SAND2011-1421C

The NNSA Enterprise Secure Network: Supporting the NNSA One Network Vision

Presented to DOE IM Conference
March 23, 2011

C. Douglas Brown
Senior Engineer, SNL

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

Overview

- Describe the current state of ESN
  - Services provided
  - Applications supported
- Discuss planned enhancements to ESN core services
  - Releases 8, 9, 10
  - New sites
  - Gateways to other networks

What is ESN?

- Enterprise Secure Network (ESN) is a project sponsored by NNSA to facilitate the secure exchange of classified information and capabilities across the Nuclear Security Enterprise. It operates at the S/RD level.
- ESN consists of independent site installations of standardized equipment and COTS software that are integrated through a common infrastructure and shared policies and procedures.
- ESN features an Enterprise-level identity model, strong (two-factor) authentication, and a centralized monitoring and analysis capability.
- ESN is currently deployed at all NNSA and multiple DOE sites, other Departments and organizations, and select allied nations. There are additional sites being integrated, and limited-access gateways under development and construction.

ESN Mission Statement and Vision

ESN Mission:

Develop and maintain a classified communication and computing environment to support secure and efficient information exchange across NNSA, DOE, other Departments and organizations, and select allied nations.

ESN Strategic Vision:

A fully integrated and seamless secure information and services sharing environment supporting the Department of Energy mission and NNSA Complex Transformation.

Twice honored for "Outstanding Information Technology Achievement in Government" in annual GCN competition.

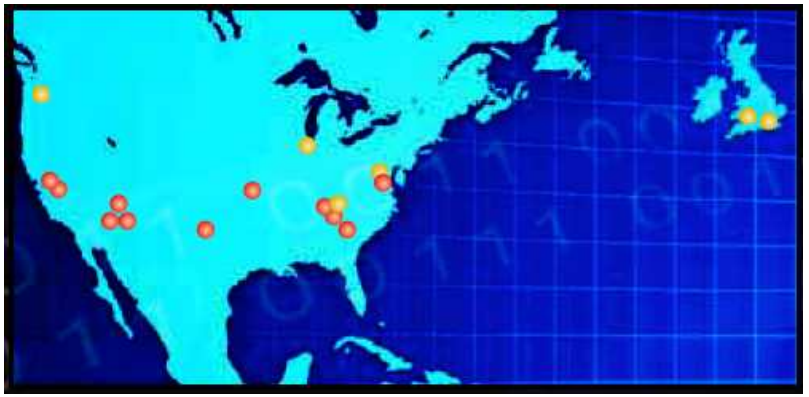
ESN Provides Core Cyber Security Services

- Cross-complex Application and Data Access
- 2-factor Cross-complex Authentication
- Enterprise Identity Management Services
- Access Management Services
- White Pages Directory
- Centralized Intrusion Detection and Monitoring
- 24/7/365 Helpdesk Support
- Basic File Sharing Services
- Centralized DNS, CA, and NTP services
- Application Registry

ESN Installations

Current Sites:

- Kansas City Plant (Kansas City, MO)
- Lawrence Livermore National Laboratory (Livermore, CA)
- Los Alamos National Laboratory (Los Alamos, NM)
- Nevada Site Office (Las Vegas, NV)
- NIARC (Las Vegas, NV)
- NNSA HQ (Washington, DC)
- Office of Scientific and Technical Information
- Pantex Plant (Amarillo, TX)
- Sandia National Laboratories
  (Albuquerque, NM and Livermore, CA)
- Savannah River Site (Aiken, SC)
- Service Center (Albuquerque, NM)
- Y-12 National Security Complex (Oak Ridge, TN)
- Pacific Northwest National Laboratory (DOE) (Richland, WA)
- Oak Ridge National Laboratory (DOE) (Oak Ridge, TN)
- Office of Science and Technology Policy (White House)
- UK Atomic Weapons Establishment

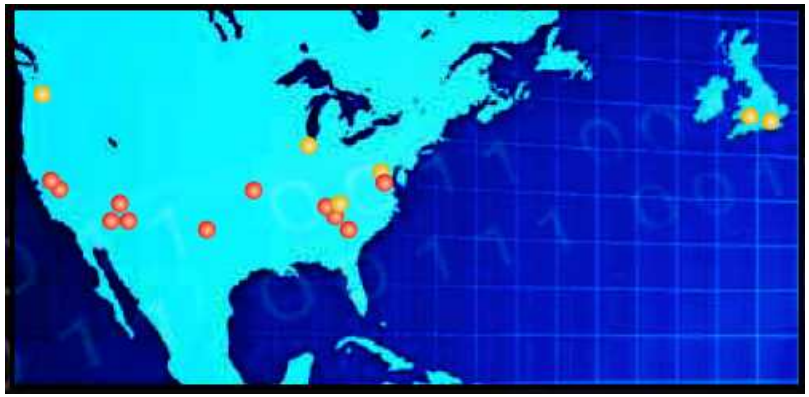


Extending our services to DOE and beyond….

ESN Installations

In-Process Sites and Gateways:

- United Kingdom Gateway – Phase I & II
- UK Ministry of Defense
- SIPRNet Gateway – Phase I & II
- Local Site Offices
- Atomic Weapons Group, USAF



Extending our services to DOE and beyond….

Applications are being deployed on ESN

- Many applications have been deployed to date
  - Spares, Order Mgmt., SDDB, DOORS, TeamCenter, Wiki, WebConf, QERTS, PhoneBook, App Registry, Basic File Sharing, Nagios, SWEURS, SFI, IPSS, PCD, WIS, APS File Viewer, APS Data Editor, APS Logging, Castle-WR, ECM
- More applications are scheduled for FY11
  - PRIDE Portal, SDDM, ROA, eCIS, Rhythm, FKB, Sniper, Library, PDMLink (5 sites), Castle-PX

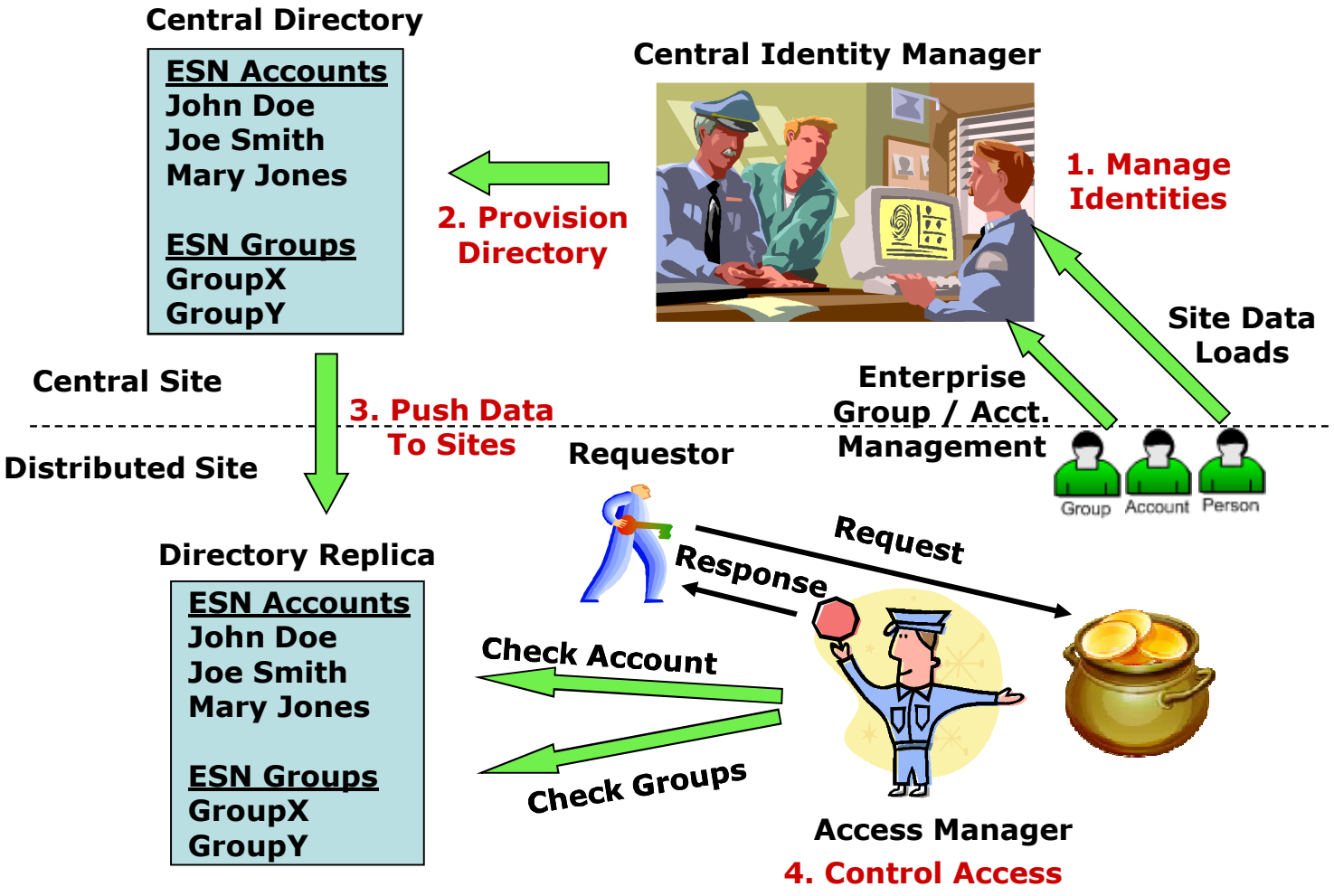
ESN is designed for high availability

- User-visible services are implemented with redundancy
- Automatic failover from primary to secondary servers
- Federated design ensures that intra-site access is available if inter-site network goes down
- Average site uptime for January was 99.77% (Nine sites were at 100%)

ESN Release 8 is scheduled for FY11

- Central Identity Manager and Directory
  - Reduces cost and complexity
- Read-only directory replicas at the sites
  - Maintains site independence in the event of a network outage
- Update software to the latest versions
  - Directory, Access Manager, Identity Manager
  - Improve vendor support
- Integrated ESN DNS Service
- Added functionality
  - Web Services, Improved integration w/apps

Release 8 Centralizes Identity Management



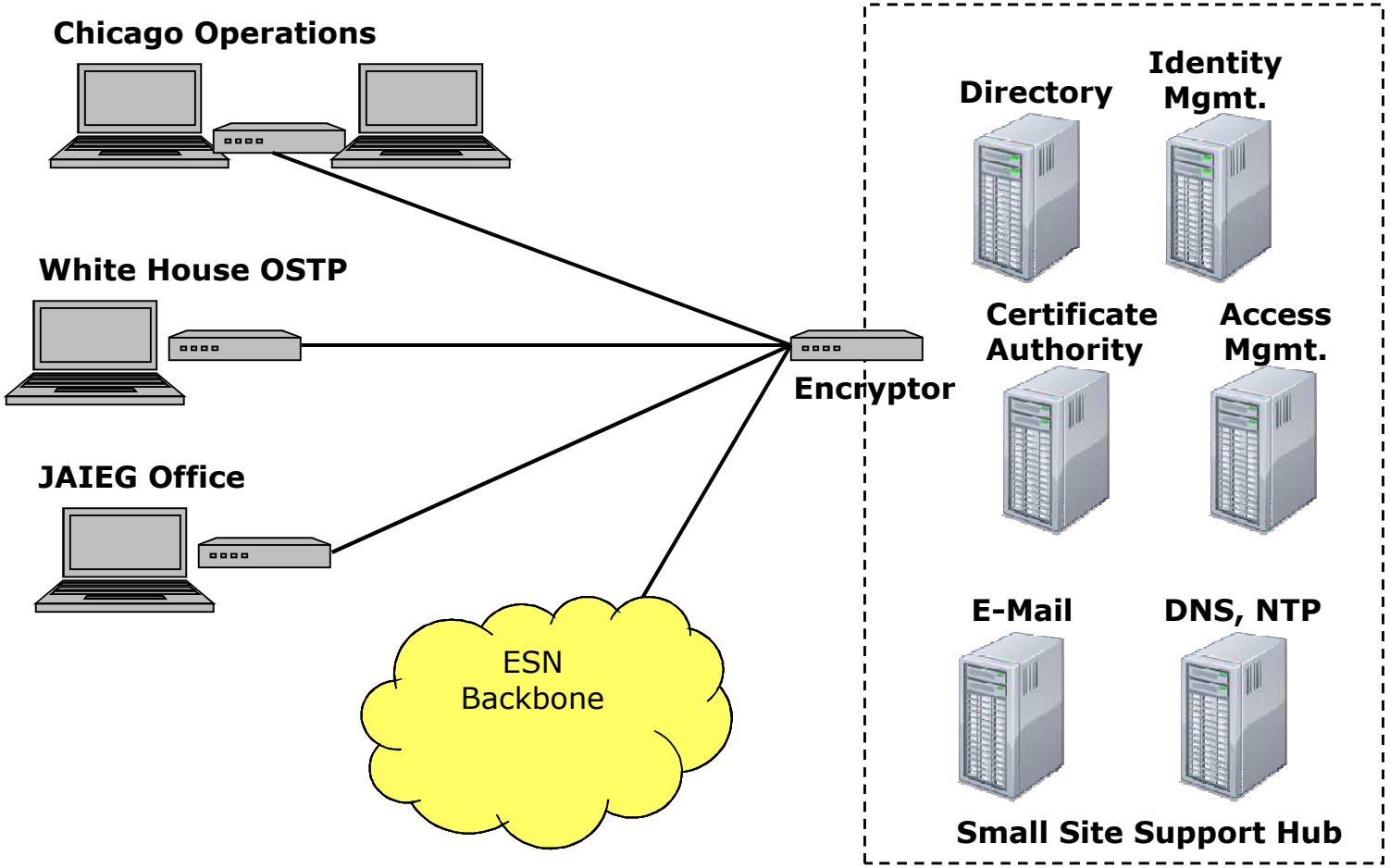
ESN has multiple connectivity options

- **ESN Standard**: Full deployment, featuring redundancy for all critical components.
- **ESN Lite:** Full functionality but without redundancy (for sites with light usage, and few hosted applications).
- **ESN Very Lite:** Connection only (for sites with their own services and no need for ESN cross-site authentication and authorization).
- **ESN Small Site:** Site administration and account management hosted at a small site hub that provides classified email and file services.
- **ESN Gateways:** Controlled-access gateways interface to cooperating agencies.

ESN Small Site Hub

- Provides infrastructure services for small sites where it is not cost-effective to operate their own installation
  - Identity Management
  - Authentication
  - E-mail and file services
- Customers of the Small Site Hub
  - NNSA JAIEG Office (2010)
  - White House Office of Science and Technical Policy (2010)
  - NNSA Site Offices (2011)
  - Atomic Weapons Group, USAF (2011)
  - Chicago Operations Office (2011)

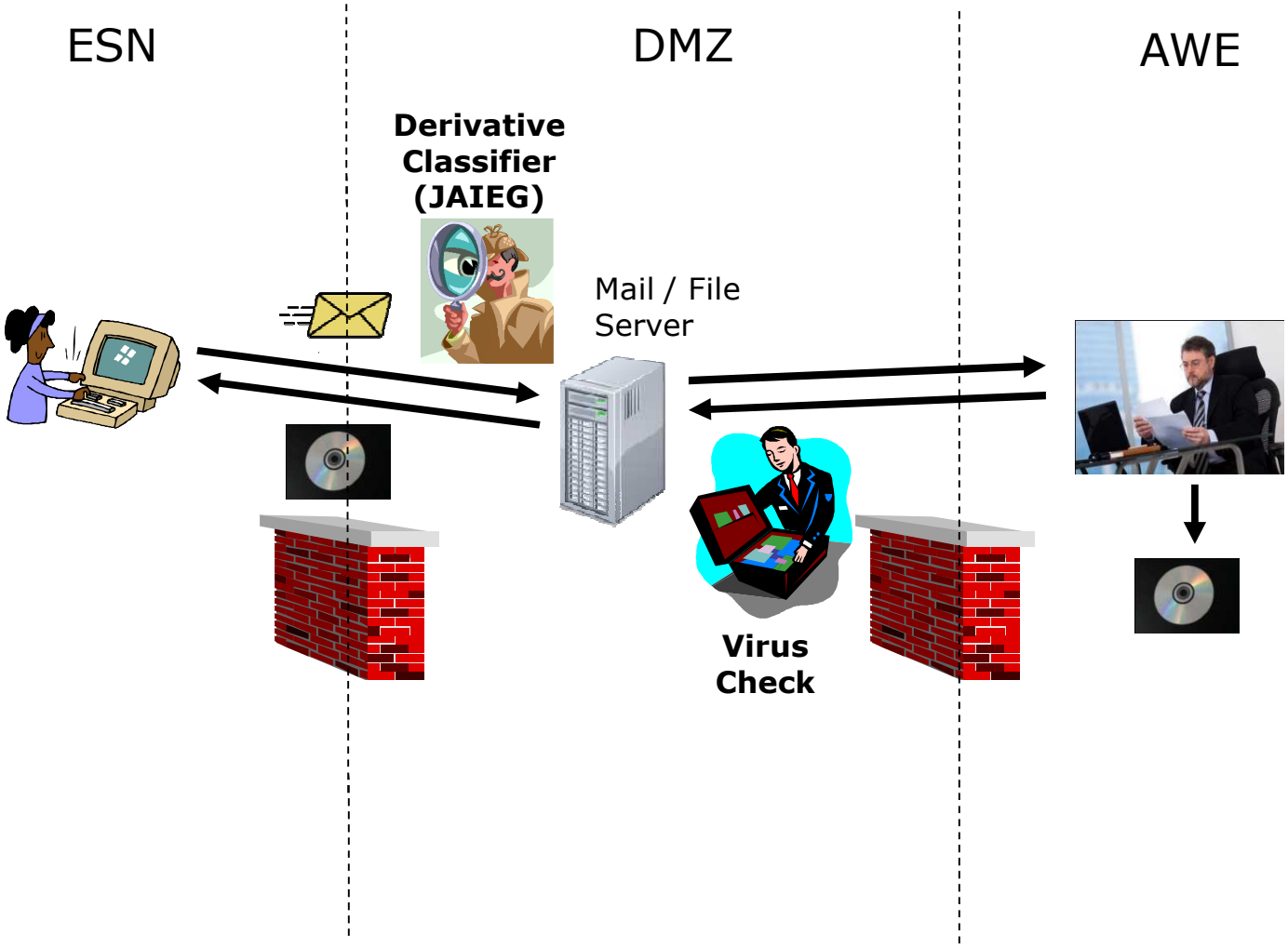
Small Site Hub Design



The ESN UK Gateway is operational

- High-level agreement reached between DOE and Atomic Weapons Establishment (AWE)
- Deploying ESN workstations at
  - UK Embassy (2010)
  - Aldermaston (AWE) (2010)
  - NNSA JAIEG Office (2010)
  - VTC at AWE and MOD (2011)
- No direct connection to UK networks
  - Data moved to/from UK systems via media
- UK Gateway ensures Derivative Classifier review of files going to AWE (S/RD)
  - UK users cannot access ESN sites
  - Can only pull DC reviewed files from Gateway
  - VTC capability under consideration

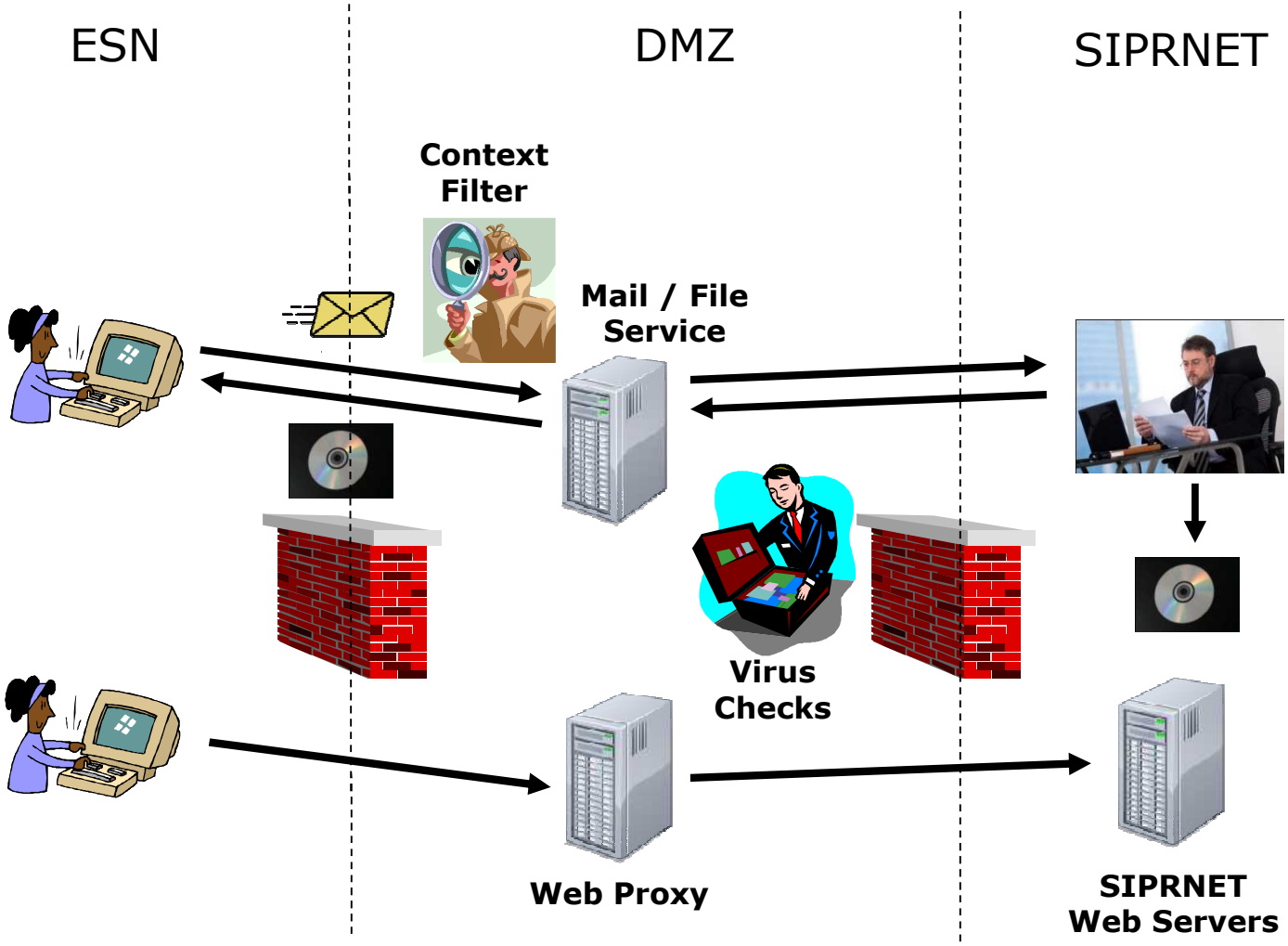
UK Gateway Functionality



Gateway to DoD SIPRNet is coming in FY11

- Provides the following services:
  - Email
  - File transfer
  - Web browsing
  - Tools developed to assist in classification review
- ESN SIPRNET Gateway is accredited by NNSA
- Defense IA/Security Accreditation Working Group (DSAWG) has given Approval to Connect (for testing)
  - Flag panel delegated final approval to DSAWG
- Final approval expected in May 2011

SIPRNET Gateway Functionality



Enhancing Future Collaborations

- Deploy & enhance SIPRNet, UK Gateways
- Deploy Small Site Hub infrastructure
- Expand ESN presence to other interested sites
- Integrate Kerberos authentication (Release 9)
- Transition from Sun to Oracle product (Release 10)
- Enhance file sharing capabilities
- Explore one-way (low to high) data transfer capabilities
- Explore cross-site classified VoIP capabilities
- Explore enhanced VTC capabilities
- Additional cooperative services to support user requirements

Summary

- The ESN is a production classified S/RD network supporting 20 sites
  - Provides strong security features
  - Many applications are being deployed
- Enhancements are being implemented
  - Release 8 is introducing central identity management and hardware/software upgrades
  - New sites are being added
  - Gateways being implemented to DoD and UK
- Other enhancements are being considered