Setting the Standard for Automation™

Managing your process control firewalls – real world life cycle challenges

Standards
Certification
Education & Training
Publishing
Conferences & Exhibits

Presenter – Tom Good

- BS Chemical Engineering – Lehigh University
- 32 years experience with system integration of IACS
- 12 years experience coordinating corporate wide cyber security measures for IACS
- 10 years experience overseeing management of IACS firewalls
- Chair and primary author of ISA S99.02.01 (IEC 62443-2-1)

Objective

- Raise awareness of the life cycle issues associated with firewalls and the challenges of managing them

- Firewalls add to the already challenging task of managing IACS life cycles.

Agenda

- Use of a firewall managed service provider
- Firewall management challenges
  - Trust
  - Technical competency
  - Division of responsibility
  - Managing change and security
- Life cycle challenges
  - People turnover
  - Hardware obsolescence
  - Software obsolescence
  - Expiration of certificates
  - Technology advances

Use of a leveraged firewall service provider

- What is a leveraged firewall service provider?
  - In-company or 3rd party providing firewall management and support functions

- Why use a leveraged service provider
  - Lack of skilled resource at each firewall location
    - Changes are infrequent: easy to forget how
    - Need a security focus, not just how to accomplish
  - Lower life cycle cost than to provide a skilled resource at each location and a backup for that person
  - Division of responsibility – some checks and balances
  - Potential for bringing external vulnerability information to the table.

Challenges with a service provider

- Fear of losing control - trusting the provider
- Establishing the level of service needed, not what you want to pay
  - Same to all locations or differentiated
- Building the management of change process that works for all involved
- Co-access to all information
  - Read only for most occasions
  - Full access in the event of an emergency
- Location and ownership of the management infrastructure

Some key decisions

- Should I use the same service supplier for all IT and process control firewalls?
  - May need differentiated services following different processes
    - Approval of changes due to scope impact of the change
    - Response time
  - Who is in charge of the contract?
  - What is the emphasis of the contract?
    - Connectivity and ease of user access
    - Security and control
    - May change over time based upon issues experienced

Key recommendation

It you are going to operate firewalls as a leveraged service, then gain the authority to run it as a leveraged service.

(Most efficient and lowest life cycle cost)

Life cycle realities

- Change occurs faster than wanted in the Operations IACS space
  - Service providers change ownership; mergers, acquisitions, divestitures
  - Firewalls are IT commodity devices
    - Hardware wears out
    - Software life cycles
    - Manufacturers and product lines are bought up and sold off
    - Infrastructure management tools have life cycles
  - Security technologies evolve to meet changing threats
  - IT technologies have major leaps
    - Virtualization
    - Cloud

Service providers change ownership

- Occurs more frequently than IACS ownership changes
  - Potential to impact personnel top to bottom
  - Experience has been more change at the top than bottom
  - Process control firewall management resources less of a commodity

- Value in maintaining internal company oversight continuity
  - IT and Purchasing turnover higher than Operations
  - Maintain a strong Operations influence

Trade-off: Personnel changes

- Change in personnel at the service provider impacts all sites

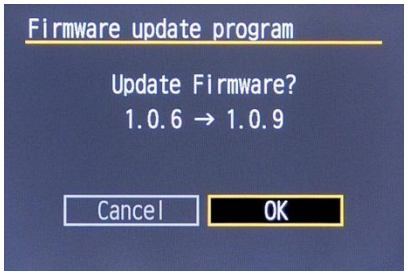
Versus

- Change in personnel at one site just impacts that site

- Responsibility for continuity of service and backfill of skilled resources is the responsibility of the service provider
  - Elapsed time to address personnel changes is likely to be less

Firewall life cycle realities

- Over period of 13 years of use, have experienced
  - Firewalls physically wear out (3 generations)
  - Firewall software sunset (1 instance)
  - Firewall companies bought up and product lines discontinued (3 times)
  - Firewall management infrastructure changes (2 instances due to physical device wear out, 2 instances due to product line life cycles)



- Over the same period of time
  - No changes to the IACS level 2 devices
  - 1or 2 life cycles of the IACS level 3 devices

Challenge with a leveraged environment

- Typical firewall life cycle 3-5 yrs
- With a large managed environment it may take 2-3 yrs to work through a full refresh cycle
- Management infrastructure likely needs to change with firewall refresh
  - Running 2 sets of tools almost as long as the sweet spot of running a single tool. (Periods of duplicate costs)
  - For several years running concurrent projects to refresh site firewalls, to operate overlapping management tools, and to move users to different tools both at the service provider and the sites

Firewall software upgrades

- Release hot fixes/patches several times a year.
- Major releases once a year for new features
- Respond to industry change – SHA-1 to SHA-2 certificates
- May require reboot of the firewall and some downtime

- Recommendation – Establish a plan to deal with upgrades just like other PM work during shutdowns.

Firewall PM work

- Appropriate annual PM work
  - Install software updates and new releases
  - Switch to the “backup firewall”
  - Any firewall configuration change that requires a reboot
  - Replace firewall if a hardware refresh is scheduled
- Ideal time is during a site shutdown
  - But everyone is already very busy
  - Not all IACS devices may be operational, so a full post-change checkout may not be possible.
  - Get the new firewall in place with minimum downtime and no interruption of user access
- And the winning priority is . . . . .?

Certificate updates

- Industry is sun-setting SHA-1security certificates
- Older firewalls may not be able to handle SHA-2 certificates without software updates
- For a large environment with out-of-date firewall software this is a significant amount of work

VeriSign®

Security reviews

- Firewall rules can quickly fall into disrepair
  - Add new rules don't remove old ones.
  - Temporary trials
  - IACS devices eliminated or replaced
  - Mistakes/typos
    - 14.244.117.0/14 instead of 14.244.117.0/24
      (Allows access to 262,142 devices instead of 254 devices)
  - Hidden Rules
  - Hosting provider changes
  - Replacement of network tools
  - Divestitures
  - Access accounts not removed when personnel changes occur

Security Review Tools

- Adopt the use of a change management tool(s)
- Strongly recommend use of a firewall audit tool
  - Eliminate unneeded rules
    - Report rules that have not ben used in xx days
    - Report devices that have not been used
    - Reports devices assigned to groups
    - Report when users last passed through the firewall
    - Report access privileges
  - Identify something wrong
    - Report sources and destinations of rejected packets

- Need IACS process knowledge and network knowledge

Summary

- Don’t let your firewalls become expensive routers.
- Life cycle management activities are necessary
  - Some tasks require specialized skills
  - Some tasks require process and IACS knowledge
  - System outages will be required
  - “No news isn’t necessarily good news” (from a security perspective)

- Firewalls add to the already challenging task of managing IACS life cycles.