

ISS Policy and Use of EA Products in Enterprise Security Management

Presented to: NAS EA Conference
By: NAS ISSM
Date: 6/26/2009



Federal Aviation
Administration



Agenda

- Background
- Defense in Depth
- Security Framework
 - Policy
 - Perimeter Protection
 - Incident Detection and Response
 - Transaction Security
 - Access Control



Background - ISS Goals

- Office of the President Goals
 - Strengthen Federal Leadership on Cyber Security: Cyber infrastructure a strategic asset
 - IPC: National Cyber Strategy
 - Harden our Nation's Cyber Infrastructure
- FAA mission
 - Constantly improve safety
 - Increased capacity and better operational performance
- CIO
 - Establishes policy and guidance in the areas of IT capital planning, enterprise services, data and information management, information systems security, portfolio and program services, privacy, and research and development
- ATO CIO
 - Represents the interests of ATO for NAS, Mission Support, and Admin Infrastructures to ensure ATO meets mission objectives
- ATO ISS Program
 - Represents all Service Units and Service Areas within ATO to enhance the Information Security posture in the FAA infrastructure.



Background – Continued

→ FAA Enterprise Architecture Environments

- NAS Operations
- Mission Support
- Administrative Systems



→ Network Connectivity Infrastructures

- FTI Ops WAN
- FTI Mission Support WAN

→ FAA Organizational Participants & Roles in Architecture Definition

➤ AIO

- Define a FAA architecture to meet federal requirements and align budgets

➤ ATO

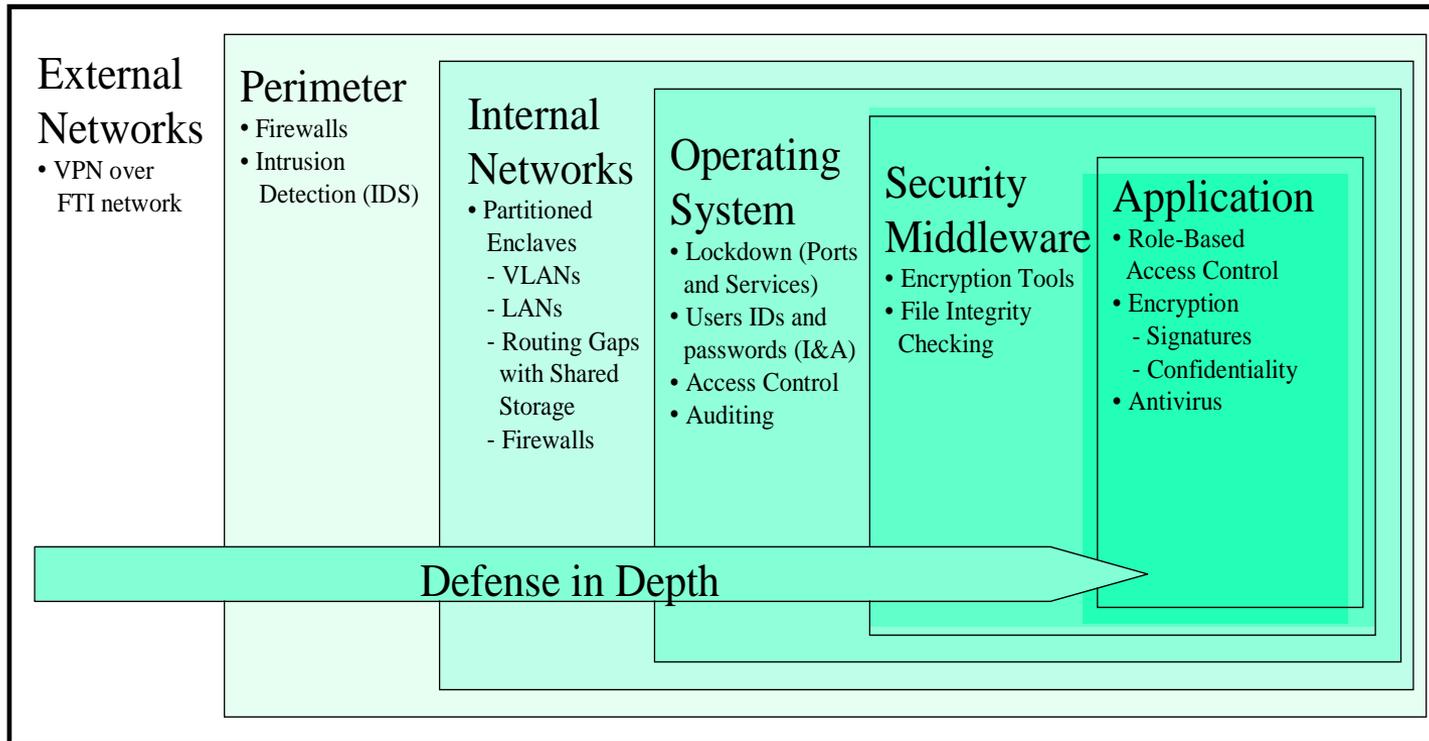
- ATO-P – Enterprise Architecture for future FAA NAS including NextGen
- ATO-F – Admin & Mission Support Architecture within ATO
- ATO-E – Architecture for future NAS En Route environment
- ATO-T – Architecture for future NAS Terminal environment
- ATO-R – Architecture for future NAS System Ops environment
- ATO-W – Architecture for ATC Communications and Weather Services

➤ ATO ISS Program

- C&A and Remediation for all ATO environments (NAS, Mission Support, and Admin)
- Incident Response



Defense in Depth



Enterprise Security Framework

- Policy
- Perimeter Protection
- Incident Detection & Response
- Transaction Security
- Access Control and Automated Policy Enforcement



Policy

→ Current Policies

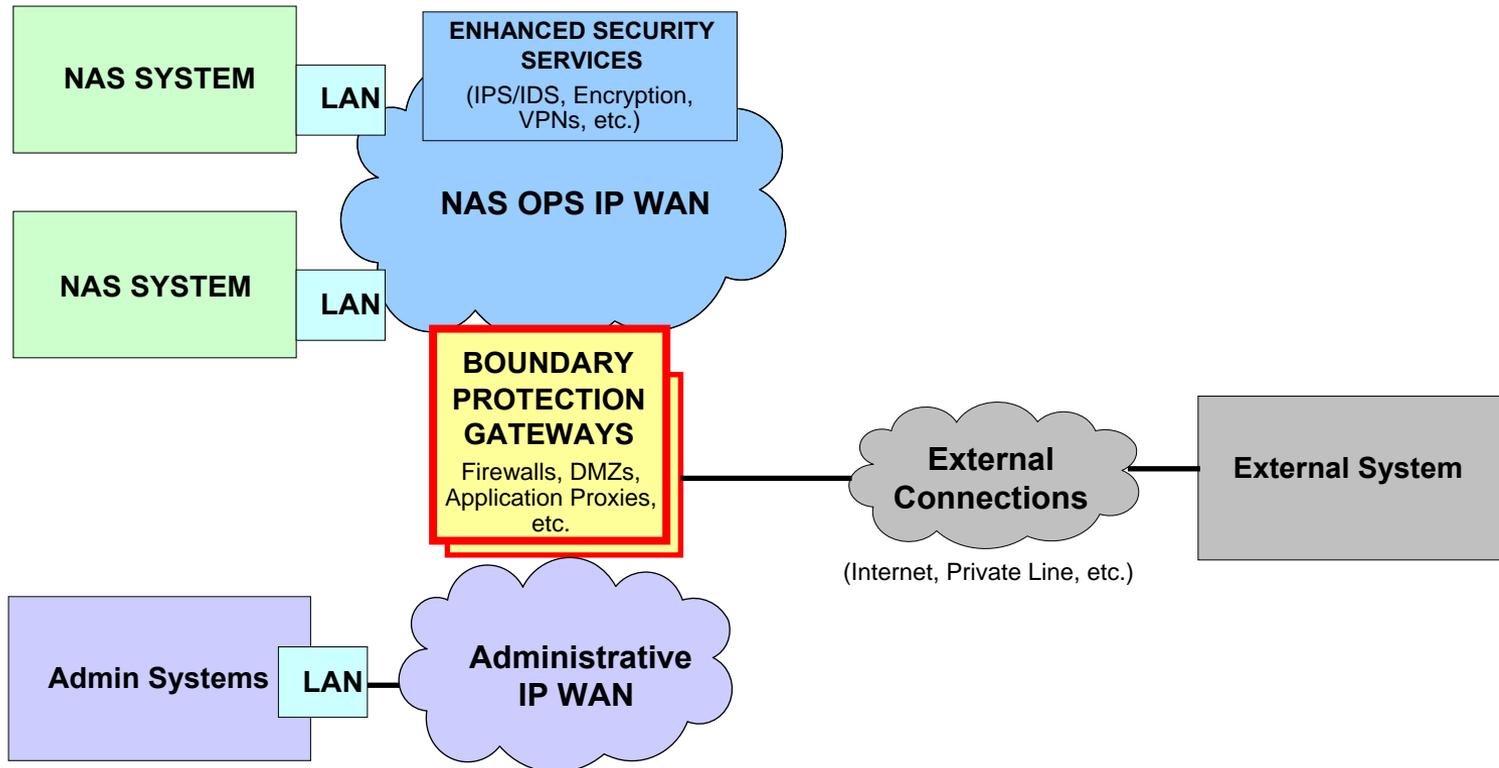
- Logical Access Control Policy (1370.105)
- Encryption Policy (1370.103)
- Digital Signature Policy (1370.104)
- Data Release Policy (1200.22D)
- NIST, FISMA and OMB Circular A-130
- FAA ISS Program Policy (1370-82A)

→ In Planning

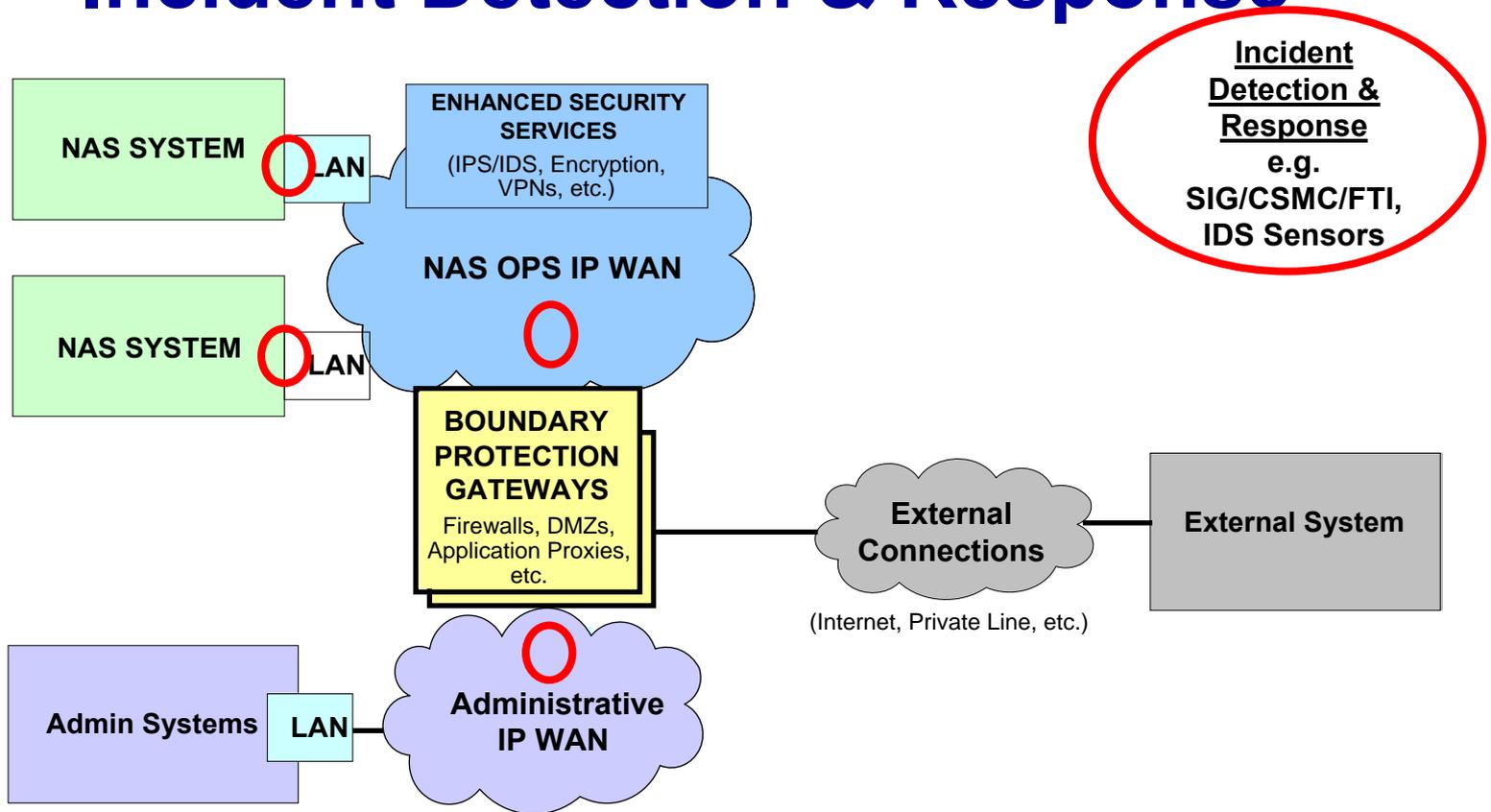
- Secure Code Assessment Policy
- Boundary Protection Policy
- VOIP Policy
- Update External Connection Policies

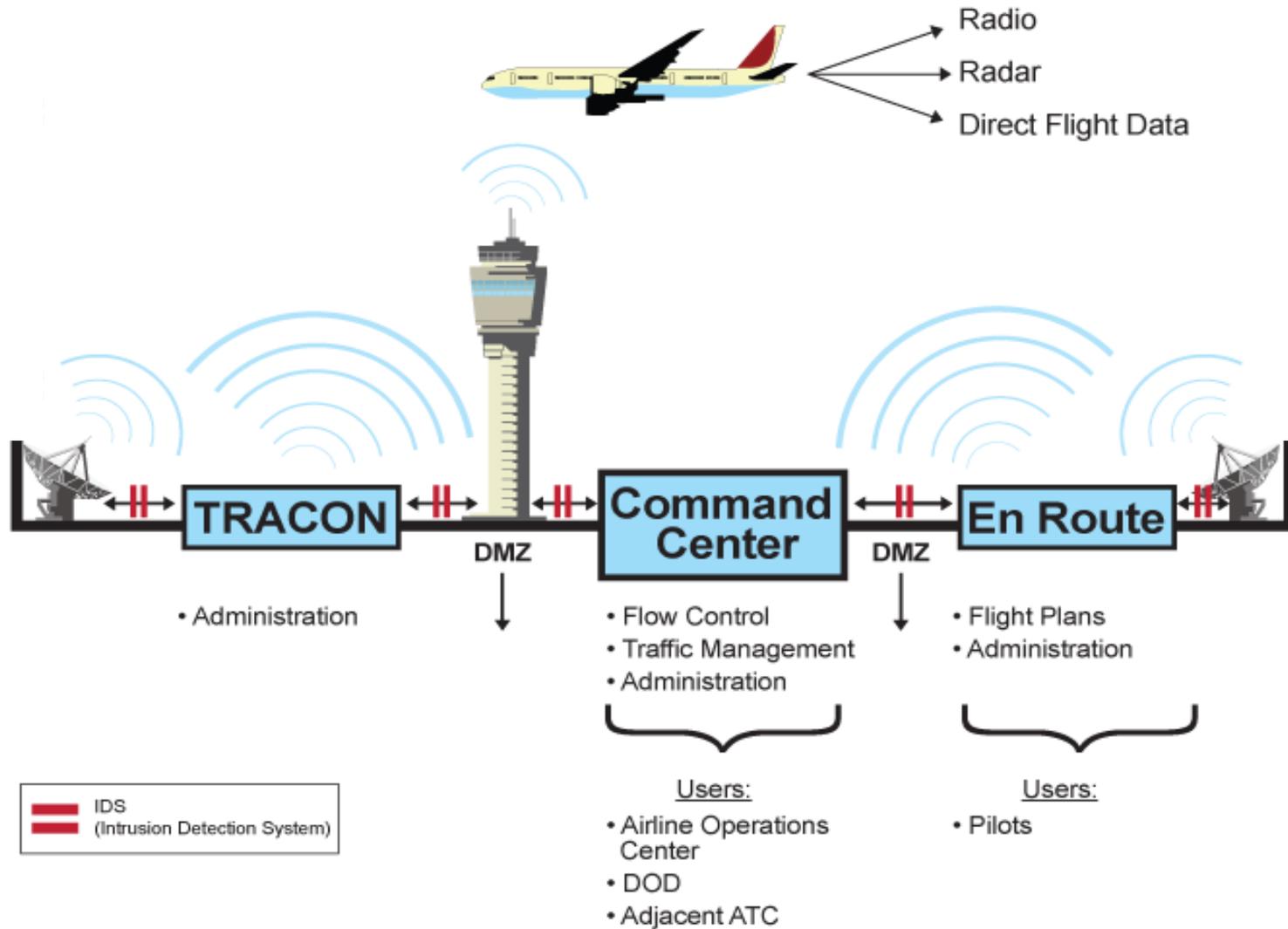


National Airspace System Isolation and Perimeter Protection



National Airspace System Incident Detection & Response





Incident Handling Methodology

- Detection of events
- Preliminary analysis and identification
- Preliminary response actions
- Incident analysis
- Response and recovery
- Post incident analysis



Security Monitoring and Operations

→ FAA has 24 X 7 security monitoring and incident response

- Functions separated for Operational and Administrative networks
- Direct interface to DOT/FAA Cyber Security Mgmt Center (CSMC)



FT11002509-00_00

→ Respond to intrusion attempts, malicious logic incidents and physical threats



Transaction Control

→ Currently

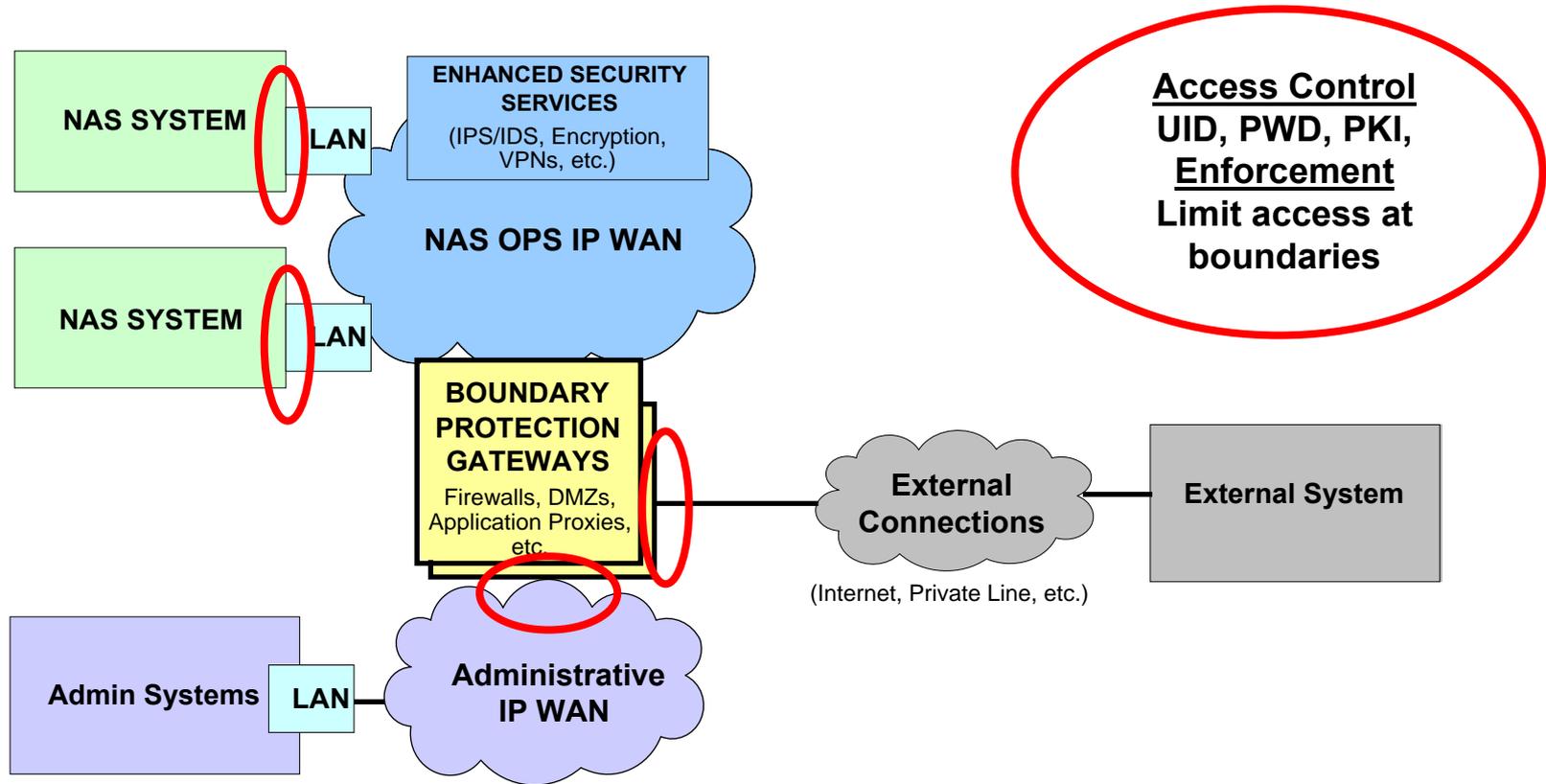
- Provide encryption, authentication, credential, middleware, and other transaction services suitable for SOA across the NAS
- Virus checks for software delivered to field

→ Future

- Public Key Infrastructure (PKI) to sign and encrypt code
- Inter-device authentication using PKI



National Airspace System Access Control / Policy Enforcement



Summary

- System by system approach to Security (initial)
- Enterprise Approach (future)

- Standardize security across systems
- Optimize ability to apply security controls
- Clearer picture to risks to Enclaves
- Foster simplified communication and connectivity between International, National and Internal organizations
- Ultimately bring us in line with the Presidential goals of hardening the cyber-security infrastructure

