CSN14: Critical Success Factors for Successful ArcSight ESM Deployments

Michael Wimpy

Unisys

Agenda

- Client Requirements
- Solution
- Data Flow Analysis and its Importance
- When Data Flow Analysis Fails

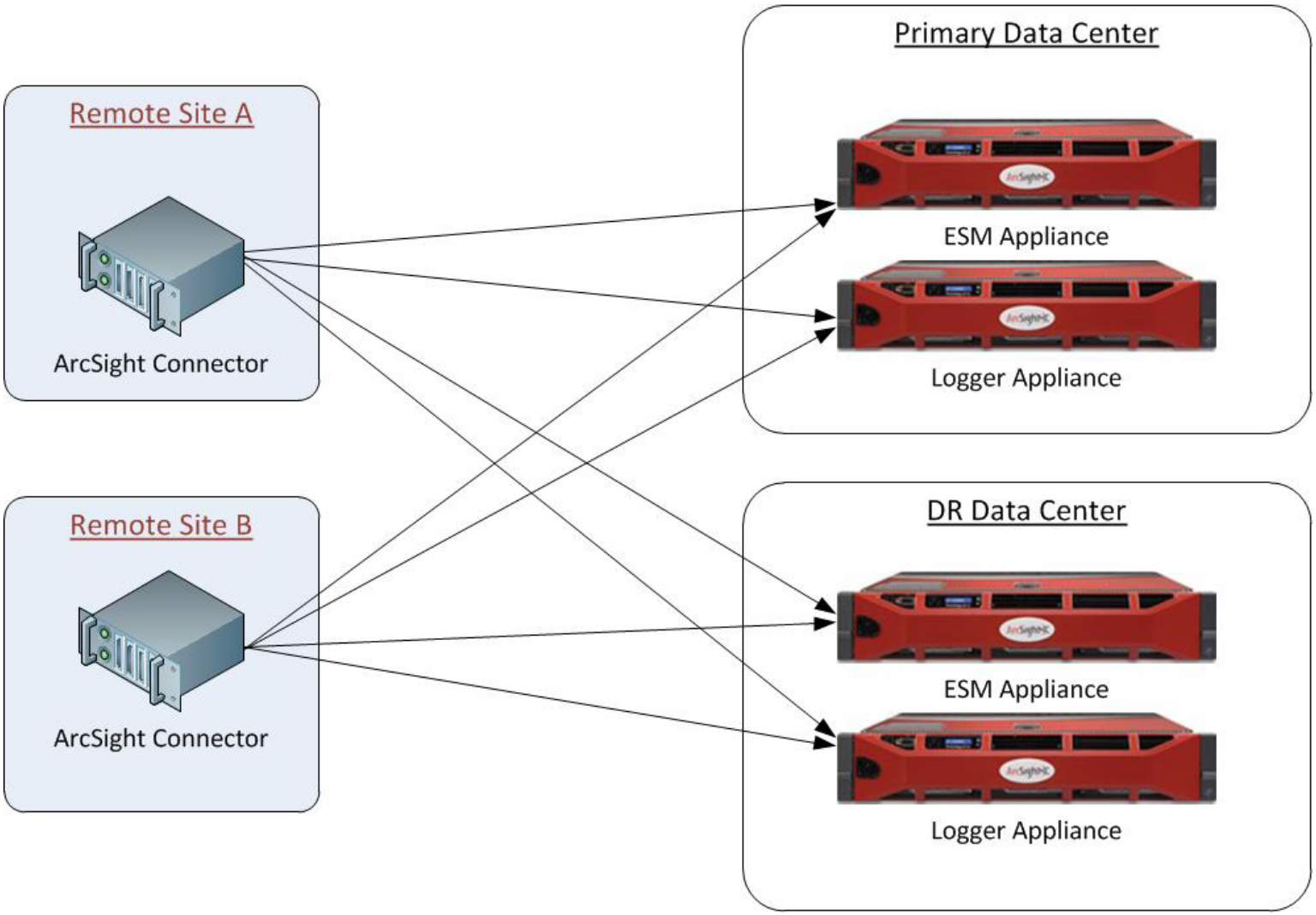
Client Requirements

- Quasi-government client with strict logging requirements
- Real-Time Correlation
- Long-Term Log Retention
- All event data must be fully duplicated at DR site

Solution

- ArcSight ESM Appliance at each site
  - Provides real-time correlation
- ArcSight Logger Appliance at each site
  - Provides long-term log retention
- Each ArcSight Connector will send 4 event feeds
  - Primary ArcSight ESM
  - Primary ArcSight Logger
  - DR ArcSight ESM
  - DR ArcSight Logger

Solution Diagram



Solution Benefits

- Highly Available System
  - Analysts can access either primary or DR system and have access to all event data
- Meets Disaster Recovery Requirements
  - All data is sent in real-time to both sites
- ArcSight appliances save SAN space by using local disk
- Each ArcSight ESM and ArcSight Logger are Independent from Each other
  - One down component will not effect any others

Data Flow Analysis

- What device types do you need to support?
- How many devices of each type?
- Can you get the EPS of the various devices?
  - Solid EPS numbers aren't generally available
- Estimate EPS based on Environmental Knowledge

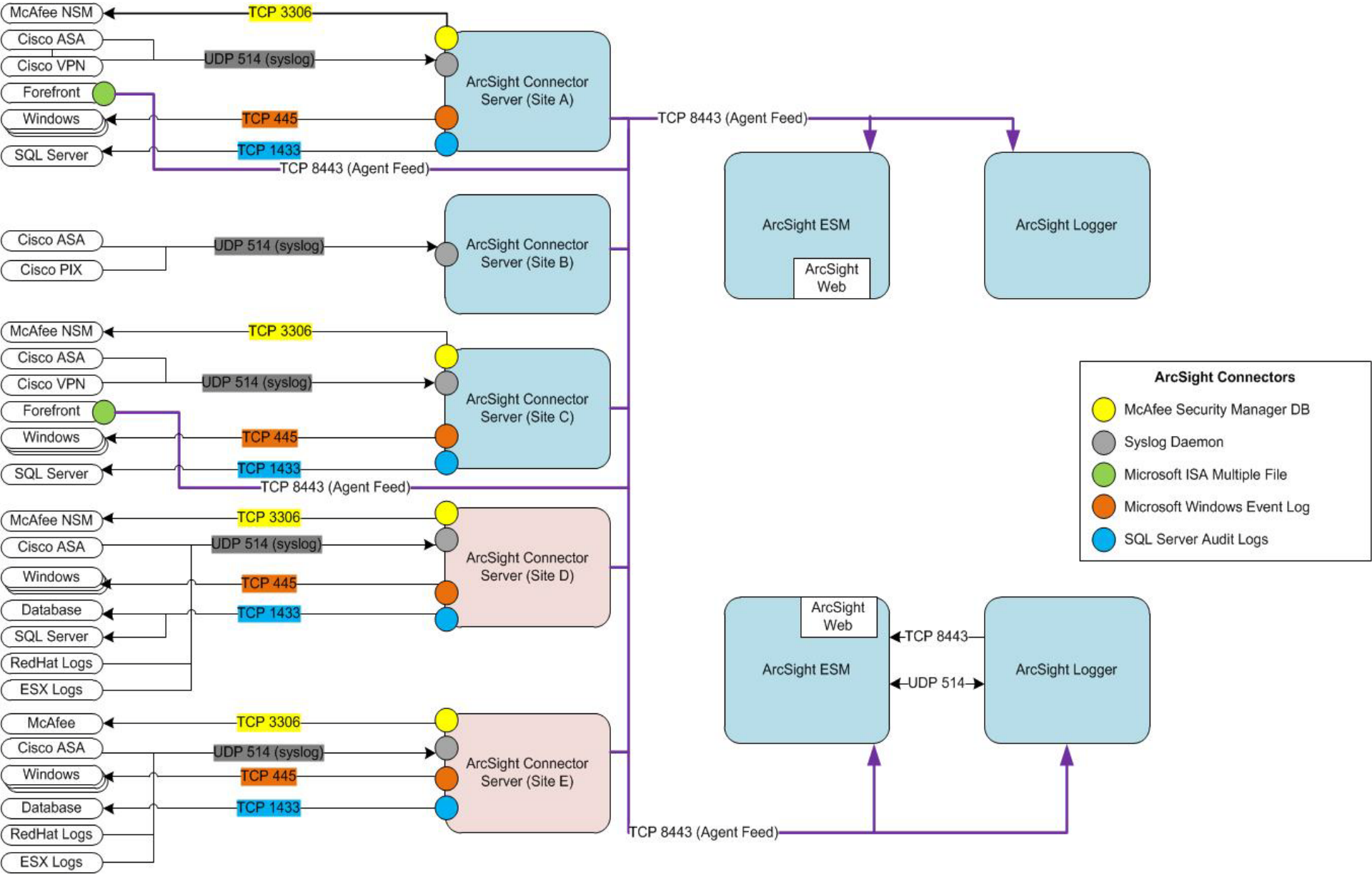
Importance of Data Flow Analysis

- Needed to move from high level overview to detailed design
- Needed to determine the number of ArcSight Connectors
- Determine the location of the ArcSight Connectors
- Determine type of ArcSight Connector feeds
  - Syslog
  - DB Reader
  - SNMP

Data Flow Analysis Recommendations

- Separate ArcSight Connector for each Product
  - Provides easy categorization of event types within ArcSight ESM and ArcSight Logger
  - ArcSight Connector problems only effect a smaller portion of the event flow
  - ArcSight Connector maintenance only effects a smaller portion of the event flow
- ArcSight Connector should be as close to data source as possible
  - Saves bandwidth
  - Provides caching in case of link failure

Data Flow Analysis Results



Data Flow Analysis Not Perfect

- Even the best analysis cannot prevent all problems
- Single syslog pipe connector was being overloaded by a Cisco ASA sending approximately 3000 EPS.
- ArcSight Connector was being overwhelmed
- A single ArcSight Connector cannot utilize all hardware resources of a server.
  - Server was idle because the connector is mostly single-threaded

Possible Solutions

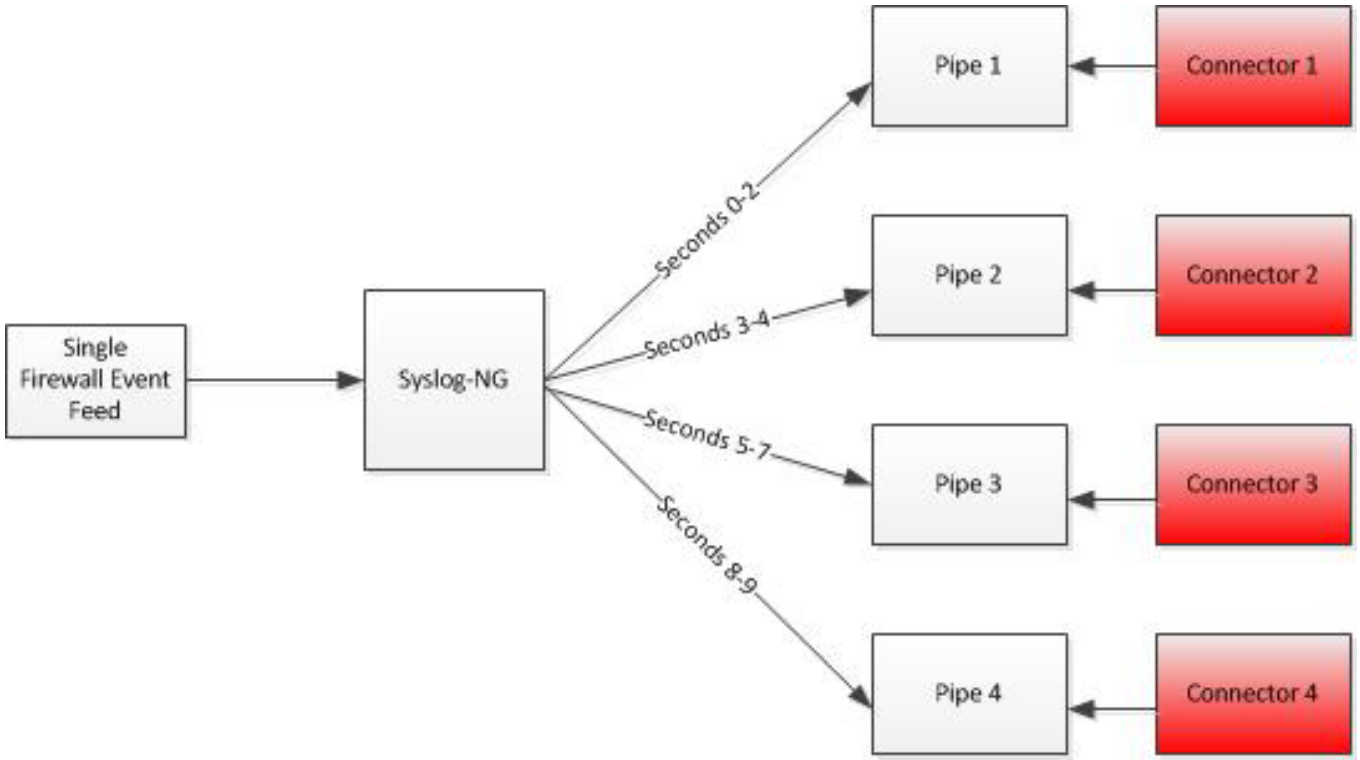
- Decreasing Firewall Logging
  - Would not meet client's stringent logging requirements
- Faster Hardware
  - Improvement from new hardware unknown
  - Cost of hardware
- Load Balance the syslog data

Load Balancing with Syslog-ng

- Syslog-ng is an open-source syslog daemon
- Supports advance configurations and filtering
- Use Syslog-ng's filtering system we can load balance the firewall feed
- Split the single firewall feed into four ArcSight Connectors

Implementation

- Create 4 UNIX pipes to receive the logs
- Install 4 ArcSight Connectors to read from each of the pipes
- Use Syslog-ng filters to split the feed based on the timestamp of the logs



Solution Benefits

- Flexible Design
  - Allows Future Scaling by using more than four connectors
- Low Cost
  - Uses open-source syslog-ng
  - Only requires additional ArcSight Connector licenses
- Quick to implement
- Fully Utilize Hardware
  - Multiple connectors allow you to use all CPU resources on a single server

Summary

- ArcSight ESM and Logger allowed us to build a scalable and highly available SIEM solution
- Determining client requirements are the first step before any real design begins
- Data Flow Analysis is critical to an efficient and scalable design
- Data Flow Analysis isn’t perfect
- Creative solutions are often necessary to deal with problems that arise

Questions

- Any Questions?