SURFnet IDS / OS3 UvA Project

SURFnet IDS

UvA Universiteit van Amsterdam

Extension of the SURFnet Intrusion Detection System Sensors to Microsoft Windows XP

Michael Rave
Coen Steenbeek

7 February 2007

Overview

- Intrusion Detection Systems
- SURFnet IDS
- Problem Definition
- Research
- Solutions
- Conclusion
- Future Work
- Questions

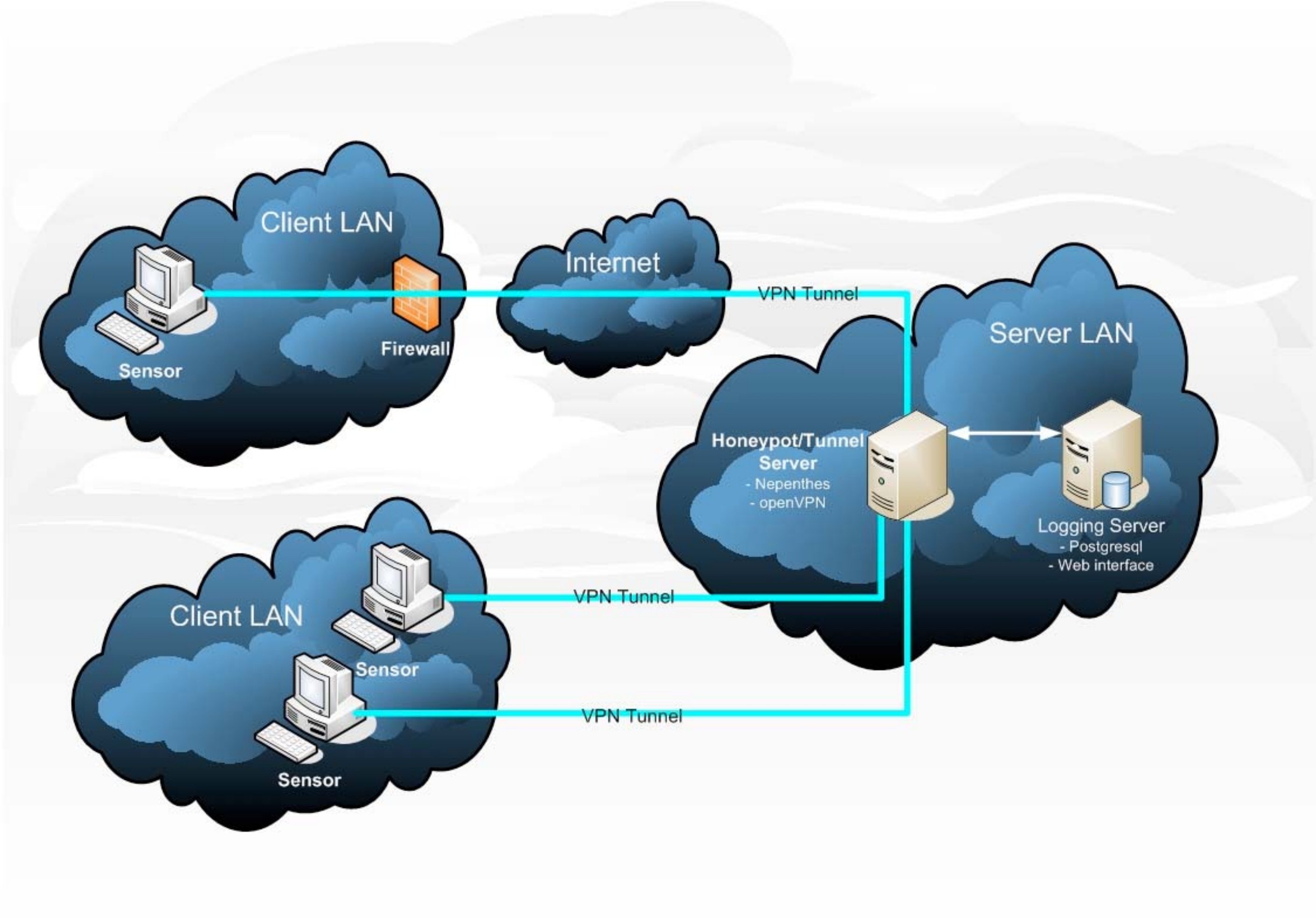
Intrusion Detection Systems

- What is IDS?
  - detects unwanted manipulations
  - Hackers, script kiddies, worms, e.c.
  - Detection, no prevention
- Different sorts of IDS's
  - Network IDS
  - Host-based IDS
  - Hybrid IDS

SURFnet IDS

- Distributed IDS
  - Client - Server model
- Distributed sensors
  - Modified Knoppix distribution
  - Layer-2 VPN tunnel in bridging mode
- Honeypot
  - Nepenthes
- Logging Server
  - PostgreSQL Database
  - Apache webserver

SURFnet IDS


Client LAN
Internet
Sensor
Firewall
VPN Tunnel
Server LAN
Honeypot/Tunnel Server
- Nepenthes
- openVPN
Logging Server
- Postgresql
- Web interface
Client LAN
VPN Tunnel
Sensor
VPN Tunnel
Sensor

Problem Definition

“How to give a desktop computer the same functionality of the current SURFnet IDS sensors without affecting the current functionality of the desktop computer?”

Sub-questions

- *How to obtain unused ports on Windows XP*
- *How to forward certain ports on Windows XP*
- *How to forward incoming traffic on certain ports to the honeypot without changing the source IP-address of the incoming packets*

Research

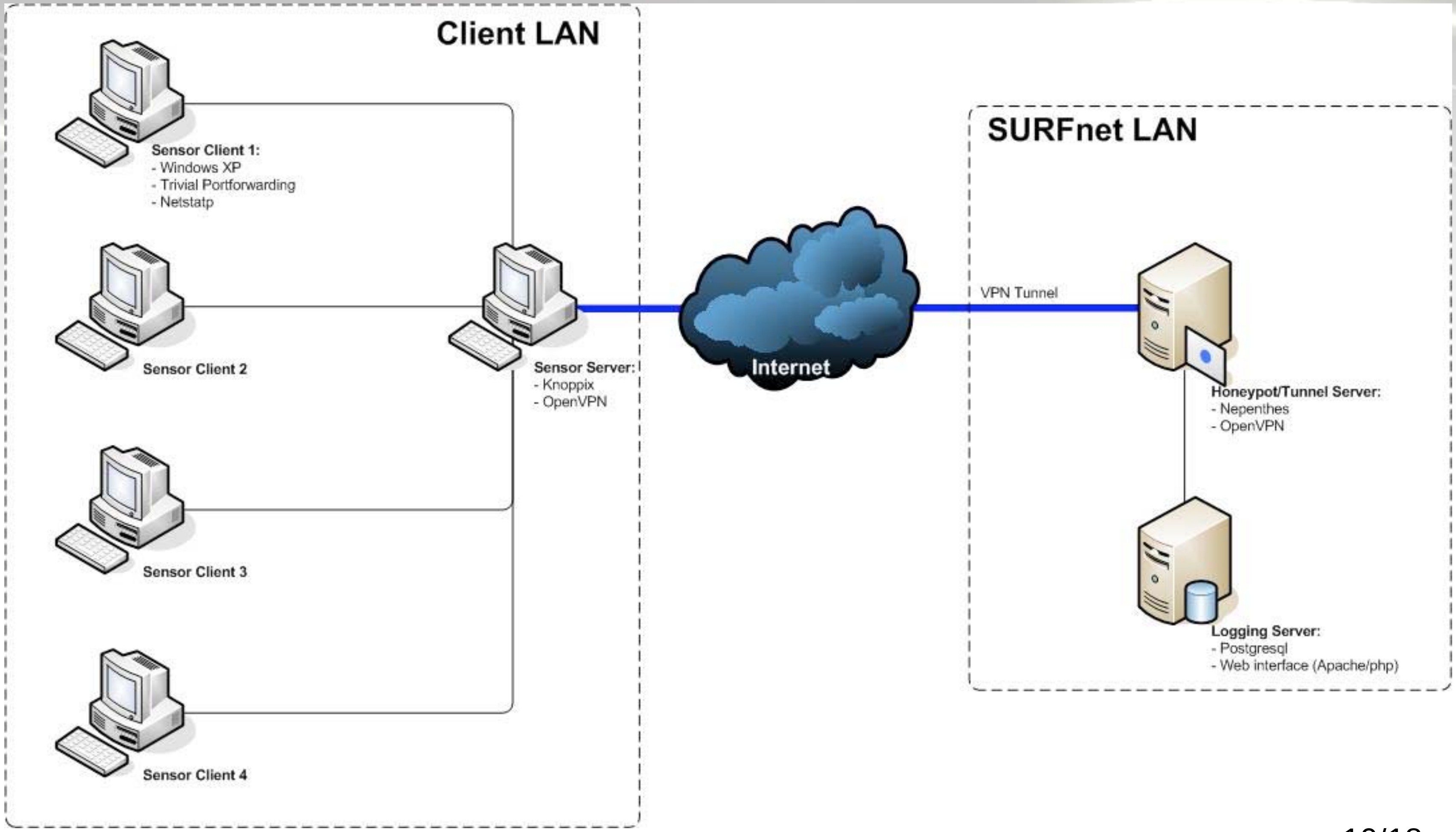
- Unused Ports
  - Netstatp
  - Nmap
  - Winpcap
  - …
- Port forwarding
  - Trivial Port Forward
  - Netsh
  - Wintunnel
  - …

Solutions

- *“How to forward incoming traffic on certain ports to the honeypot without changing the source IP-address of the incoming packets”*
- Indirect Solution
- Direct Solution

Solution

Indirect



Implementation

Indirect

- Challenges Indirect
  - Source IP-address of attacker
- Solution
  - IP-tunneling/IPSec/IPv6?
  - Not tested

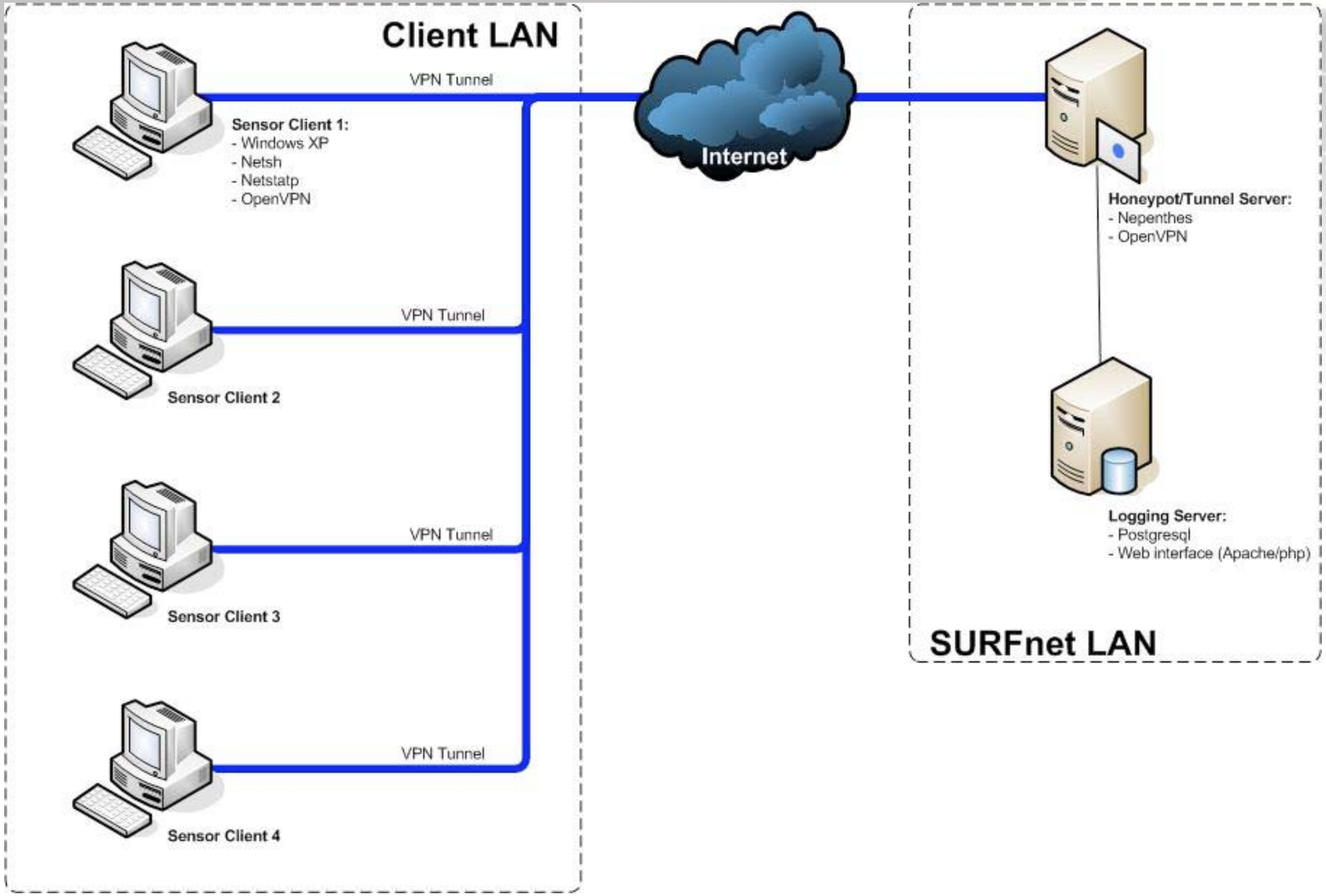
Advantages/Disadvantages

Indirect

- Advantages
  - Sensor Server already present in current setup
  - Only one VPN connection
  - Better structure
- Disadvantages
  - IP-tunneling/IPSec/IPv6 introduces difficulties
  - No working concept so not tested

Solution

Direct



Implementation

Direct

- Challenges Direct
  - Source IP-address of attacker
  - Routing through same tunnel
- Solutions
  - Netsh, pre-routed NAT
  - Source based routing

Advantages/Disadvantages

Direct

- Advantages
  - Secure VPN tunnel
  - No changes to current sensor
  - Already tested succesfully
- Disadvantages
  - Every sensors needs its own VPN tunnel
  - Many rules in source based routing tables

Future Work

- IP-tunneling/IPv6/IPSec for indirect solutions
- Further tests
- Efficient port checking
  - No opening of ports
  - Opening when attacked

Conclusion

- Summary
  - Two Solutions
  - First tested successfully
  - Second needs more research and testing
- We recommend
  - Direct solution
    - Secure VPN tunnel
    - Successfully tested
    - No modifications to old-style sensor
    - Only small modifications to honeypot server
    - Both sensors (old and new) in conjunction

Questions?