



Implementing Network Access Controls



Using the Information Systems Architecture

William P. Flinn



Agenda:

- Hypothesis
 - Overview of Network Access Controls (NAC)
 - Why is an ISA Framework Needed?
 - Significant Background Information
 - Organization and Infrastructure
 - Policies, Standards, and Procedures
 - Security Baselines and Risk Assessments
 - User Awareness and Training
 - Compliance
 - Conclusion
-

Hypothesis

- NAC system provides aggressive security measures
 - Implementing NAC requires the key elements of an ISA framework
 - Without using an ISA framework, the project will be unorganized and doomed to failure.
-

Overview of Network Access Controls (NAC)

- Port Security
 - “Quarantining”
 - Ensures only “healthy” computers access the network
 - Uses hardware and software solutions to perform host inspections and provide DHCP configuration controls
-

Why is an ISA Framework Needed?

- Information Systems Architecture (ISA) provides organized process
 - NAC is a large project
 - NAC is an aggressive security measure
 - Risk for both implementing and not implementing
 - Project Management techniques will be key elements in implementation
-

Significant Background Information

- Large enterprise
 - 9,000+ Desktops
 - 300+ Servers
 - Field offices and data centers – 400 sites world-wide
 - Telecom equipment (routers/switches/circuits) at all sites
 - Remote access (Cisco VPN) widely used by field inspectors and WAH (telework) personnel
-

Organization and Infrastructure

- Large number of resources needed to support system
 - Support personnel will have to be cross-trained
 - Windows Engineers, Network Engineers, Help Desk
 - Enterprise routers and switches interact with NAC and do inspection processing
 - Is the existing equipment compatible/capable?
-

Policies, Standards, and Procedures

- Stated policy in place requiring NAC
 - Standard equipment that will interact well with infrastructure
 - Product selection
 - Is it Common Criteria Certified?
 - Does this matter?
 - Procedure guides need to be clear and well written
 - Support personnel and cross-training
-

Security Baselines and Risk Assessments

■ Baselines

- Router, Switch, Server performance
 - Perform testing to anticipate processing loads
 - Before and after implementation

■ Assessing the risks:

- To implement – Possible business risks
 - Not to implement – Possible security risks
-

User Awareness and Training

- Used to overcome:
 - Security unawareness
 - Empathy
 - Resistance to compliance with policy
 - Show the users how aggressive security will keep their data safe
 - Help users realize their responsibilities in security
 - Assist users with understanding how they will interact with the system – what might happen
-

Compliance

- How well is the organization following and complying with defined policies, standards, and procedures
 - Federal Government regulations
 - HIPAA
 - Sarbanes-Oxley
 - Gramm-Leach-Bliley Act
-

Conclusion

- The ISA framework provides an organized and methodic implementation process for NAC
 - ISA elements help implementation process ensure all necessary points are considered:
 - Infrastructure
 - Policies, Standards, Procedures
 - Baselines and Risk Assessments
 - Awareness and Training
 - Compliance
-

Questions and Answers

