CNI Boundary IT Security Assessments

Jonathan Cowlard

IT Security Assessment Technical Lead

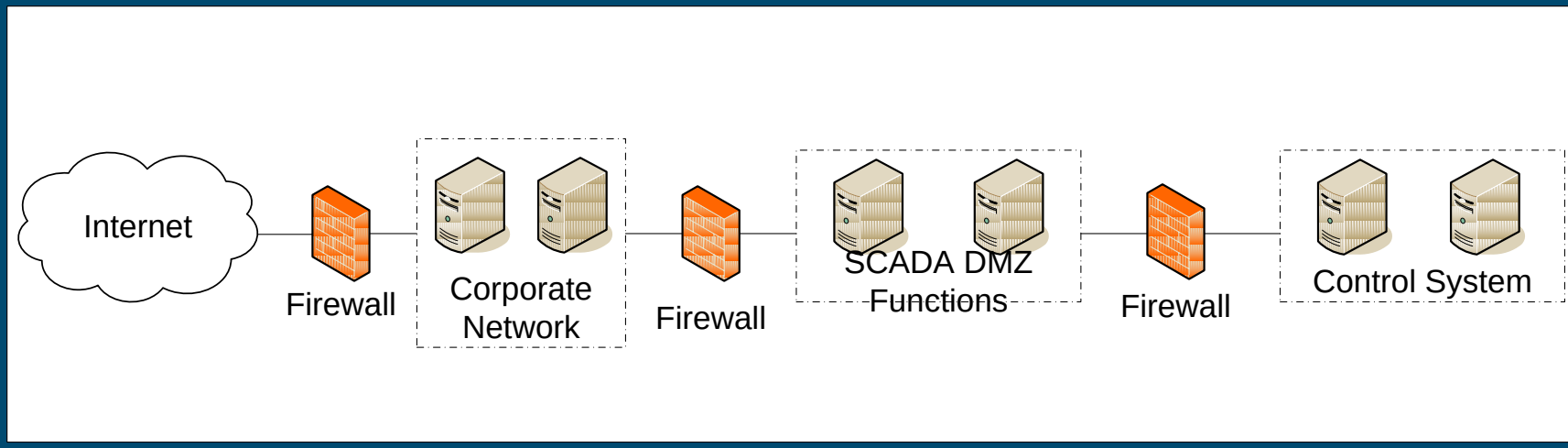
Background

- Task
  - Assess IT security of Critical National Infrastructure (CNI)
  - Broad range of control system designs
- Aim
  - Inform current control system vulnerabilities picture
- Assumption
  - Corporate network security has been breached

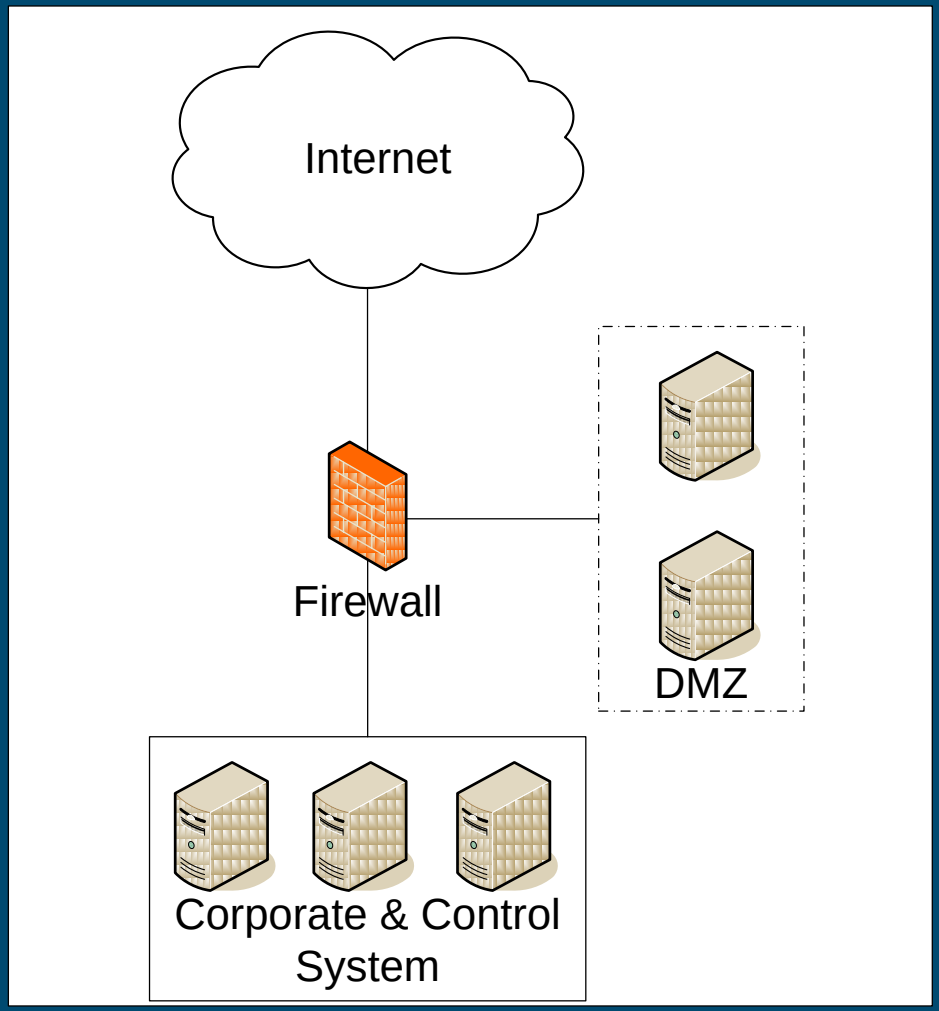
Presentation Overview

- CPNI Best Practice
- Examples: Weak Network Designs
- System Vulnerabilities
- Policy Weaknesses: Observations
- Recommendations
- Conclusions

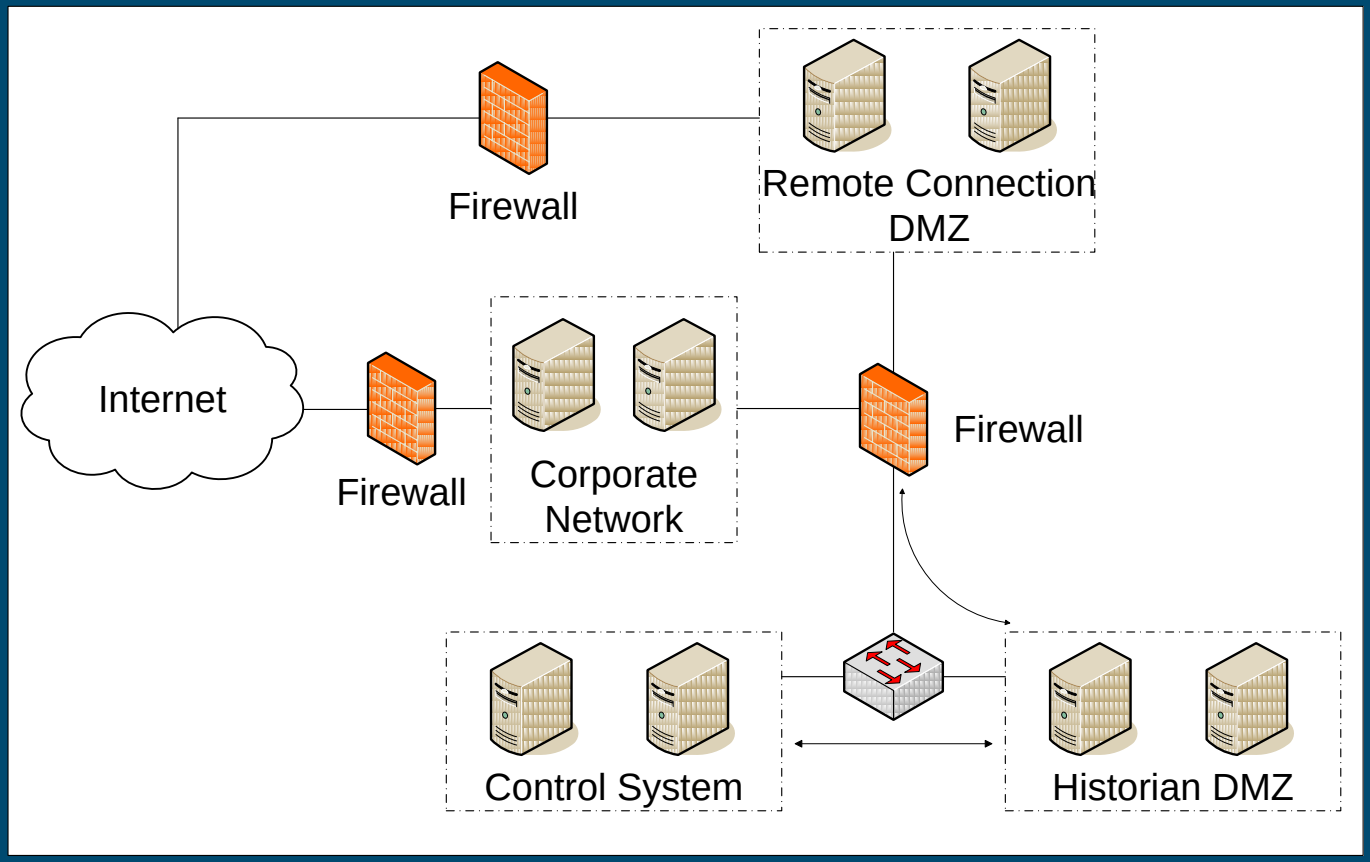
CPNI Best Practice Guideline



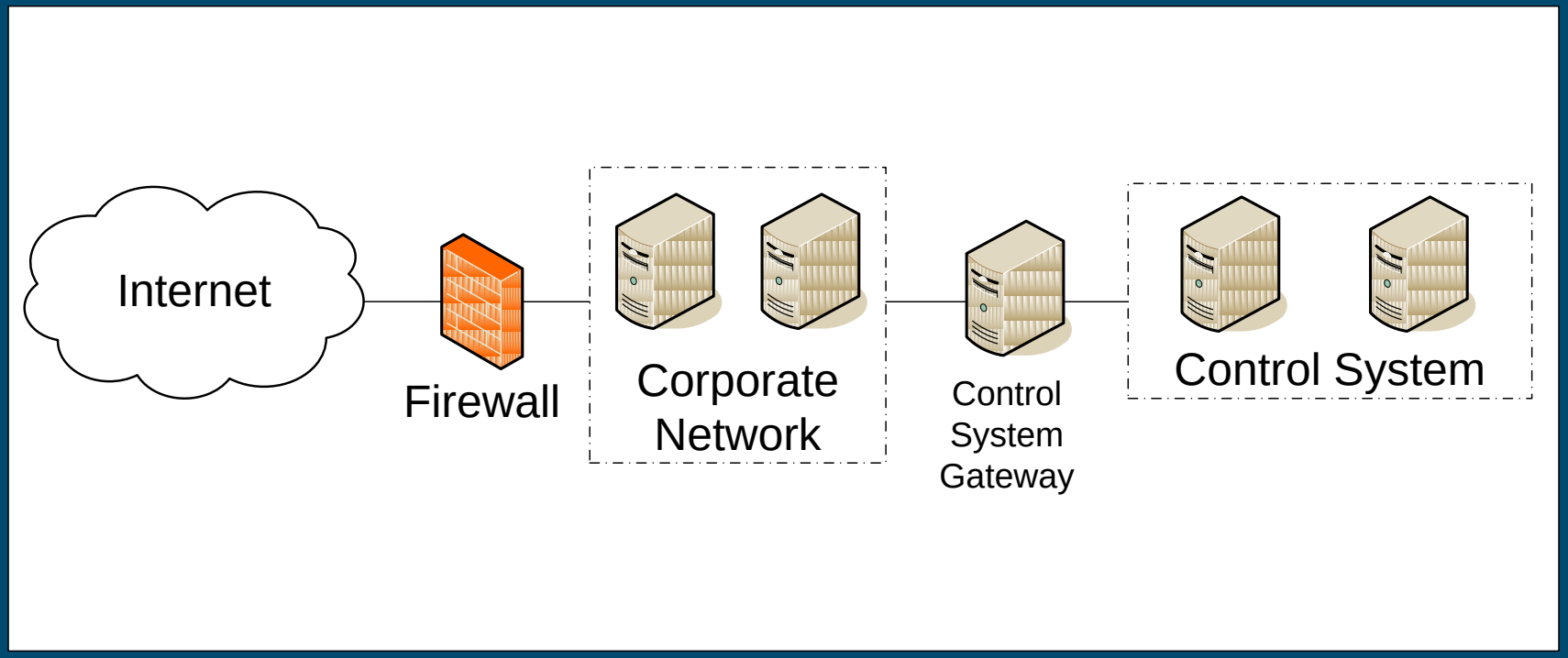
Example: Weak Network Design



Example: Weak Network Design cont…



Example: Weak Network Design cont…



System Vulnerabilities

- Unpatched Software
  - Publicly known vulnerabilities
- DMZ insecurity
  - Enabling communication through DMZ
- Information leakage
  - Intranet sites
  - Insecure communications
- “Trusted” Network Architecture
  - Reliance of secure corporate connectivity

Policy Weaknesses: Observations

- Lack of accountable roles and responsibilities
  - No single person responsible for security in control system domain.
  - No Impact analysis of outsourcing upon accountability.
  - No culture of IT Security.
  - Accountability for physical malfunction due to control system insecurity.
- Inadequate documentation
  - Minimal configuration documentation.
  - System integrity levels unclear.
- Patching strategy
- Auditing

Recommendations

- Retrofitting Security
  - Firewalls / IDS
- Provide clear demarcation between corporate and control system networks
  - Implementation of CPNI best practice
- Responsible patching is a quick win
  - Test patches before live deployment
- Clear IT Security Strategy, implementation and review
  - Accountable roles for implementation
- Future implementation of Defence in Depth

In Summary…

- Vulnerabilities discovered in all networks
  - Likely to provide route to control system network
- Remediation action is available
  - Responsible patching and retro-fitting of security devices
- Network security strategy
  - Ensure accurate configuration documentation
  - Create a point of contact responsible for control system network security