The Virtues of Continuous Deep Packet Capture and Stream-To-Storage

March 31, 2008

Paal Tveit
VP of Engineering | Solera Networks

SHARKFEST **'08**
Foothill College
March 31 - April 2, 2008

Introduction

- Why Continuous and Why Complete?
- Deployment Strategies
- Value and Benefits
- Use Case Scenarios
- Demonstration
- Q & A

Why Not a Sample?

A sample only gives you a piece of the puzzle

- Samples are often guesswork
- Packet header captures will miss important payload data
- Samples don't represent what happened – not an historical picture
- Trends will be missed

Why not get the whole picture?

- Complete capture and stream-to-storage can reveal all

Deep Packet Capture

Considerations for Deep Packet Capture solutions:

- Full packet (header and payload – Layer 2-7)
- Lossless – nothing gets dropped
- Capture at today's speeds, up to and including 10Gb
- Must be able to capture, store, organize and filter

Stream-To-Storage – The Full Record

- Continuous capture is key
  - Full record can provides foundation for analysis
  - Large record identifies trends
  - Always on – catches everything when you don't know what to look for
- Repository must be large enough for a sufficient record and extensible
- Ability to pull data to permanent storage
  - Archive select traffic for long-term analysis or compliance
- Internal RAID must match network performance
- Fibre Channel and/or iSCSI SAN

Platform: Open vs. Proprietary?

Proprietary platform based on tightly-coupled hardware capture and software analysis tools. Specific solutions that focus on point analysis (top talkers, protocol distribution, etc.).

New open platform providing a software-based solution allows for greater flexibility.

- COTS
- Virtual Machine
- APIs

Software vs. Hardware

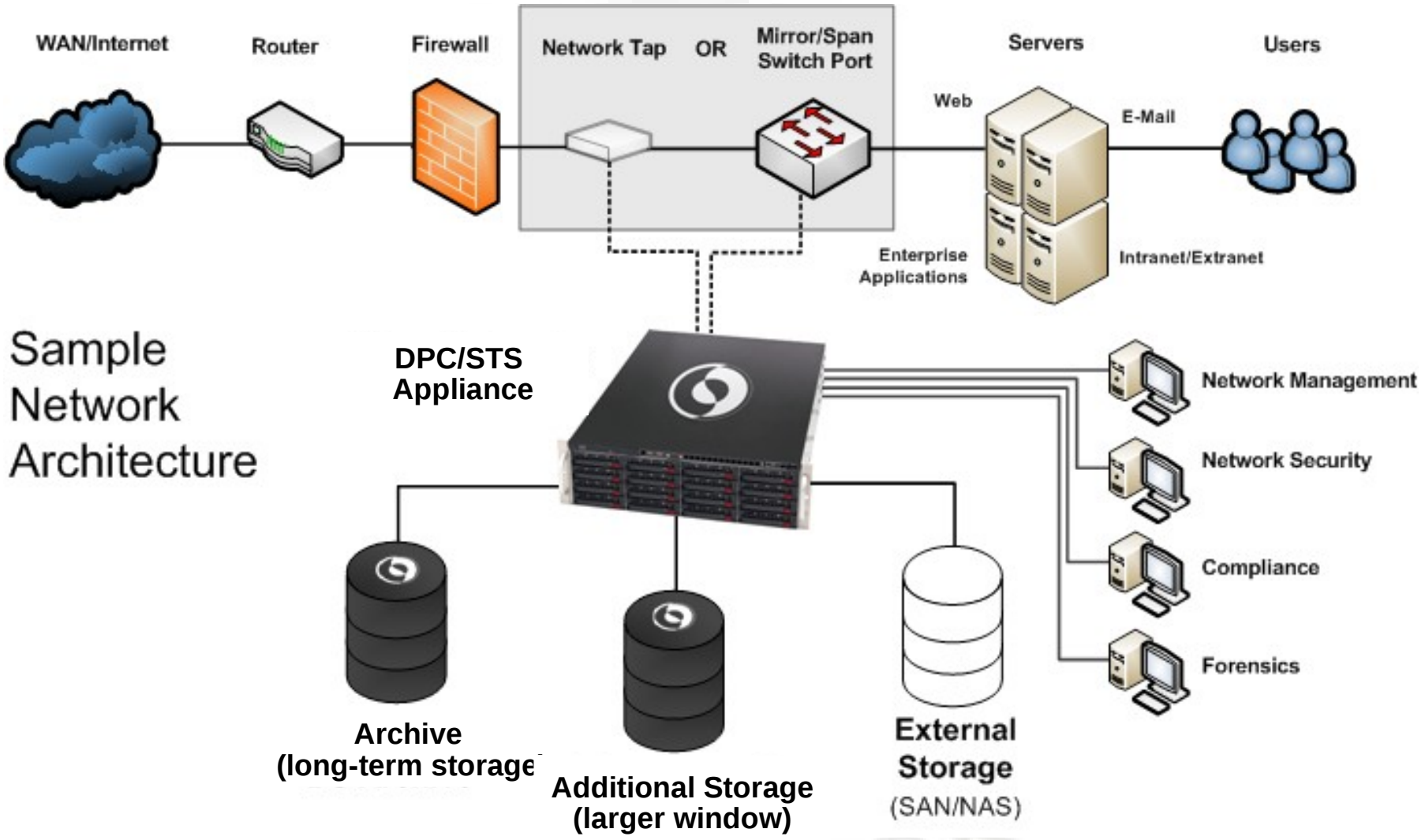
Hardware:

- Dedicated appliances/custom-built appliances
- Proprietary capture cards
- Locked into applications provided by vendor

Software solutions:

- Portability
- Virtual appliances
- Custom applications and development

Deployment – Physical Network



Analysis Methods

- pcap snapshot files from the historical record
- Regeneration onto another network
  - DPI solutions
  - Traffic shaping
  - Throttle traffic to match speeds of analysis tools
- Virtual Interfaces
- APIs for integration into DPC solution

Analysis Tools – Now with Full History

Numerous tools can benefit from a complete record of network traffic

- Packet Analysis Tools
- Instant Messaging (IM) Analysis Tools
- HTTP Analysis Tools
- Web Reporting Tools
- Intrusion Detection/Prevention Systems (IDS/IPS) Tools
- Network Security Tools
- OS Detection Tools
- Network/Application QOS Tools
- Custom-developed toolsets

Challenges

Network Security

- Incomplete Views

Data Loss Prevention

- No Record of Events

Network Management

- Limited Visibility

Compliance

- Not Comprehensive

Challenges/Solutions

Network Security

- ~~Incomplete Views~~ / Comprehensive Surveillance

Data Loss Prevention

- ~~No Record of Events~~ / Complete Auditable Record

Network Management

- ~~Limited Visibility~~ / Replay Actual Events

Compliance

- ~~Not Comprehensive~~ / Unabridged Record of Events

Examples of Use

- Network Security
- Network Forensics
- Network Management
- eDiscovery
- Compliance

Network Security

- Prolonged intrusion
- Security policy update validation
- Data leakage detection

Network Forensics

- DOS and DDOS analysis
- Virus proliferation analysis

Network Management

- Network performance analysis
- Network reliability analysis

eDiscovery

- Network traffic as evidence

Compliance

- Sarbanes-Oxley
- HIPAA

Demonstration

Look at virtual appliance captures

Download pcap

Use Wireshark to analyze pcap

Virtues of DPC and STS - Recap

- You have the whole picture, not just a sample
- It's always on, acting as your backup
- Nothing is lost
- Reduce mean time to resolution of network problems – find the root cause, not just symptom
- Open systems allow flexible deployment and analysis options
- Supports network security, network management, forensics/eDiscovery, and compliance initiatives

It is becoming a best practice – complete network visibility is a priority

Q & A

Thank You

Paal Tveit

VP of Engineering | Solera Networks

ptveit@soleranetworks.com