SURFnet

SURFnet IDS
a Distributed Intrusion Detection System

Rogier Spoor (project leader)

Jan van Lith (developer)

Kees Trippelvitz (developer)

Amsterdam 24-1-2006

Goals

- Understanding:
  - types of malicious network traffic within a LAN
  - amount of malicious network traffic within a LAN
  - spreading of worms
- Setting up:
  - a scalable IDS solution
  - an IDS that is easy to manage and maintain
- Comparing results with other sensors
- Limit malicious outbound traffic SURFnet

Why build something new?

- Sensor must be maintenance free
- IDS must be scalable and easy to manage
- No False Positives! (cannot use *snort*)
- Design IDS based on high speed networks (LAN/WAN)
- Design IDS “should” be able to analyse L2 traffic

Sensor

- remastered Knoppix distribution
- USB boot
- Open-vpn between Sensor and Central Server

Need:

- PC capable of USB boot + 1 NIC
- DHCP LAN (2x DHCP)
- Open-vpn session through local firewall (TCP 1194)

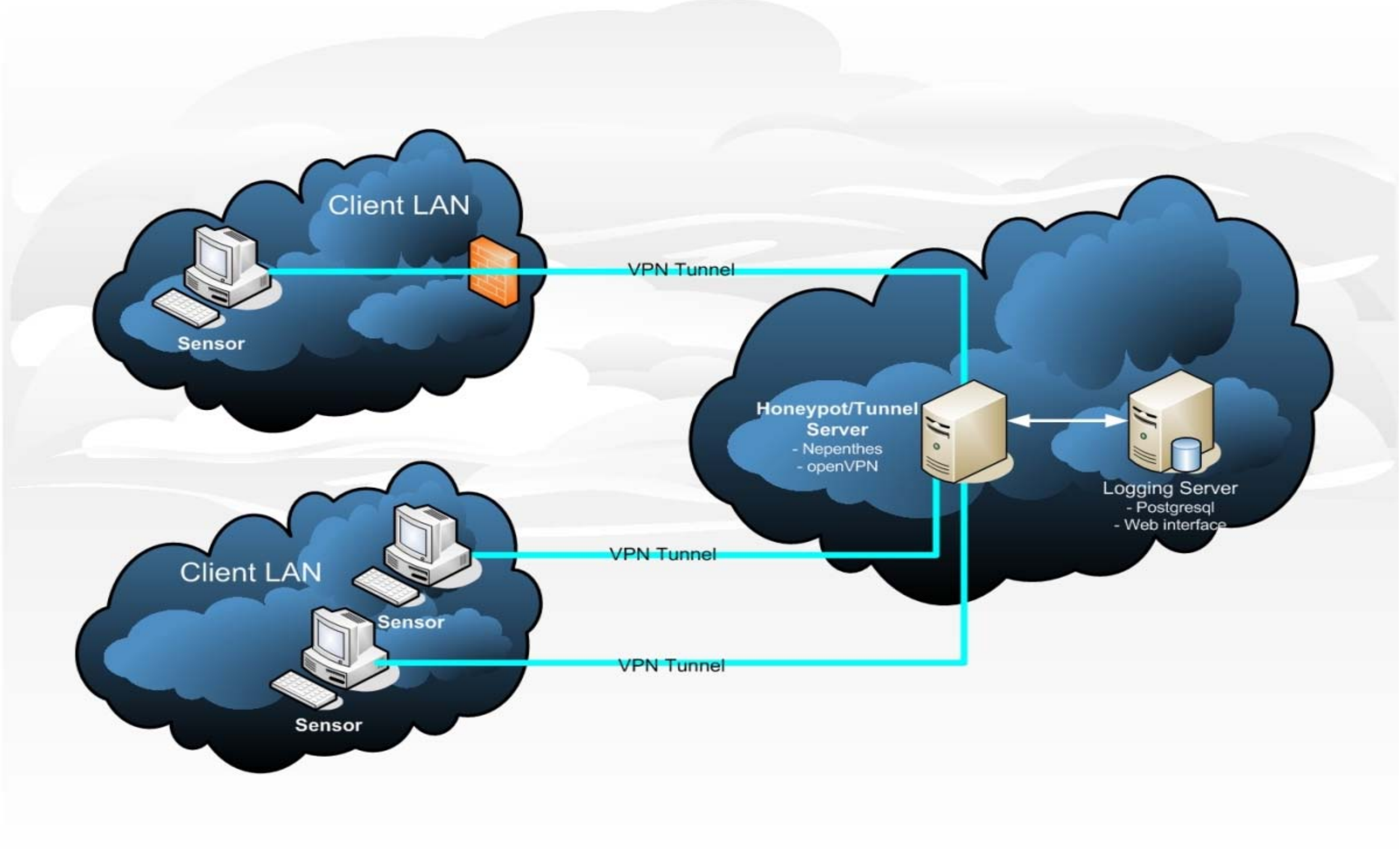
Honeypot / Tunnel server

- Based on *nepenthes*
  - a low-interaction honeypot
  - Link: http://nepenthes.sourceforge.net
- Open-vpn tunnel to sensor
- Manage X509 certificates/keys of sensors
- Source-based routing

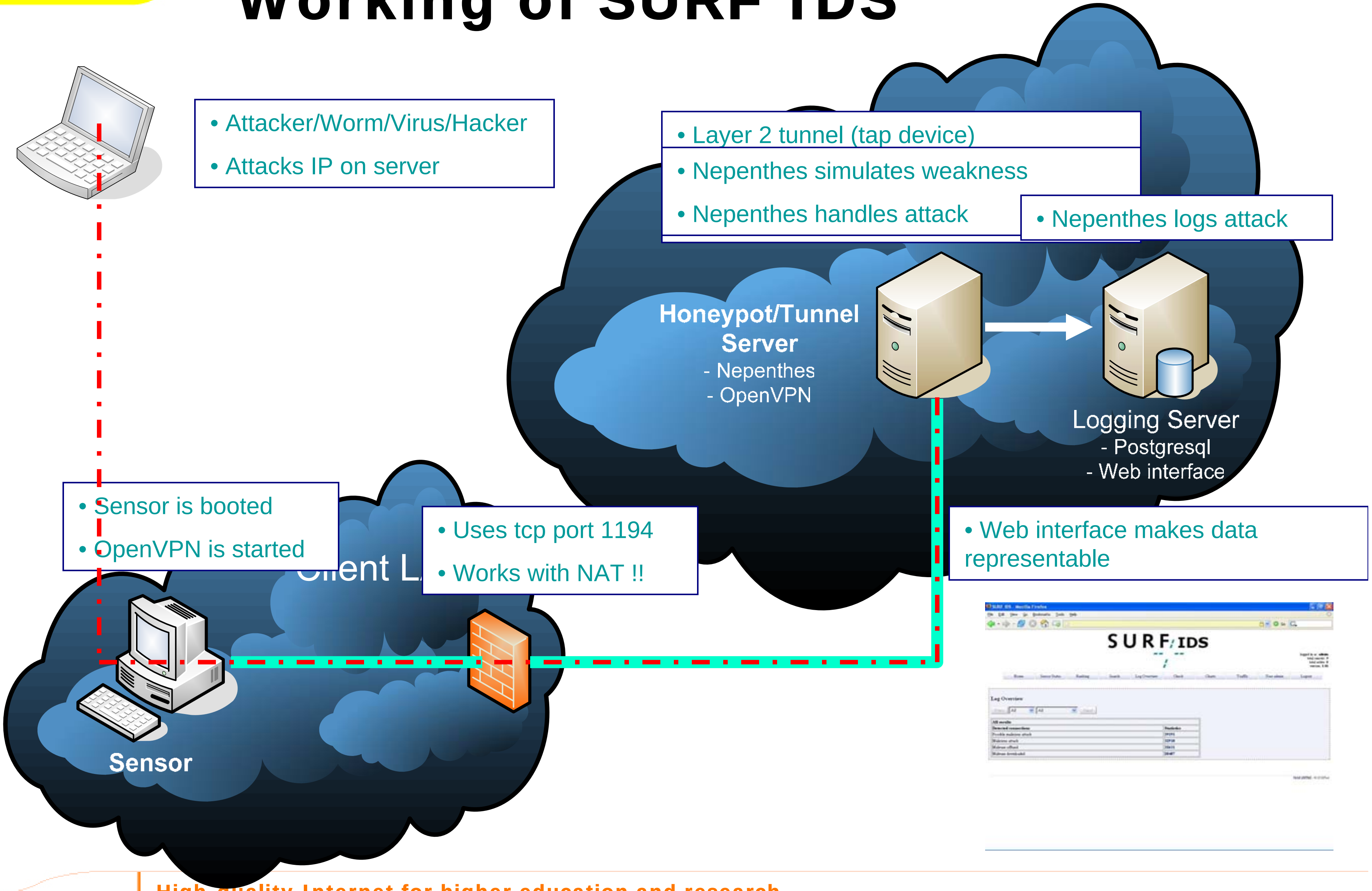
Logging server

- *Postgresql*
- Web interface
- Show statistics of sensors (groups/individual)
- Show statistics of different attacks
- Ranking of sensors
- Mail logging
- IDMEF

Global Overview



Working of SURF IDS



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

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

- Nepenthes logs attack

- Sensor is booted
- OpenVPN is started

- Uses tcp port 1194
- Works with NAT !!

- Web interface makes data representable

Future

- Start an IDS service for SURFnet customers
- Open source licensing (GPL) and packaging
- Additional honeypots on the central server
- Logging interface for tools like AIRT
- Interface for a quarantaine environment
- Static assignment of IP addresses on server and sensor
- Multiple VLAN support for sensor

Demo

Questions?

Website http://ids.surfnet.nl