As presented at NIKSUN WWSMC
July 25-27, 2011 | www.niksun.com

# Securing the AF Intranet

**NIKSUN**

**World-Wide Security and Mobility Conference**

**Col (ret.) Russ Fellers**

**25 July 2011**

# Agenda

- Network Security: AF Perspective
- AF Network Security Challenges
- Goal: One AF, One Network
- AF Intranet Defined
- Focus on AF Intranet Gateways
- Way Ahead

U.S. AIR FORCE

# What *IS* Network Defense?

- Protect the Network (from denial, degradation, intrusion)
- Protect the Host (from compromise, infection, "insiders")
- Protect the Application (from breakage, exploitation, misuse)

- Confidentiality (keep pertinent data private, inc. access/usage)
- Integrity (keep data and users safe, whole, unaltered)
- Availability (keep network and resources *up* and functional)

- Authenticity (keep messages, transactions 'true', verifiable)
- Non-Repudiation (prove beyond doubt that you did/didn't do)

- Defense-in-Depth? (heterogeneous conduit, multi-layered)
- Mission Assurance? (crown jewels, fight-through, survivability)

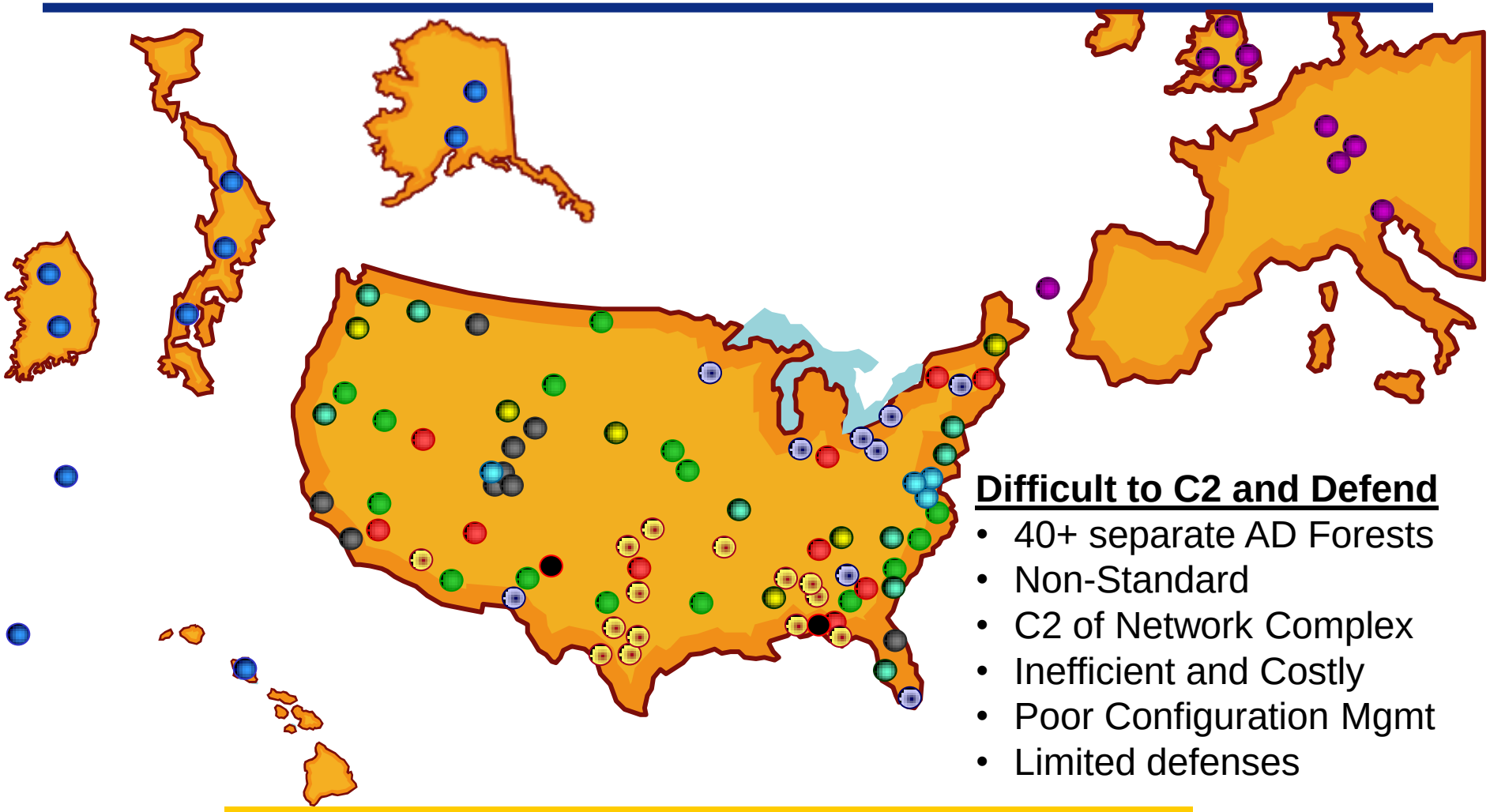
U.S. AIR FORCE

# *Why Security is Essential to AF Operations and Cyber Dominance*

- **AF networks were previously used primarily for administrative functions and daily communications**
- **Today nearly every critical support function relies on the AF-GIG—airlift, logistics, personnel, readiness, medical support, security forces, finance…**
- **AF nets are increasingly integral to core AF operations: C2, ISR dissemination, real-time reachback, airborne comms, telemedicine, just-in-time supply, coalition comms**
- **As air and space networks are further integrated, geolocation, in-flight comms, battlefield C2, weapon system data integration, ATO transmission, real-time targeting, refueling coord, close air support…all will be dependent on AF nets**

*Modern Warfare is Net-Centric Warfare …*
*and our Nets are Under Threat*

# The Challenge:
# Previous State of the AF Network

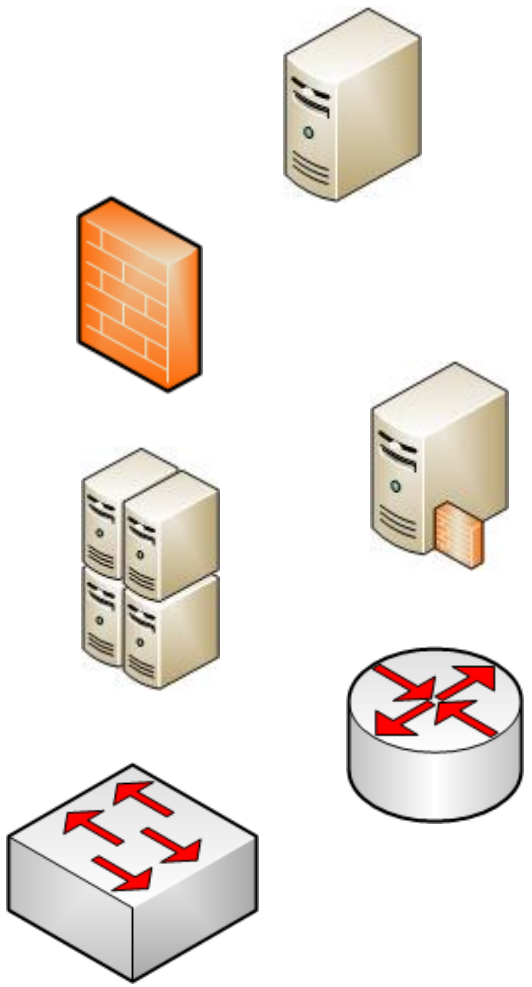


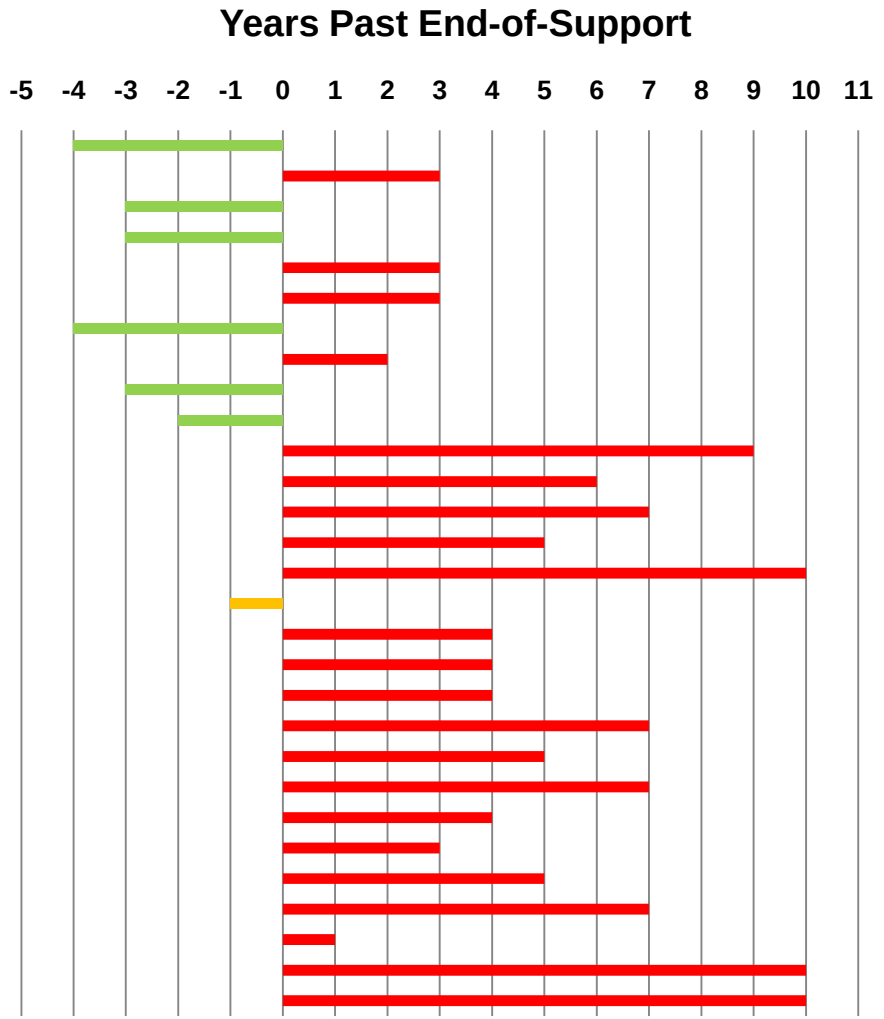
**Difficult to C2 and Defend**

- 40+ separate AD Forests
- Non-Standard
- C2 of Network Complex
- Inefficient and Costly
- Poor Configuration Mgmt
- Limited defenses

**Hundreds of "Front Doors" to protect**

# More Challenges: Aging Infrastructure



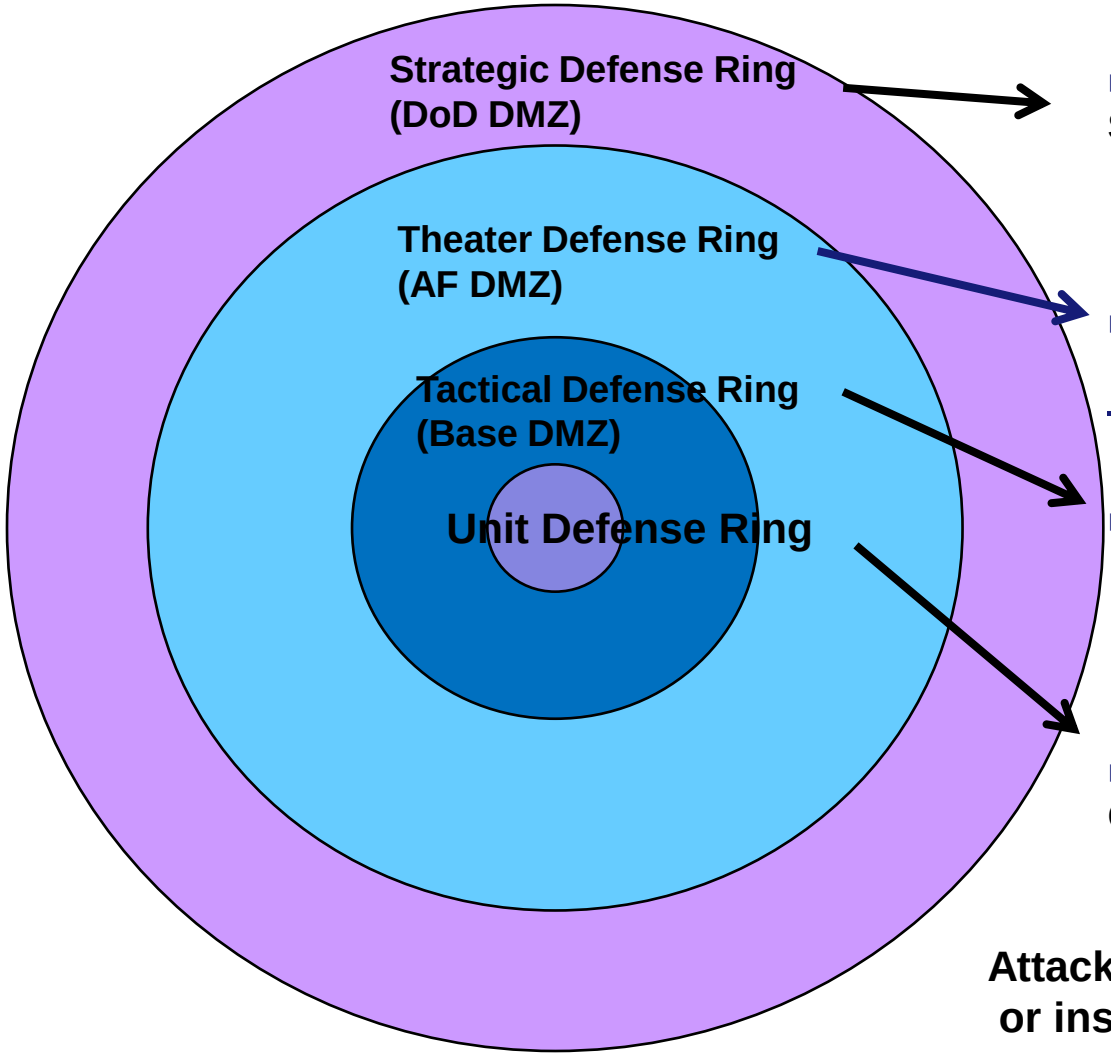


# Goal…One AF, One Network

- Centrally managing network defense and security—all firewalls managed at AF-level instead of at each base—increase Info Assurance
- Going from 10 MAJCOM command elements to 2
- Consolidating the AF from a federation of 9 MAJCOM nets to 1 AF net
- Consolidating network storage, e-mail, and network servers
- Centrally managing network services
- Providing Core Enterprise Services
- Providing an AF-level help desk
- Modernizing the infrastructure and operational/tactical tools to manage and secure the USAF's portion of the GIG


*Deploying IT infostructure to secure and manage the Air Force network*

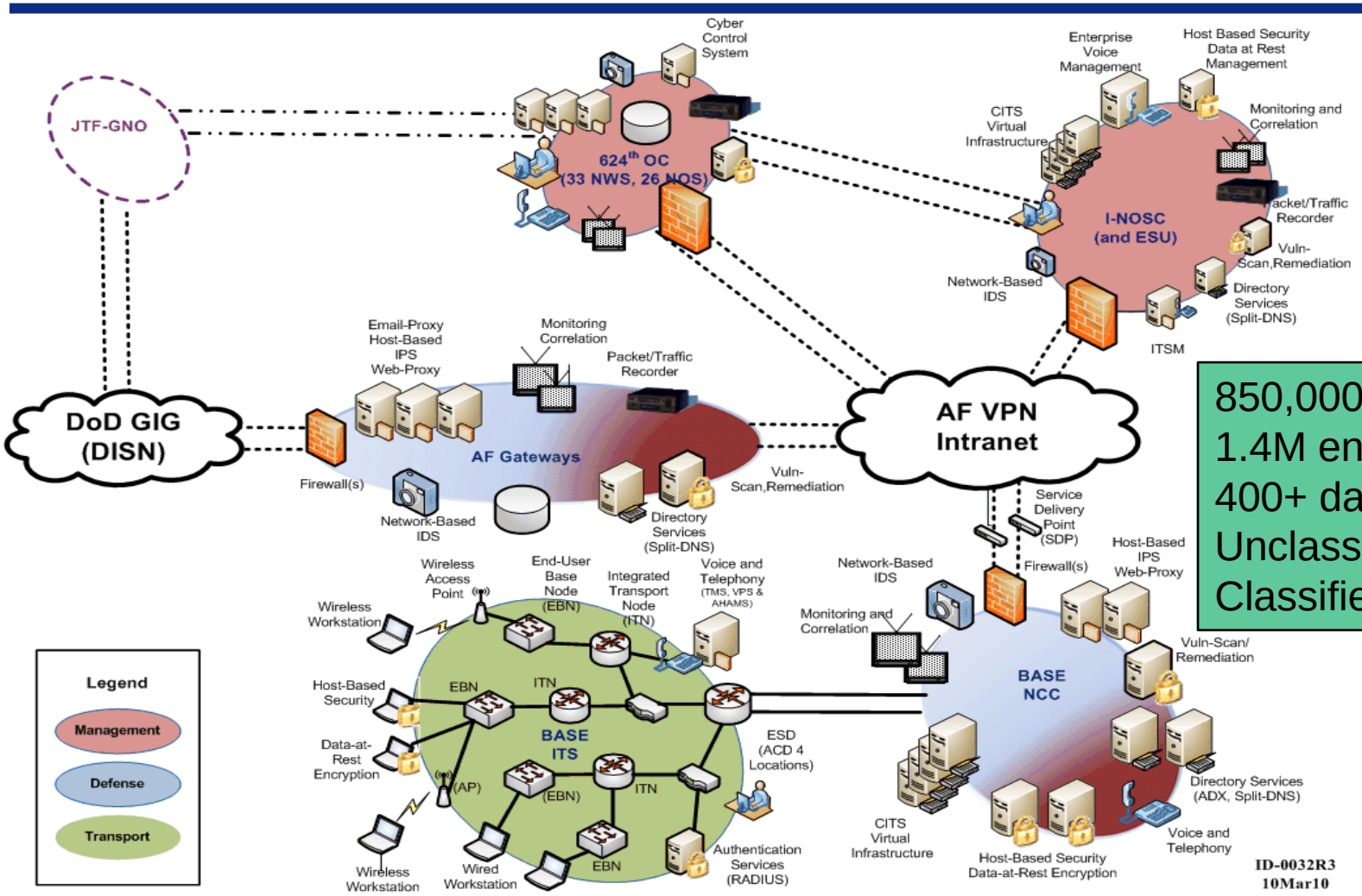
# The Goal
# Layered Defense




- DoD DMZ under Defense Information Systems Agency C2 to protect the GiG
- ***AF DMZ under AF C2 to protect The AF Intranet (AFNet)Gateways***
- Base DMZ under AF C2 to protect individual base
- Individual system protection under AF C2 to protect against insider threat

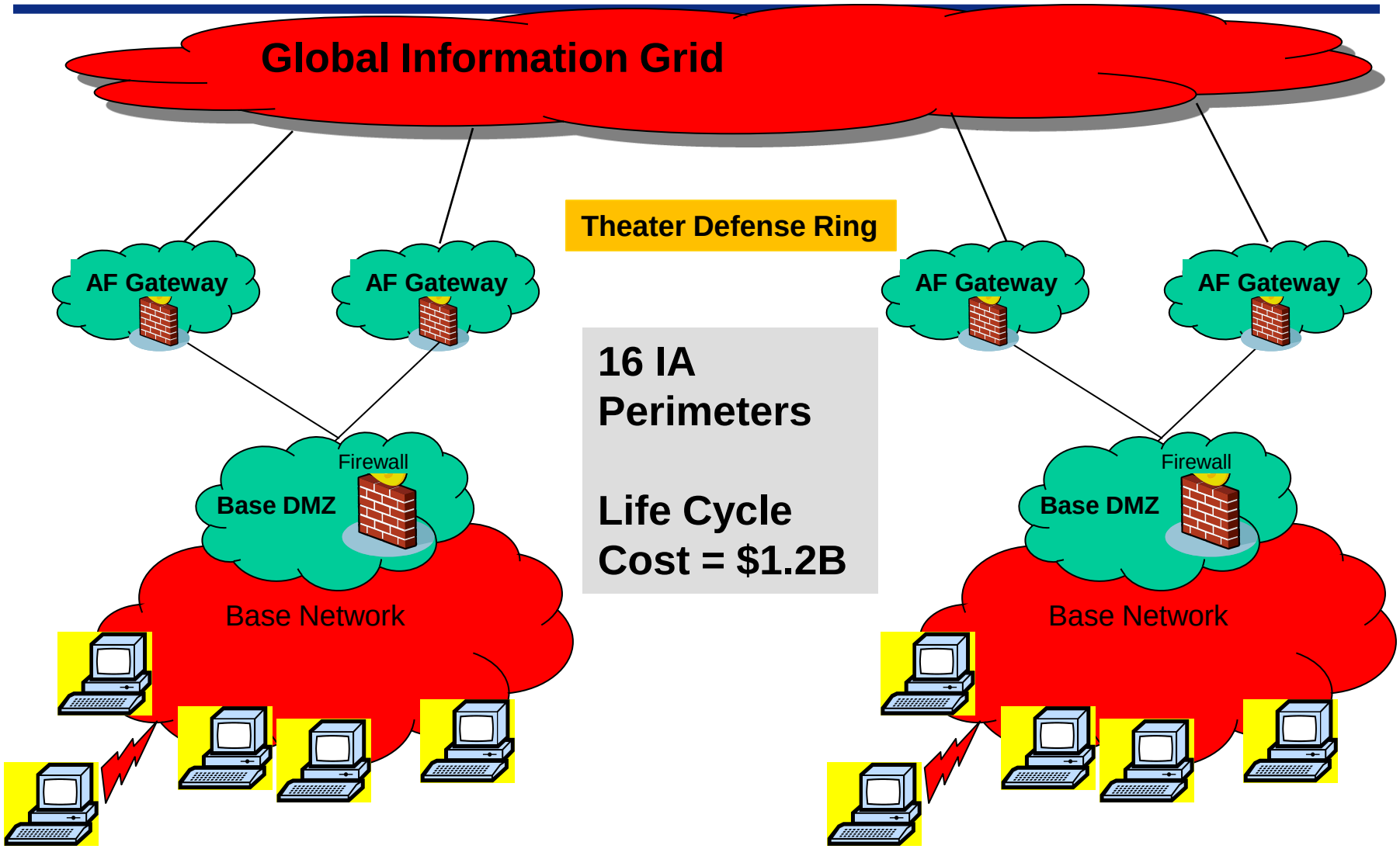
**Attacks can be initiated from outside or inside the network**

# Backbone of the AF Mission: AF Intranet (AFNet)



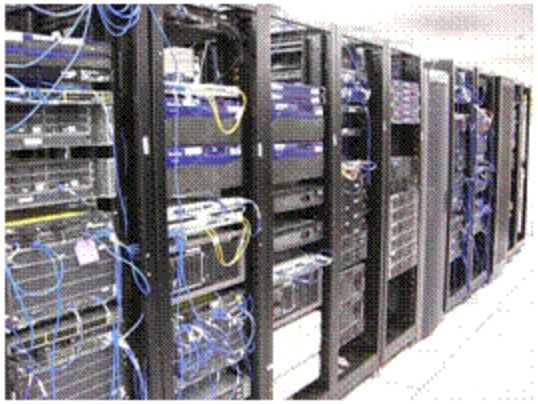

850,000+ users
1.4M endpoints
400+ datacenters
Unclassified & Classified networks

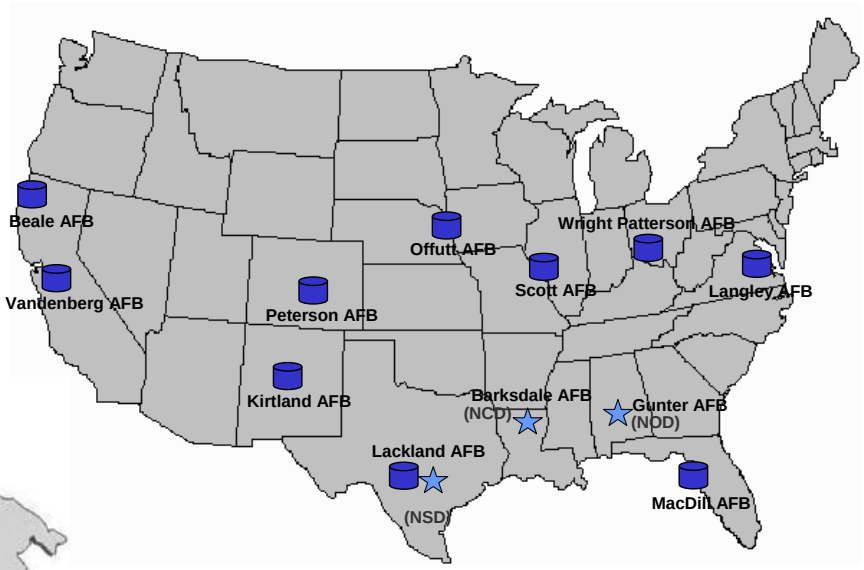
# AFNet Increment 1 (Block 30 Spiral 1)

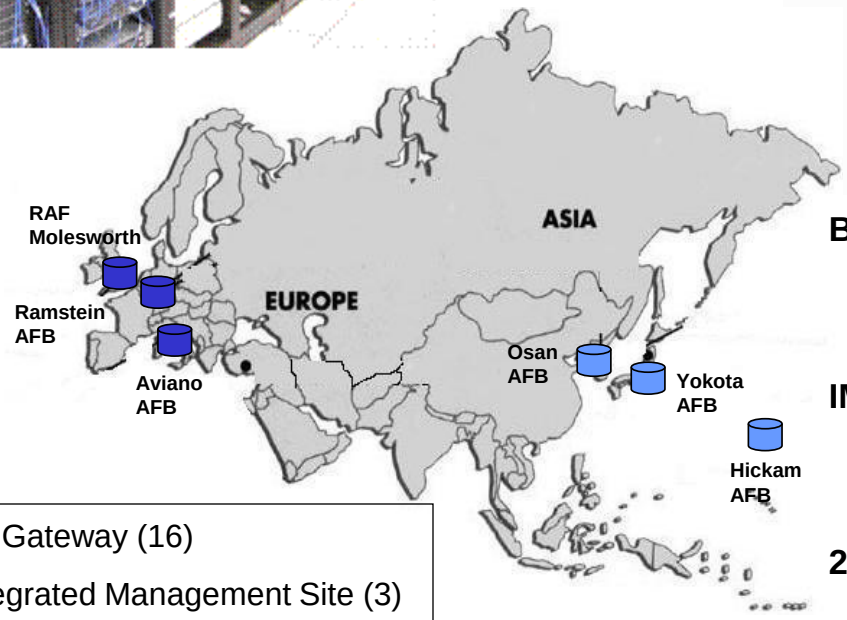


# 16 AFNet Gateway Locations

## Net Defense for AF Intranet






AF Gateway (16)

Integrated Management Site (3)

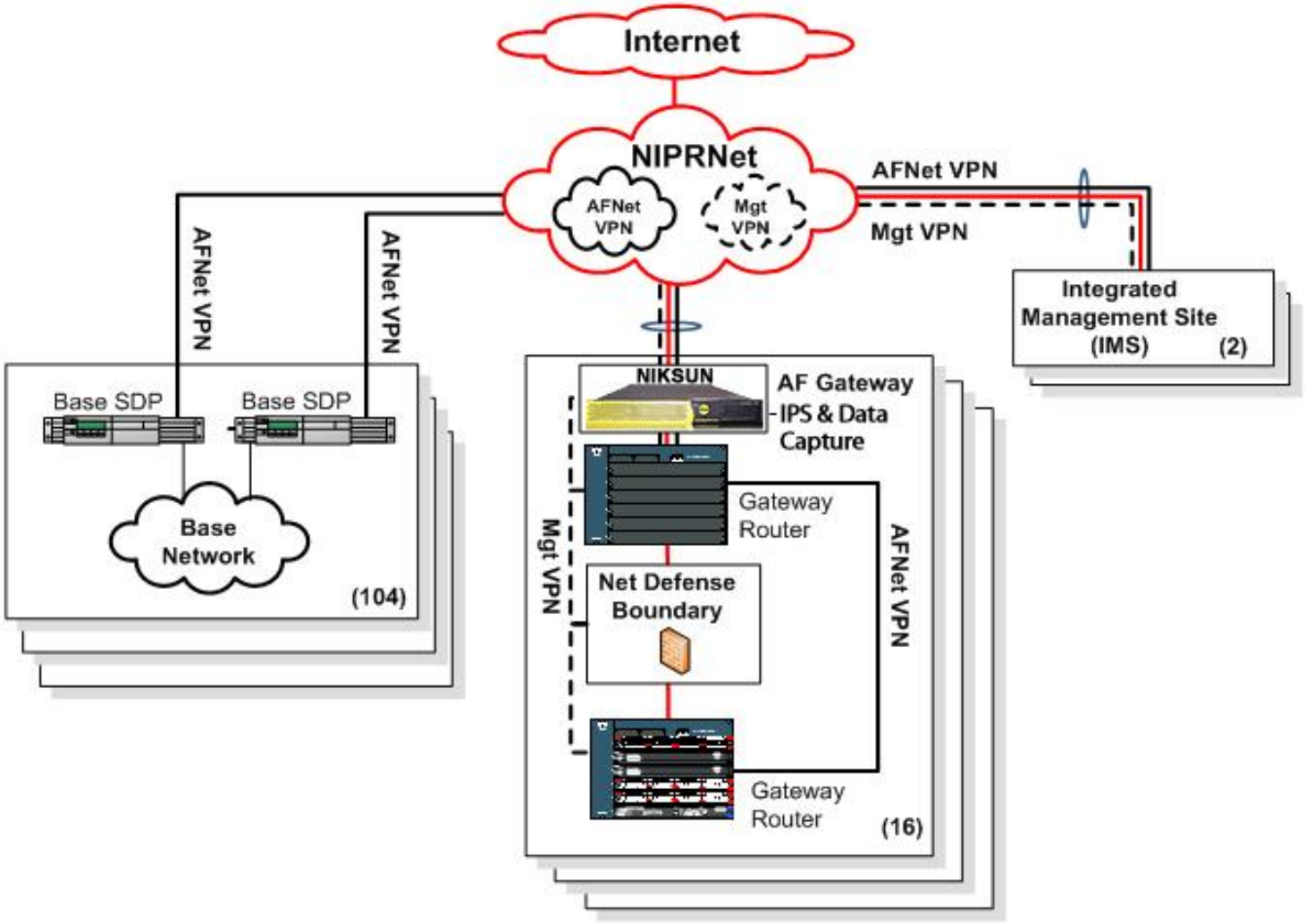
+89 AF Bases

**Bases assigned a primary and secondary Gateway**
- All traffic entering/leaving AF traverse a Gateway
- Automatic failover to secondary

**IMS provide central AF Net Management**
- Security Management
- Fault Management
- Performance Management

**2 IMS**
- Network Operations Division and Network Security Division IMS COOP each other

# AFNet Gateway Architecture



U.S. AIR FORCE

# AFNet Gateway Status

- All 16 Gateways fully operational
- All AF and ANG base traffic through a Gateway

- DoD Operational Test and Evaluation rated the system – “Operationally Suitable and Effective”

- AF ecstatic! Gateways have cut out “noise” and let operators focus on the real threat

- Gateways undergoing extensive modernization
  - Unexpected Web 2.0 impacts on design
  - Long acquisition/deployment timelines vs. IT life cycle

U.S. AIR FORCE

# Future AF Trends
# The 4 "C"s

- **C**ommoditized infrastructure through competition and enterprise buys
- **C**onverged hardware and software services
- **C**onsolidated data centers
- Private **C**louds (Infrastructure, Platform as a Service)

U.S. AIR FORCE

# Way Ahead

- Budget pressures will drive –
  - Incremental capability growth via modernization of fielded systems
  - Solutions higher up “the stack”
- Will require increased partnering with industry
  - Early and often
  - Influence requirements (where the AF sets the bar for competition)
  - “**Operationalize**” fielded systems (squeeze the rock)

U.S. AIR FORCE

# Questions?