Onderzoek naar de veiligheid c.q. beveiliging van de SURFnet IDS dienst.

Lourens Bordewijk & Jimmy Macé

Amsterdam 8-2-2006

Achtergrond IDS dienst

- SURFnet netwerk
- Aangesloten instellingen te maken met security incidenten
- Om inzicht te geven in de incidenten, heeft SURFnet het D-IDS ontwikkeld

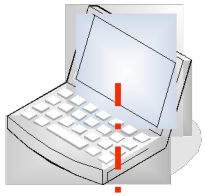
Doel

- Onderzoeken van beveiligingsrisico's
- Onderzoeksresultaten kunnen maatregelen opleveren
- Voortaan veiliger aanbieden van D-IDS

Projectuitvoering

- Identificeren en analyseren van het huidige ontwerp
- Nagedacht hypothetische zwakheden
- 7 mogelijke aanvalscenario’s
- Testen
- Optimaliseren ontwerp en implementatie
- Technische en niet-technische maatregelen

Huidige Situatie - SURFnet D-IDS



- Attacker/Worm/Virus/Hacker
- Attacks IP on server

- Layer 2 tunnel (tap device)
- Nepenthes simulates weakness
- Nepenthes handles attack

- Nepenthes logs attack

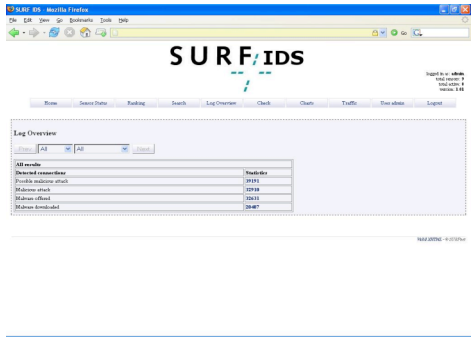
Honeypot/Tunnel Server
- Nepenthes
- OpenVPN

Logging Server
- Postgresql
- Web interface

- Sensor is booted
- OpenVPN is started

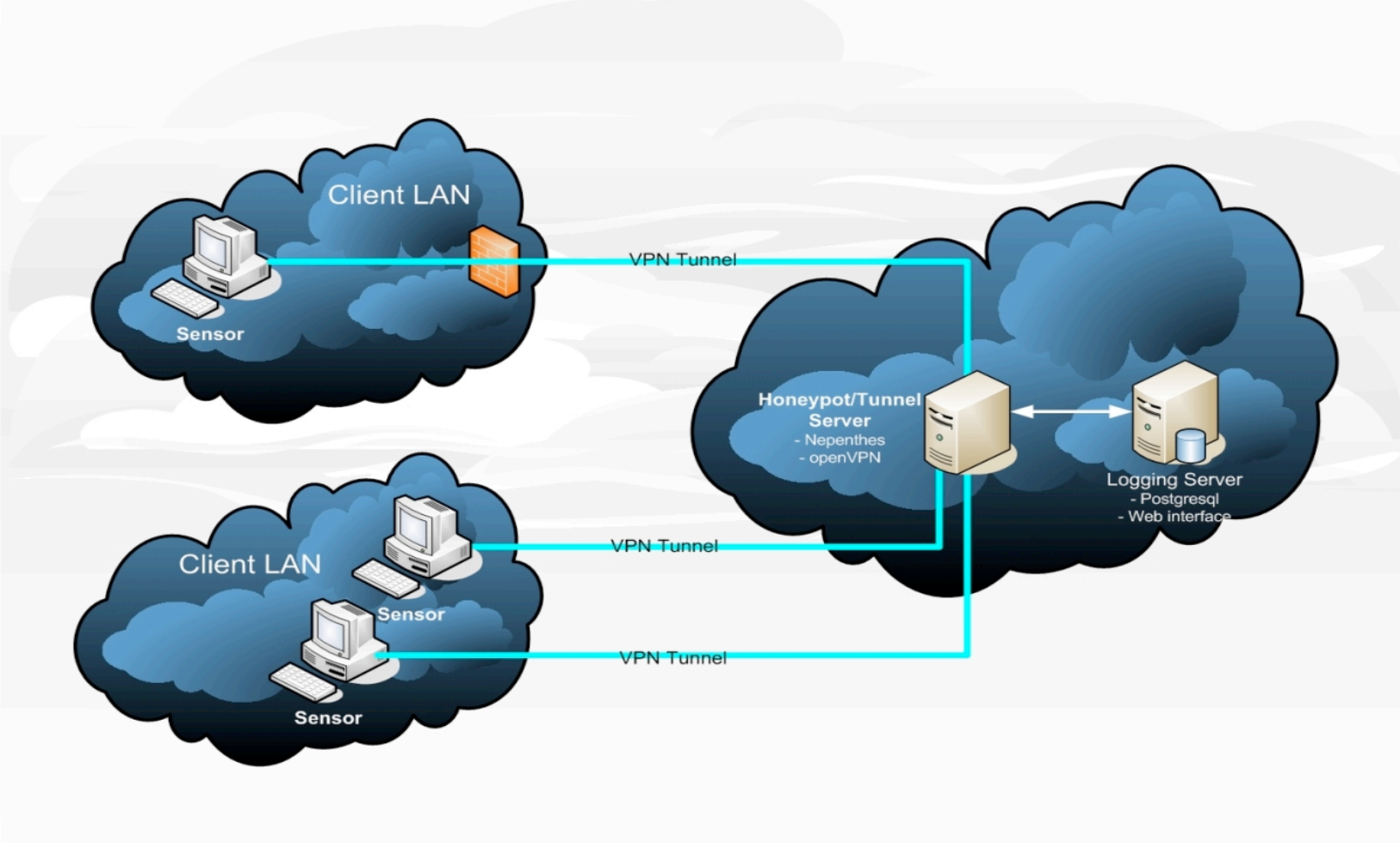
- Uses tcp port 1194
- Works with NAT !!

- Web interface makes data representable



Sensor

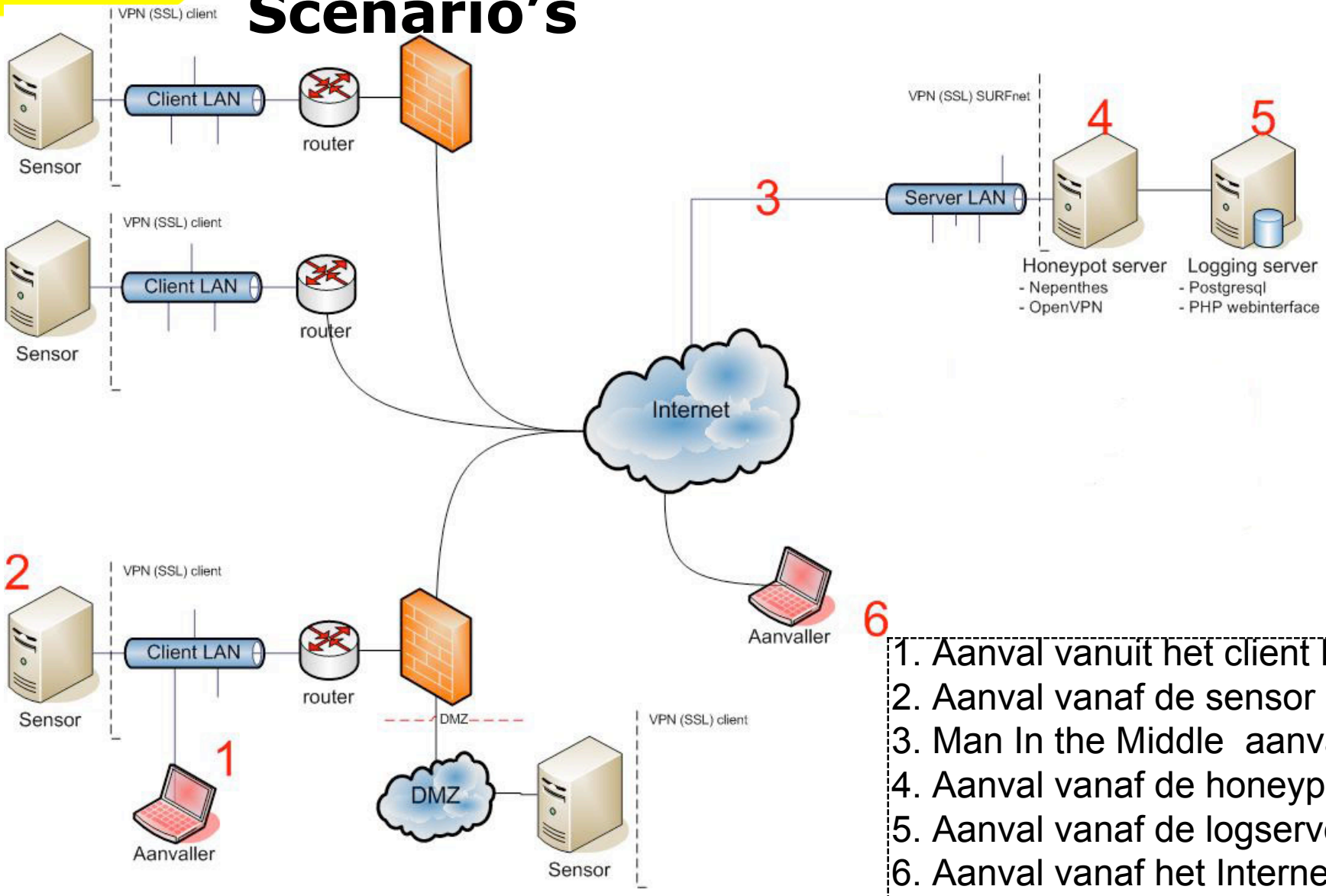
Distributed Intrusion Detection System



Onderzoek

- Black/White box penetratietest
- Getest op:
  - Beschikbaarheid
  - Integriteit
  - en vertrouwelijkheid
- De kwetsbaarheden zijn geïdentificeerd door middel van:
  - Fingerprinting;
  - Geautomatiseerde en handmatige kwetsbaarheid scan;
  - Een kwetsbaarheid analyse;
  - Systeem software en security analyses.

Scenario's

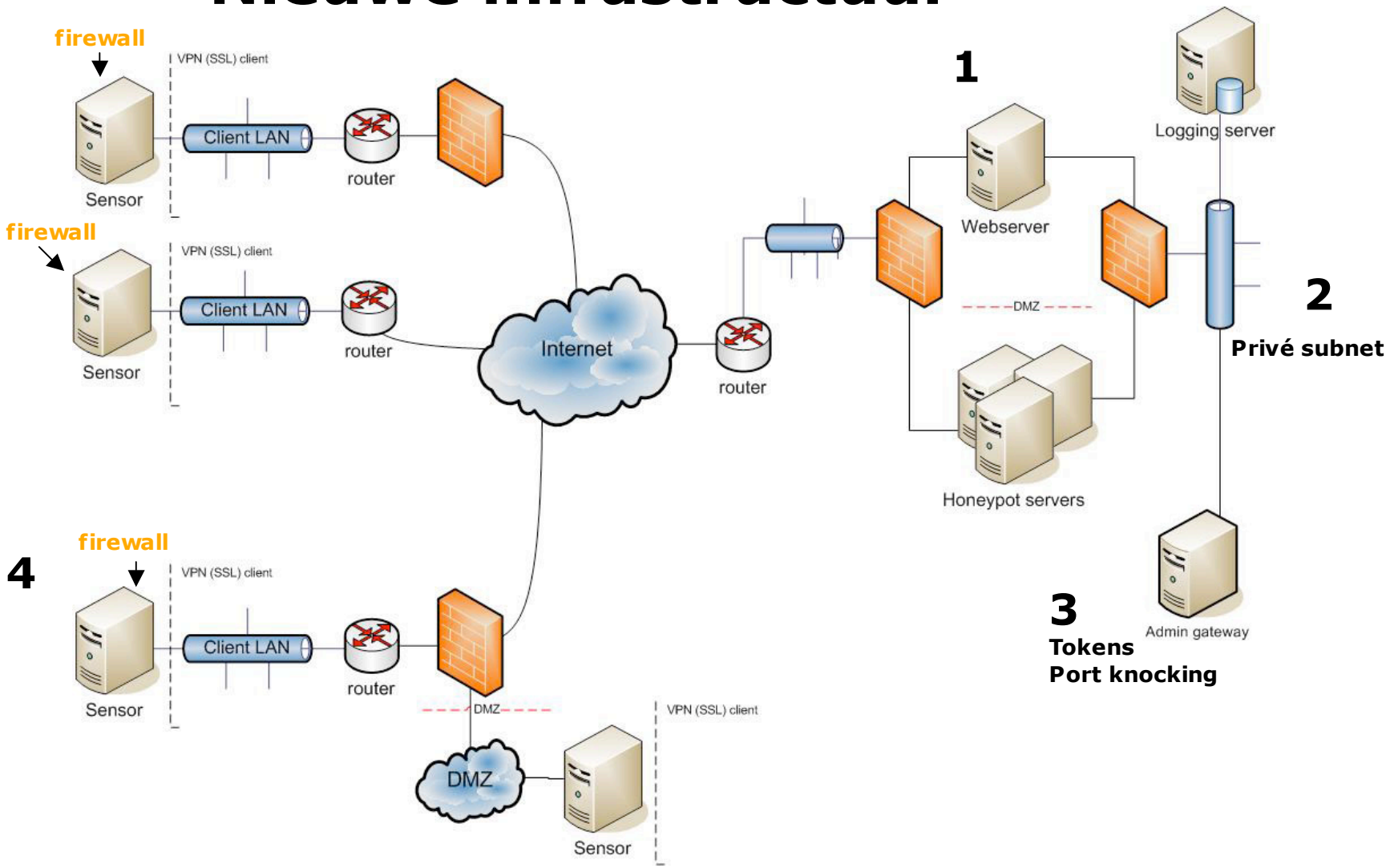


1. Aanval vanuit het client LAN
2. Aanval vanaf de sensor
3. Man In the Middle aanval
4. Aanval vanaf de honeypot
5. Aanval vanaf de logserver
6. Aanval vanaf het Internet
7. Fysieke beveiliging

Bevindingen

- Software niet up to date
  - PHP, MC, OpenSSH, imagick lib
- Overbodige software pakketten geïnstalleerd
- Configuratie fouten software

Nieuwe infrastructuur



De maatregelen

- Defense-in-depth
- Implementatie

Algemene maatregelen

- Basis, veilig besturingssystemen
- Besturingssystemen hardenen
- Besturingssystemen strippen
- Updaten van services
- Beveiliging van de services optimaliseren
  - Apache, OpenVPN, PostgeSQL...
- Integriteits tools, zoals Tripwire of Aide
- Middels TCP-wrappers
- Er moet regelmatig geaudit worden, Nessus en Tiger
- Audit trails analyseren

- Ook beheerders pc's!

Fysieke maatregelen

- Bootloaders en BIOS
- HD eerste bootdevice
- Behuizingen beveiligen

- HD/USB-stick encryptie, Safeboot?

Niet-technische maatregelen

- Mailinglijsten, nieuwsgroepen, websites monitoren
- Policy D-IDS opstellen:
  - Wachtwoorden & accounts
  - Beheerders procedures maken sensoren
  - Beveiliging, regelmatig auditten & trails analyseren..

- Na leven policy!

Conclusie/advies

- SURFnet D-IDS biedt een schaalbare, eenvoudig te beheren en onderhouden IDS dienst
  - Lastig om alle punten exact te verifiëren
- IDS dienst kent enkele beveiligingsrisico's:
  - Update en configuratie fouten.
- Maatregelen consequent doorvoeren
- Afweging tussen kosten, gebruiksgemak en risico’s
- Best-effort oplossing.

Toekomst

- Audit Nepenthes (zekerheid beveiliging)
- Firewall (IP-tables) sensoren
- Veilig OS
- Maatregelen reflecteren in een security checklist voor de beheerders
- Policies opstellen

Vragen

?