Expansion of the SURFnet Intrusion Detection System

R. Buijs
P. Siekerman

System and Network Engineering

Universiteit van Amsterdam
SURFnet

7-2-2007

Contents

Assignment

Suggest improvements to SURFnet IDS.

- Greater diversity

IDS product research

Intrusion Detection Systems

- What is an IDS?
- HIDS
  - Host based
  - Monitors attacks to host
- NIDS
  - Network based
  - Monitors malicious traffic on network, multiple hosts

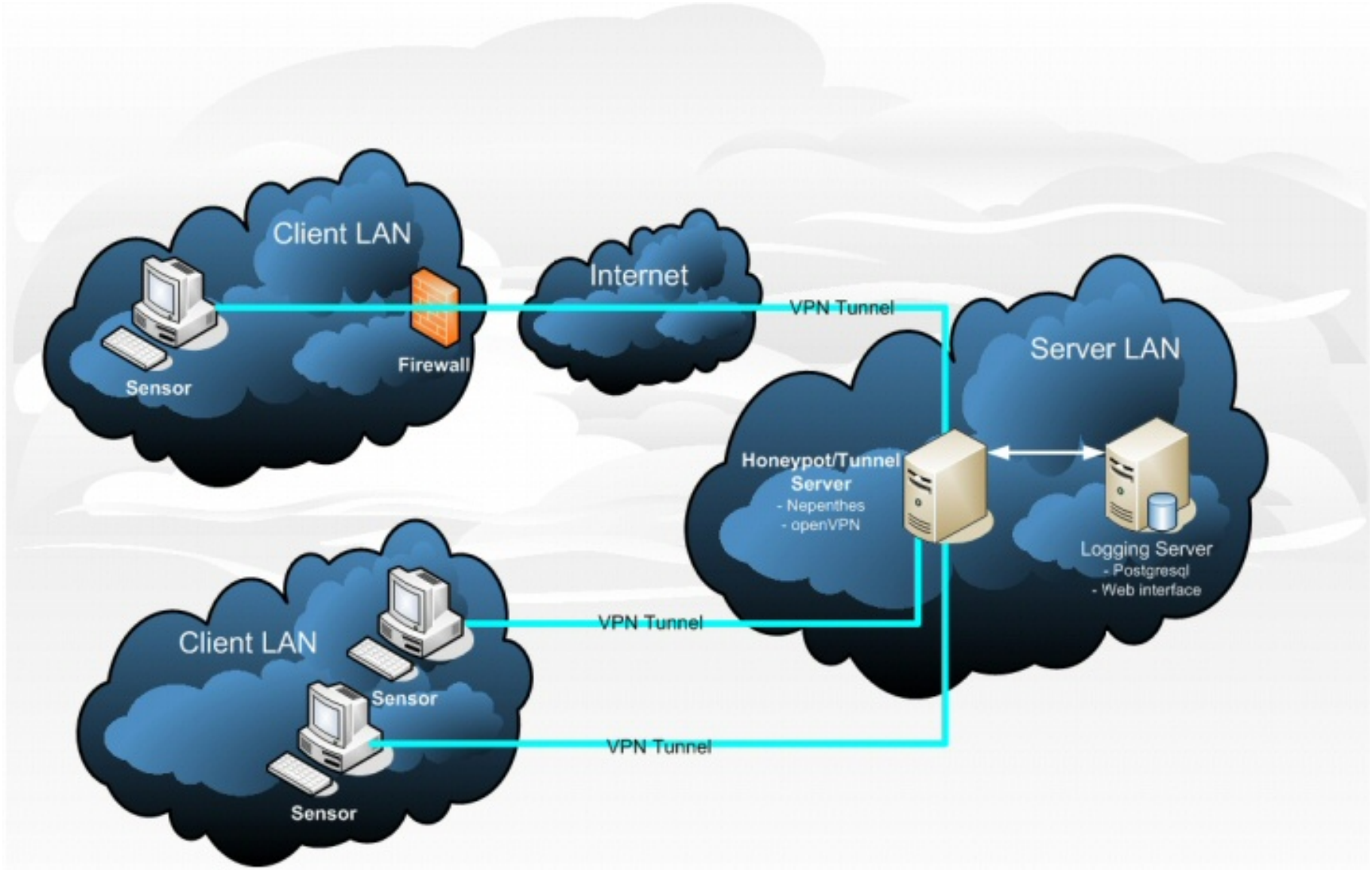
Intrusion Detection Systems

- Low-interaction
  - Service emulator
  - Limited to emulation
  - Easier to detect
- High-interaction
  - Runs real services
  - Real host, or virtual
  - Zero day attacks

SURFnet IDS

- Distributed sensor-based HIDS
- Sensor
  - Any PC
  - USB stick
  - Remastered Knoppix
  - OpenVPN

SURFnet IDS


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

SURFnet IDS server

- Nepenthes
  - Simulates vulnerabilities, and collects mallware
  - More than 20 simulations currently available
  - Reports to PostgreSQL database
- Argos
  - High interaction IDS
  - Can be used to analyse Zero day attacks

SURFnet IDS Webinterface

- Customer can log in
- Access to information of their sensor
- Which attacks
- Statistics

IDS Software: Filesystem Integrity Checking

- Tripwire
- Samhain
  - Client-server based
- Aide

IDS Software: Low-interaction honeypots

- Honeyd:
  - Simulates a host with vulnerable services
  - Simulates complicated networks
  - Well documented
  - Infrequently updated

IDS Software: Low-interaction honeypots

- Honeytrap:
  - Simple: "Poor man's service emulator"
  - Mirror mode
  - Regularly updated
  - Badly documented
  - No community

IDS Software: Prelude (1)

- Prelude:
  - IDS Framework
  - Sensors
  - IDMEF (XML)
  - Policies
  - Web-interface Prewikka

IDS Software: Prelude (2)

- Prelude test:
  - Slow
  - Web-interface needs to be modified

IDS Software: Snort

- Network traffic analyse tool
- Operation Modes
  - Sniffer / logger mode
  - Inline mode
  - Network intrusion detection mode

IDS Software: Snort NIDS mode

- Rules
- Alerts
- Logging

- Implementation

- Maintenance

Conclusion

- Let SURFnet IDS detect more malicious traffic
- Our advice: Integrate Snort
- SURFnet IDS will cover a greater diversity of malicious traffic

Questions?