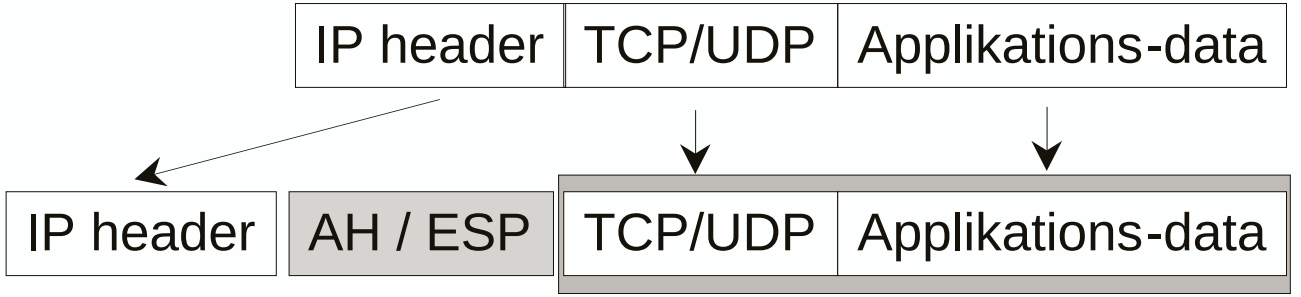
- **Encapsulating Security Payload (ESP):**
  - Confidentiality (data is encrypted)
  - plus: parts of AH
  - DES, 3DES, Blowfish, ...

IPsec SAs

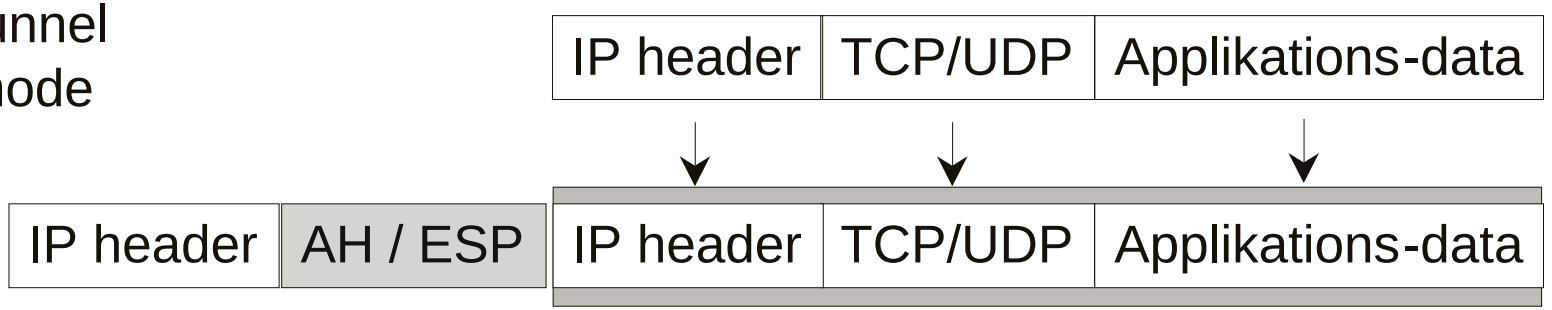

Host
Host
Host
Security
gateway
SA
SA
SA
SA
SA
SA
SA
Security
gateway
Security
gateway

Transport and Tunnel mode

Transport mode



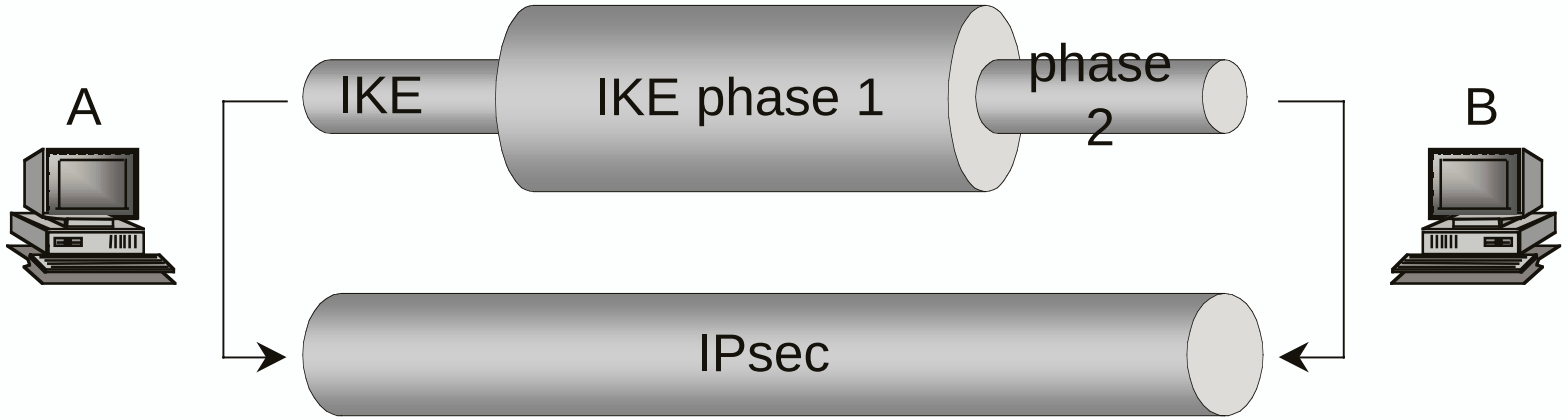
Tunnel mode



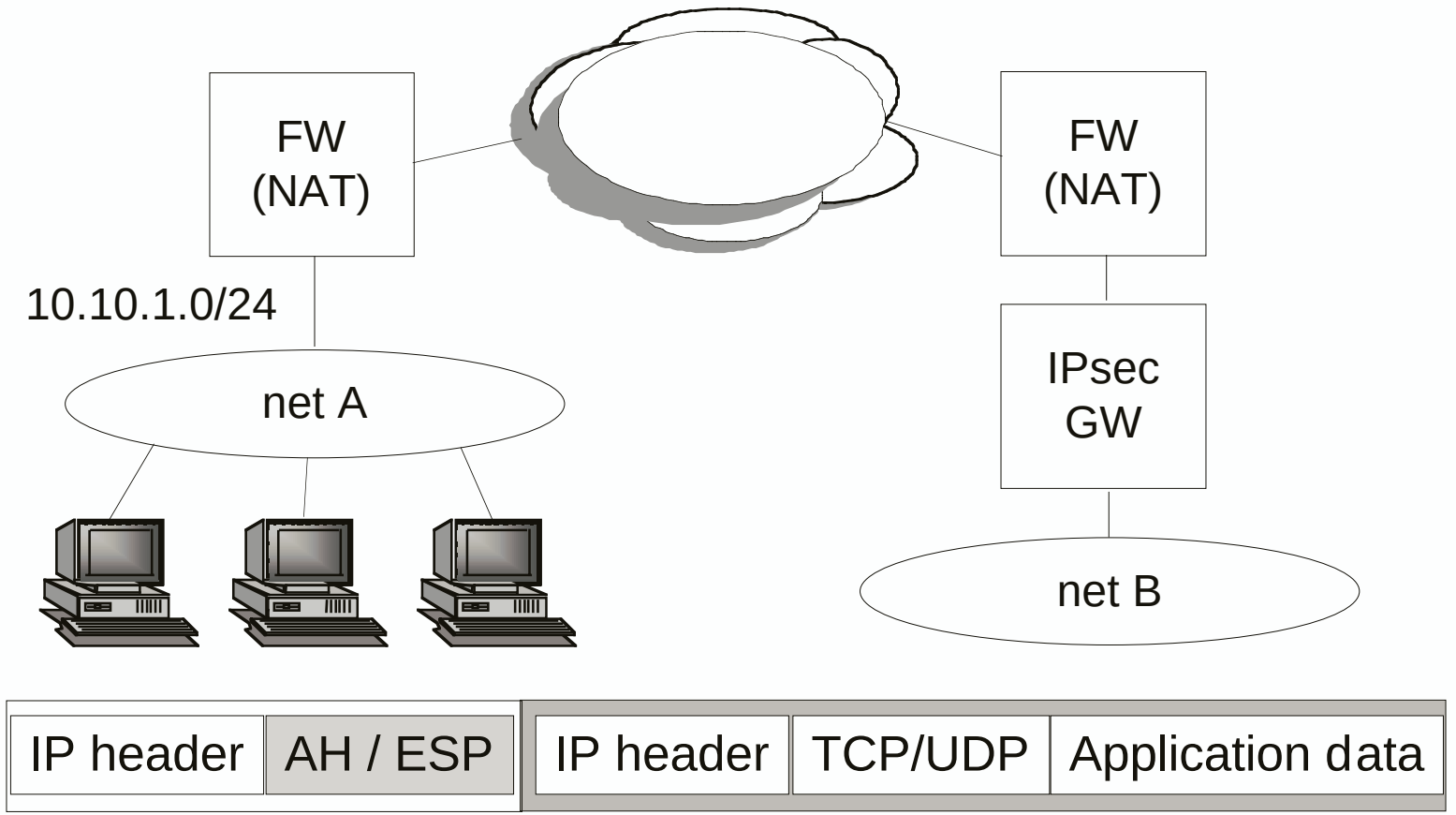
Internet Key Exchange -- IKE

- **IKE has two phases:**
  - Phase 1 (main mode) ⇒ ISAKMP SA
  - Phase 2 (quick mode) ⇒ Application (IPsec) SA
- **UDP / 500**

- **Why key exchange?**
  - Initiate sessions
    - Protected / controlled session setup
  - Keys age...
    - Exchange triggered by amount of data
    - Exchange triggered by time
  - Using a central key server
    - New participants in the network

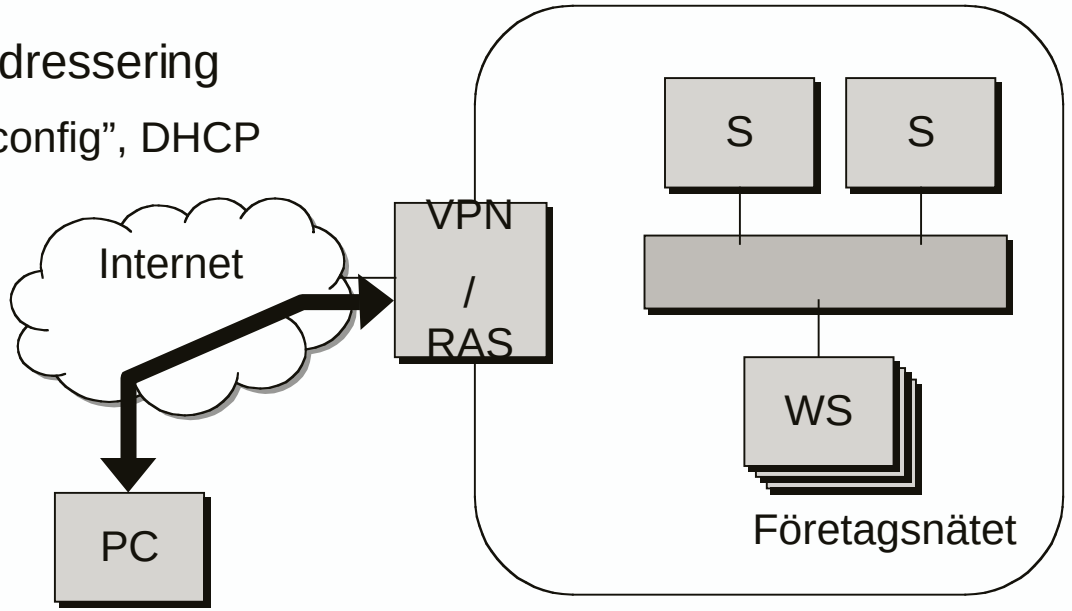


Exempel: NAT and friends



Hur används IPsec?

- **Microsoft Windows 2000**
  - IPsec i transport-mode mellan klient och IPsec GW.
  - L2TP för att skapa en tunnel.
- **Alla andra...**
  - IPsec i tunnel-mode mellan klient och GW.
  - Olika principer för addressering
    - Hårdkodat, “mode config”, DHCP

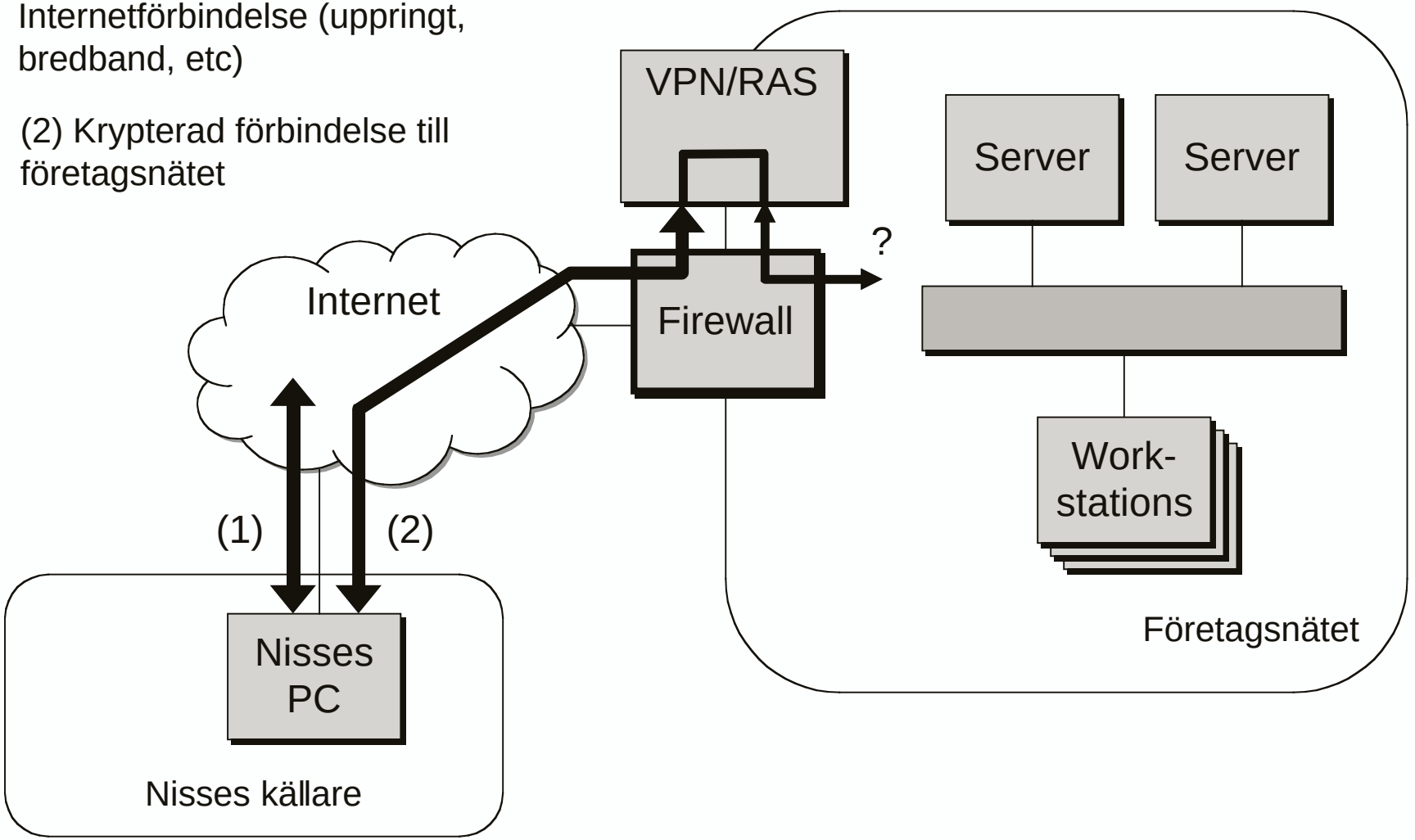


Arkitektur: Nätbyggnad, olika krav och alternativa lösningar

En vanlig lösning: VPN över publikt nät

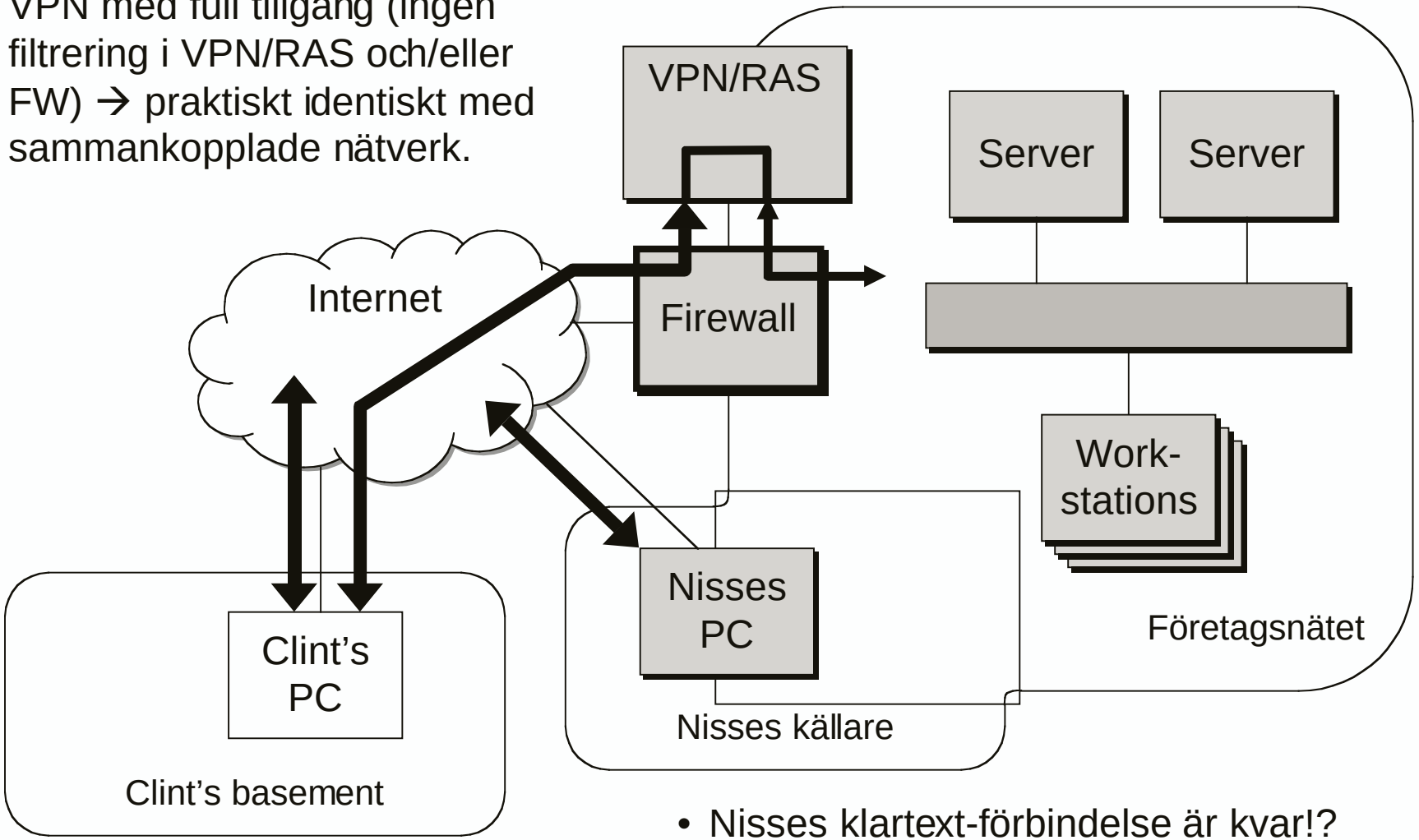
(1) Vanlig klartext Internetförbindelse (uppringt, bredband, etc)

(2) Krypterad förbindelse till företagsnätet



Det utdragna gummibandet

- VPN med full tillgång (ingen filtrering i VPN/RAS och/eller FW) → praktiskt identiskt med sammankopplade nätverk.

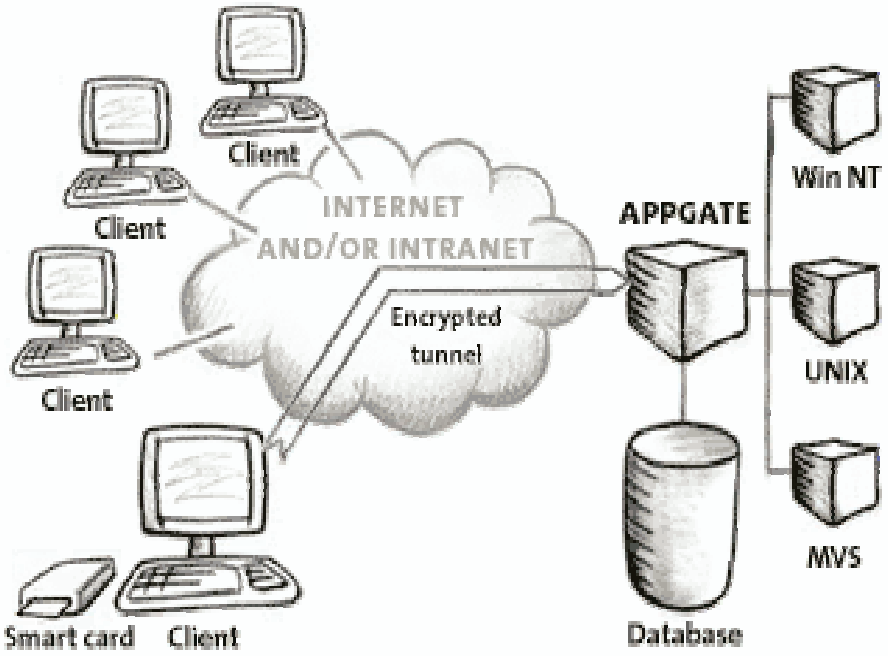


- Nisses klartext-förbindelse är kvar!?

Hot mot distansarbetsplatsen

- **Virus**
  - Sprids på många olika sätt. Nimda: e-mail (Outlook), IIS, ...
  - NetBus / BO / etc.
- **“Alltid på”**
  - Trivialt att genomsöka stora nät
- **Generella operativsystem med komplexa applikationer**
  - Time to market
  - Dålig design, komplexa beroenden
- **Integritet?**
  - Skall användaren få använda distansarbetsplatsen privat?

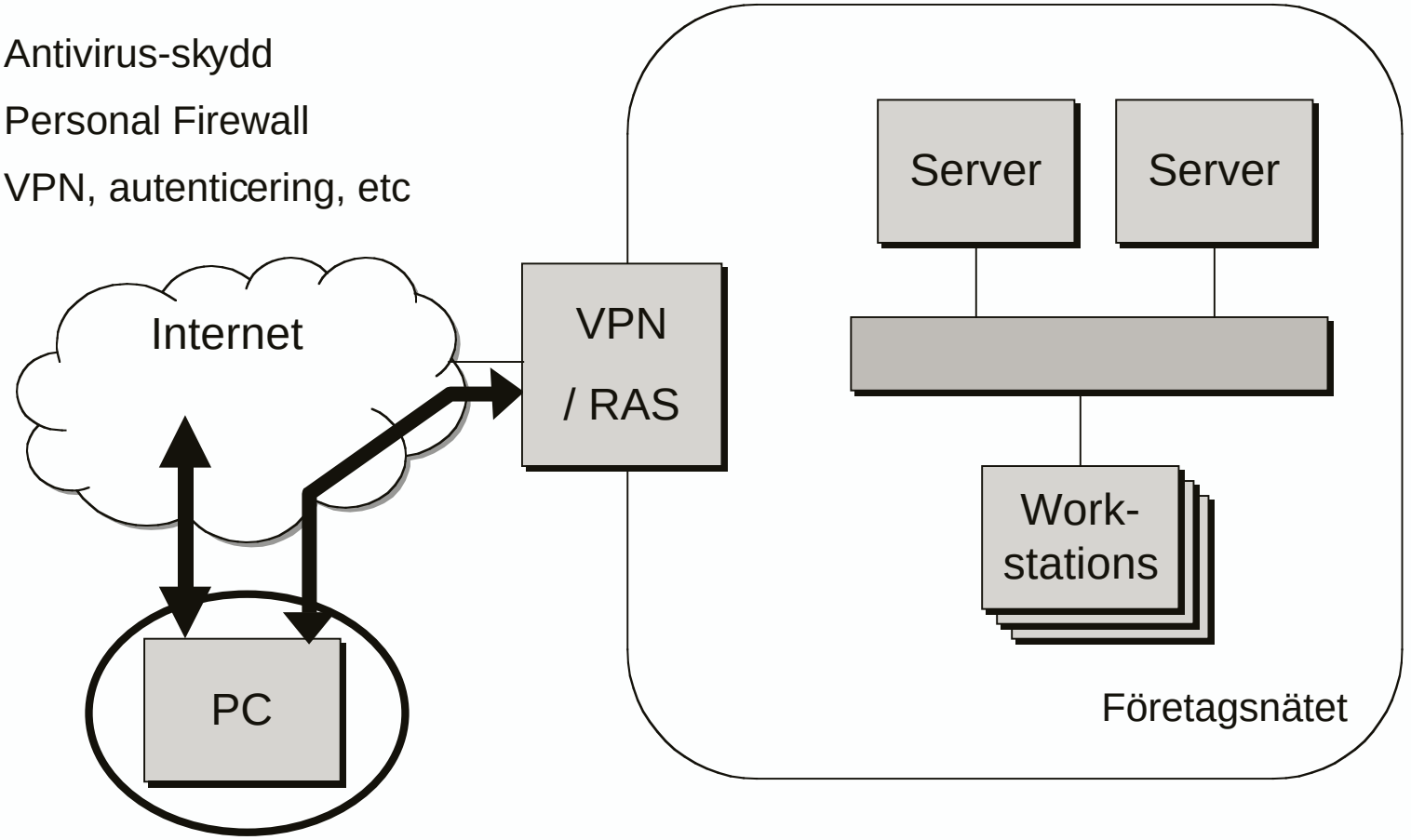
Exempel: AppGate



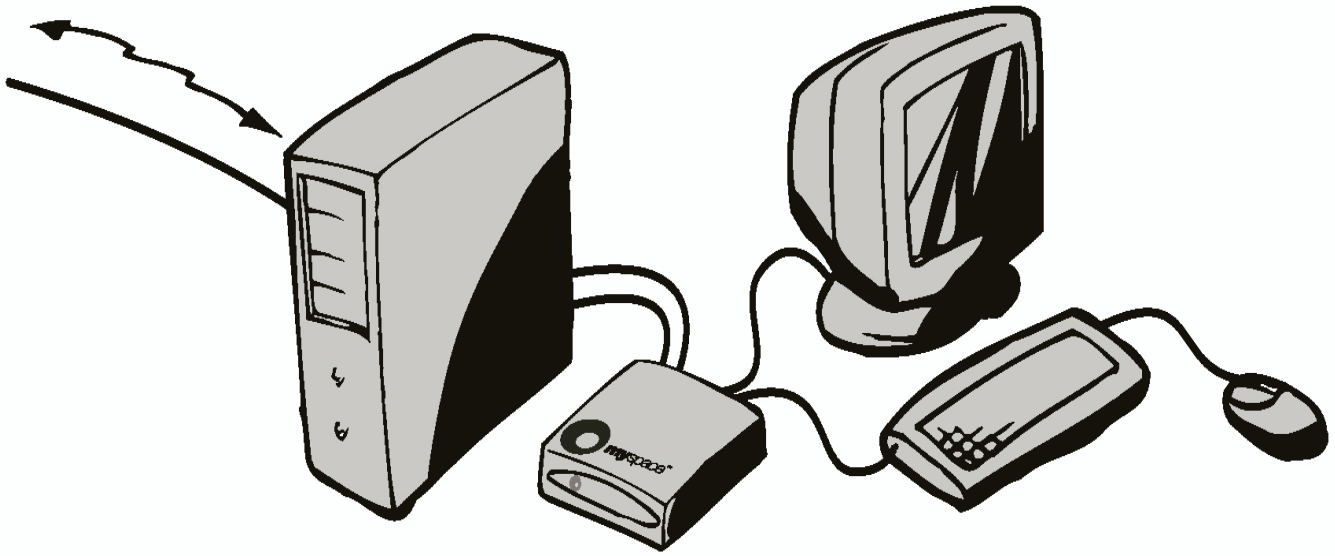
- **Åtkomst till styrs på applikationsnivå. Beroende på ett antal "selektorer" (var, vem, när, etc), som översätts till "roller", ges tillgång till olika tjänster.**

Exempel: “Sec@Home” (Guide)

- **“Paraply”-program kontrollerar:**
  - Antivirus-skydd
  - Personal Firewall
  - VPN, autenticering, etc

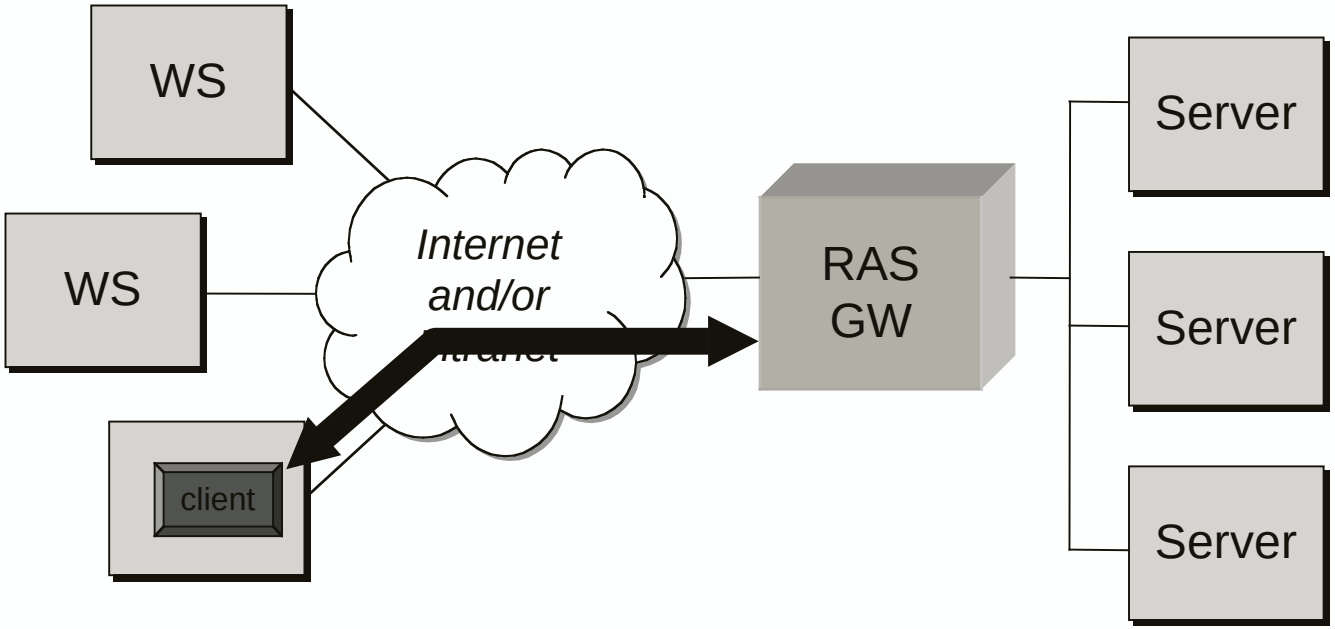


Exempel: MySpace



- **Känsliga applikationer exekveras i “MySpace-lådan”, i en kontrollerad och säker omgivning.**
- **“MySpace-lådan” har inga kopplingar till PCn, och är därför inte beroende av dess skydd.**

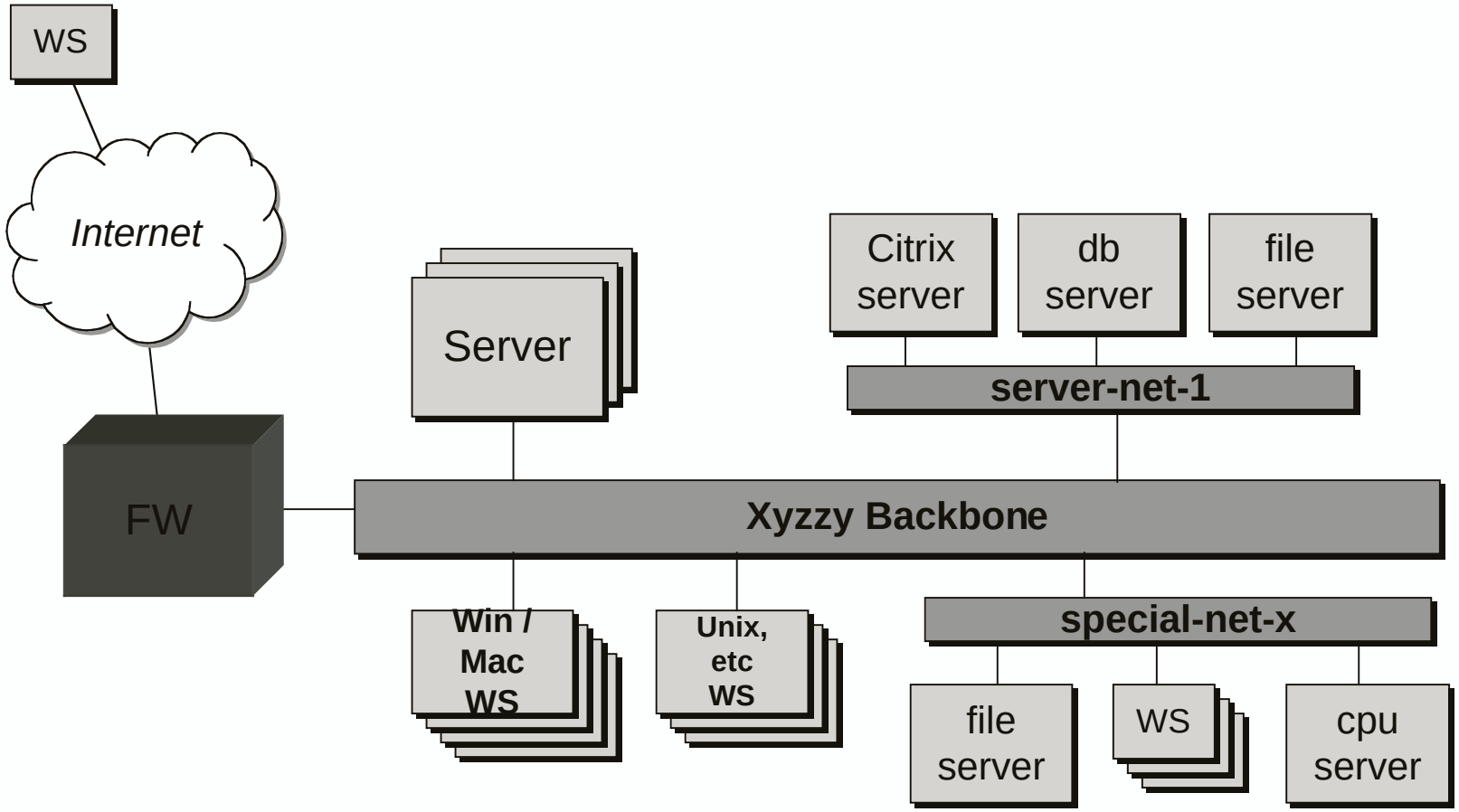
Alternativ: Feta servrar och tunna klienter



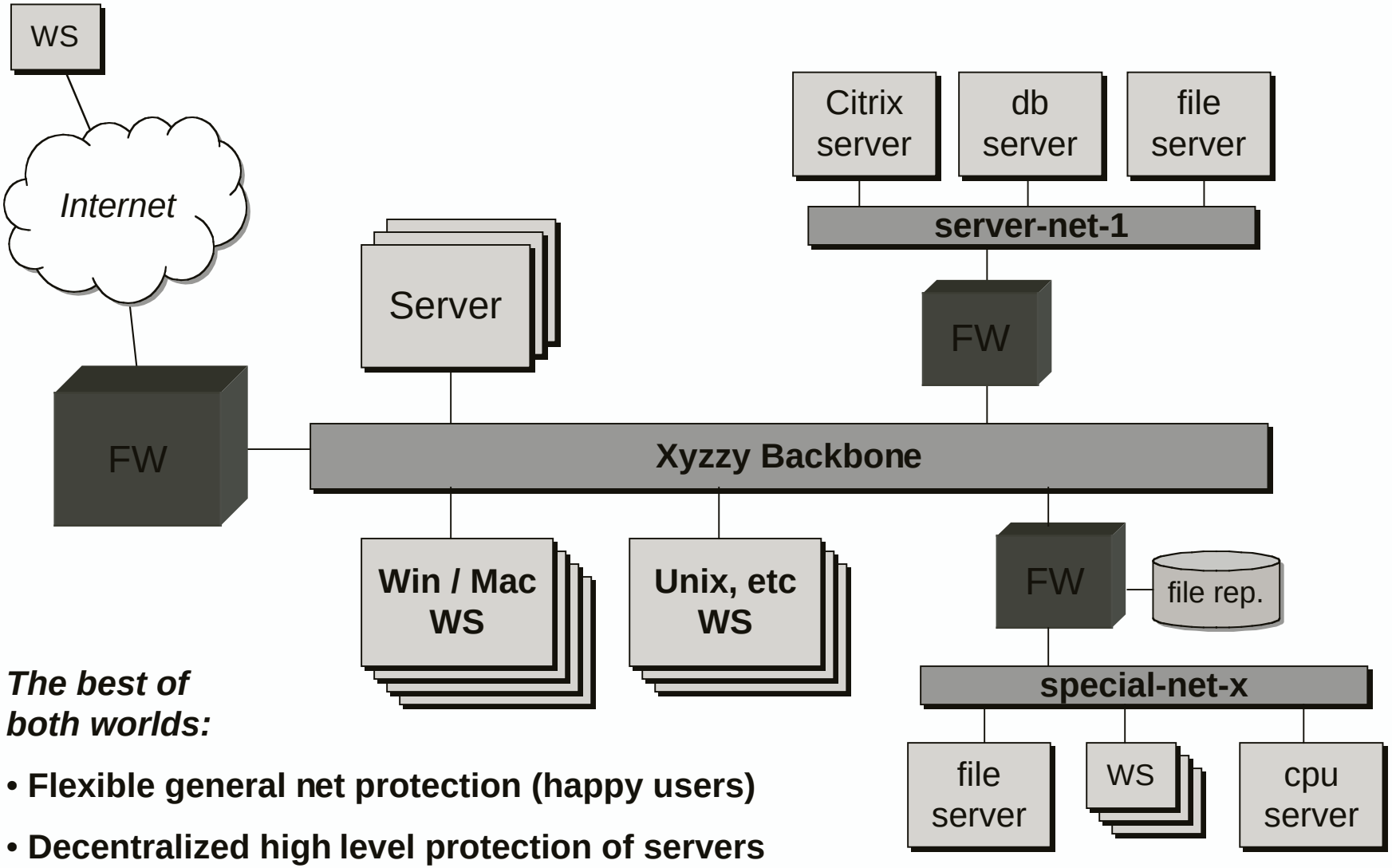
- **En “tunn klient” används som display-terminal. Applikationer exekveras på servrarna (t.ex. NT TerminalServer / Citrix).**
- **Säkerhetsproblem vi inte kommer undan:**
  - Virus, NetBus/BO.
  - Tunna klienter (hw) kan ha problem med nya säkerhetssystem.

Framtiden:
Flexibel nätverks- och säkerhetsdesign
(vad betyder “insidan” respektive “utsidan”)

The old Xyzzy company network



The new Xyzzy company network



The best of both worlds:

- **Flexible general net protection (happy users)**
- **Decentralized high level protection of servers**

Slutsatser

- **Policy bestämmer, måste förankras hos både användare och management! Utbildning.**
- **Teknik: Säkerhet på djupet, olika mekanismer på olika nivåer. VPN eller RAS eller distansarbete, har inte EN teknisk lösning, utan måste vara en kombination av lösningar.**
- **Målet är att bygga en jämn/balanserad säkerhetsnivå, där användaren känner att han/hon har kontroll av vad som sker! Säkerhet börjar och slutar med användaren.**