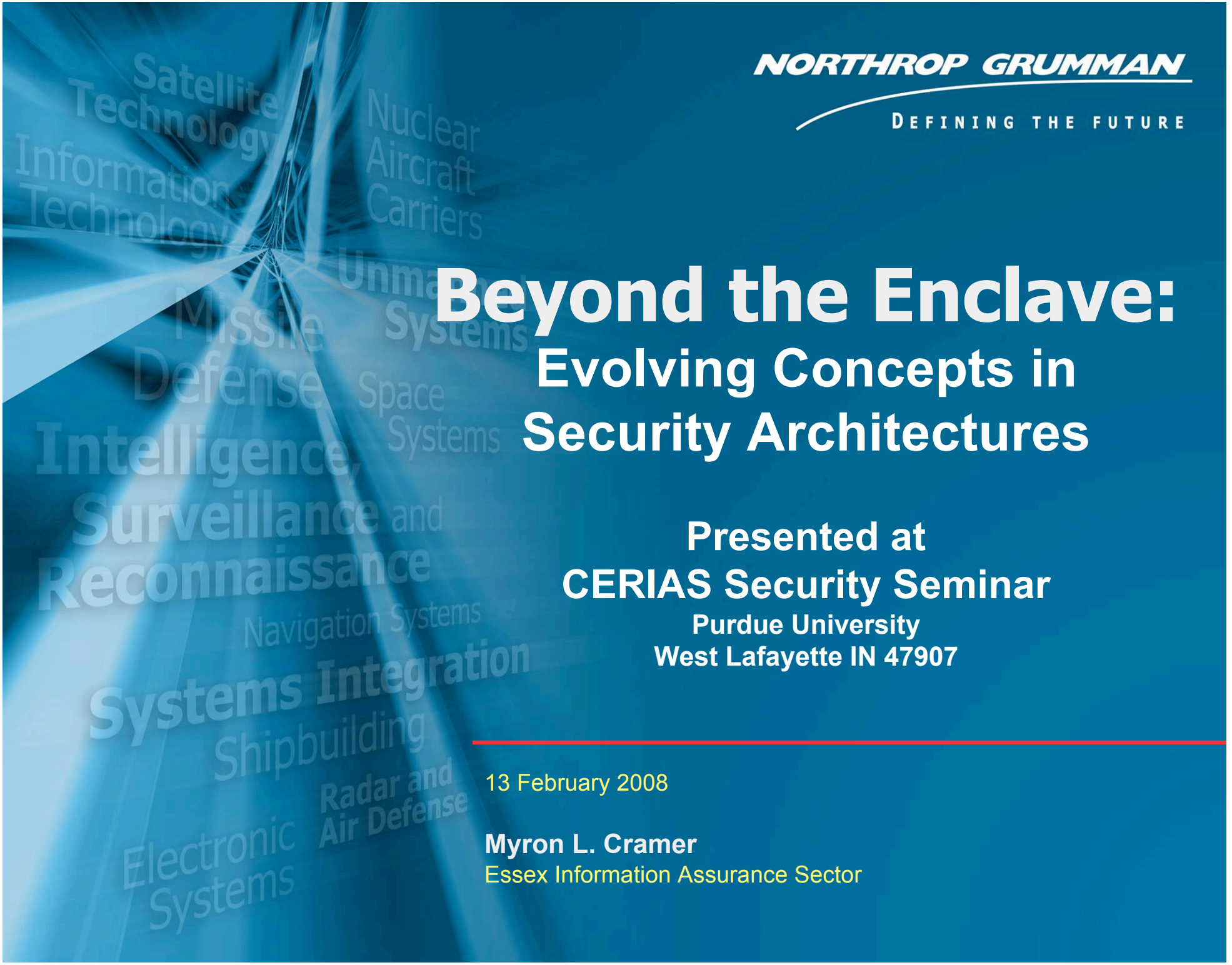


NORTHROP GRUMMAN

DEFINING THE FUTURE

Beyond the Enclave:
Evolving Concepts in Security Architectures

Presented at
CERIAS Security Seminar
Purdue University
West Lafayette IN 47907

13 February 2008

Myron L. Cramer
Essex Information Assurance Sector

Overview

- **Problem**
  - Conventional Enclave architecture does not easily support collaborative information sharing, web services, or other needs
- **Solution**
  - Apply architectural concepts and models
  - Apply new information technologies
  - Develop New security solutions
- **Assumptions**
  - Cross-domain information sharing requirement
  - Web services information infrastructure

NORTHROP GRUMMAN

Topics

- Problem
- Security Architectures and Engineering
- Enclave Architecture Model
- Implementing the Enclave
- Cross-Domain Problem
- Cross-Domain Architectural Concepts
- Web Services
- Solution Technologies

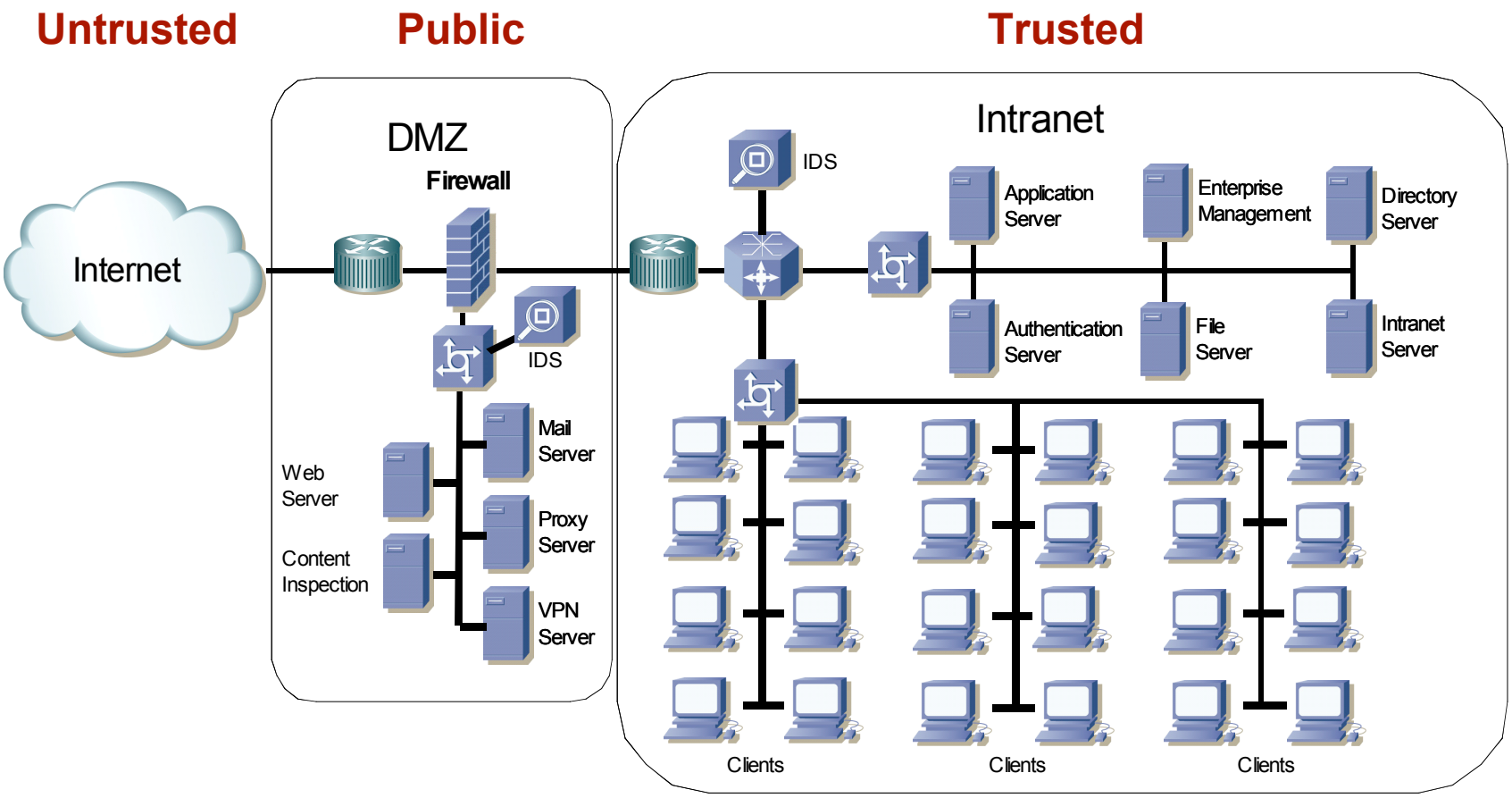
NORTHROP GRUMMAN

Problem

- **Traditional**
  - How to secure information systems
  - How to control access
  - Implementing a “need to know” policy
- **New Challenges**
  - How to satisfy increasing needs for collaboration across an insecure internet
  - How to secure distributed applications
  - Implementing a “need to share” policy

NORTHROP GRUMMAN

Enclave Architecture



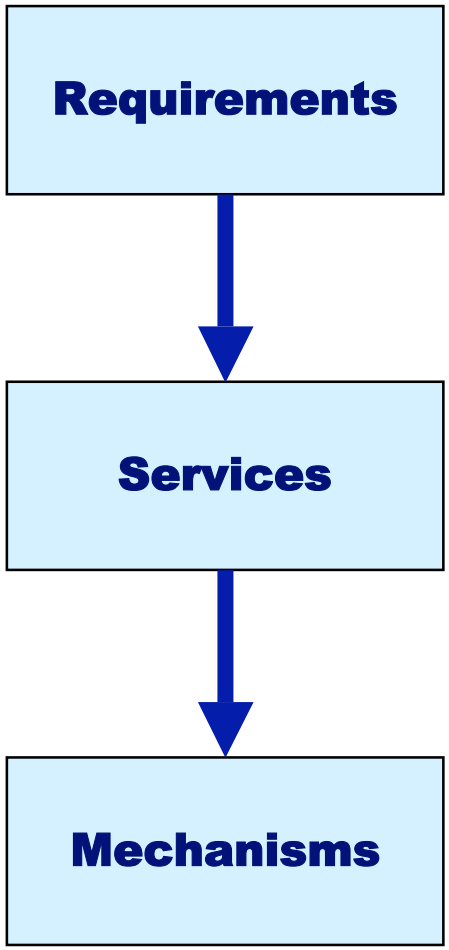
The enclave architecture is the gold standard for security architectures.

Security Concept

- **Security Architecture and Engineering**
  - Information security requirements are translated and implemented through a security architecture and design
  - Designs utilize products including firewalls, intrusion detection systems, virtual private networks, and public key infrastructures
- **Solution Integration**
  - Selection and integration of products, people, and processes to implement the security design
  - Solution uses products within their capabilities to provide “defense –in depth”
- **Operational Concept**
  - Integrated processes within the security architecture

NORTHROP GRUMMAN

Security Architecture & Engineering



- **Policy**
  - International, Federal, State Law and Regulations
  - Corporate Policies
  - Inter-organizational Agreements
- **Requirements Translation**
  - Operational Environment
  - Risk Exposures
  - User Communities
  - Information Administration
  - Security Specifications
- **Design**
  - Architectural Implementation
  - Product Performance Specification
  - Components Selection and Configurations

Includes both a process and a product

NORTHROP GRUMMAN

Security Requirements

- **Confidentiality**
  - Assurance that information is not disclosed to unauthorized entities or processes
- **Integrity**
  - Assurance that data or processes have not been altered or corrupted by unauthorized entities or by chance
- **Availability**
  - Assurance that authorized users will have timely, reliable access to data and information services

NORTHROP GRUMMAN

Confidentiality Requirements

- **Access Control**
  - Discretionary Access Control (DAC)
  - Mandatory Access Control (MAC)
- **Account Management**
- **Audit**
- **Covert Channel Analysis**
- **Identification and Authentication (I&A)**
  - User accounts
  - Passwords
  - Strong (resistance to replay)
- **Labeling**
- **Least Privilege Enforcement**
- **Marking**
- **Parameter Transmission**
- **Recovery**
- **Resource Control**
- **Screen Lock**
- **Separation of Roles**
- **Session Control**
- **Storage**
- **Transmission Separation**

NORTHROP GRUMMAN

Integrity Requirements

- **Backup & Restoration**
- **Change Control**
- **Configuration Management**
- **Integrity Mechanisms**
  - Cyclic Redundancy Checks (CRC)
  - Integrity locks / encryption
  - Digital signatures
- **Malicious Code Protection**
- **Recovery**
- **System Integrity**
  - Security support structure
- **Transmission of Data**
- **Validation**
  - Security Support Structure
- **Verification**
  - Security procedures
  - Security mechanisms

NORTHROP GRUMMAN

Availability Requirements

- **Availability**
  - System restoration processes and procedures
- **Backup**
  - Systems and procedures for backup and restoration
  - Storage and recovery of access controls
- **Communications**
  - Adequate backup communications
- **Contingency planning**
  - Disaster recovery
- **Denial Of Service Prevention**
- **Maintenance**
  - Preventive
  - On call
  - On site
- **Monitoring**
  - Intrusion detection
- **Power**
  - Uninterruptible power supply
  - Alternate power
  - Graceful transfer
- **Priority protection**
- **Recovery**
  - Trusted & secure
- **Verification**

NORTHROP GRUMMAN

Non-Repudiation / Accountability

- Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data

- Validation of transactions for the services offered by the information system

NORTHROP GRUMMAN

Fundamental Principles

- Separation
- Least Privilege Enforcement
- Interdependency Analysis

NORTHROP GRUMMAN

Separation

- **Physical, Functional, & logical separation of users, services, and information**
- **Separation of roles**
  - System security officer and the system manager/administrator are performed by different people
- **Separation of data**
  - Information of different sensitivity levels is segregated from each other
  - Information is separated at rest and in transit

NORTHROP GRUMMAN

Least Privilege Enforcement

- The principle requiring that each user or process is granted the most restrictive set of privileges or accesses needed for the performance of authorized tasks
- A default “deny” policy, except where permission is justified

NORTHROP GRUMMAN

Interdependency Analysis

- **The principle that all functions and processes within an information system are interwoven and interrelated... an analysis of the security posture of a system must take into account these interdependent relationships.**

NORTHROP GRUMMAN

Implementing a Security Architecture

- **Integrating a Solution**
  - Firewalls
  - Intrusion Detection Systems
  - Vulnerability Scanners
  - Anti-Virus Systems
  - Virtual Private Networks (VPNs)
  - Authentication Systems
  - Cryptographic Applications

This involves the integration of products, people, and processes to implement the security design. An effective solution uses products within their capabilities to provide "defense in depth"

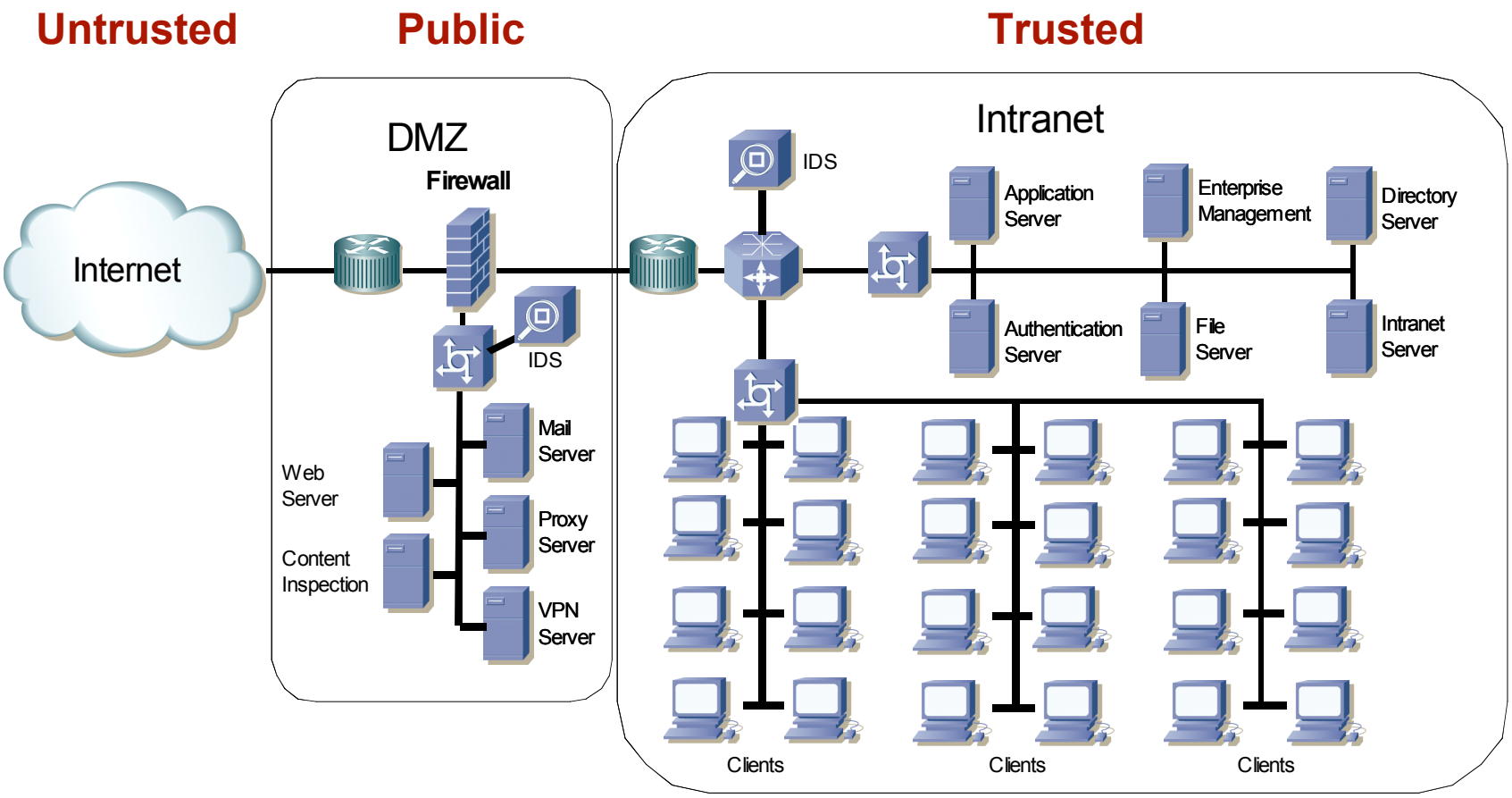
NORTHROP GRUMMAN

Organizing for Protection

Protect Enforces separation Applies Least Privilege Enforcement Principles	Anti-Virus Firewalls Proxy Server Intrusion Prevention Content Inspection Host access controls Application access controls Cryptographic applications
Measure Determines the condition of an information system	Network Mapping Vulnerability Assessment Intrusion Detection
Support Provides enabling and infrastructure services	Directory Service Incident Response Enterprise Management Security Infrastructure Management

NORTHROP GRUMMAN

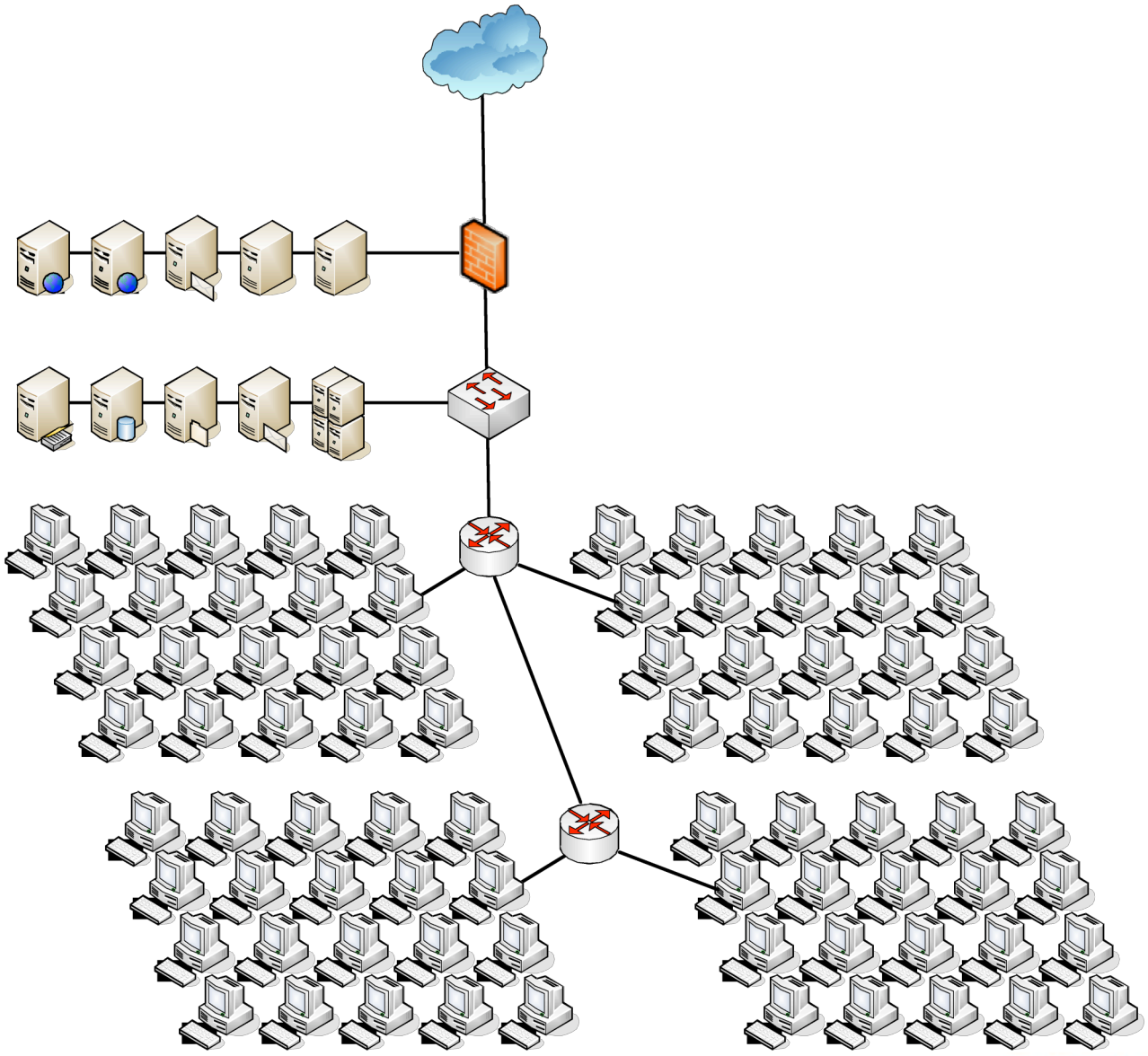
Enclave Architecture



The enclave architecture is the gold standard for security architectures.

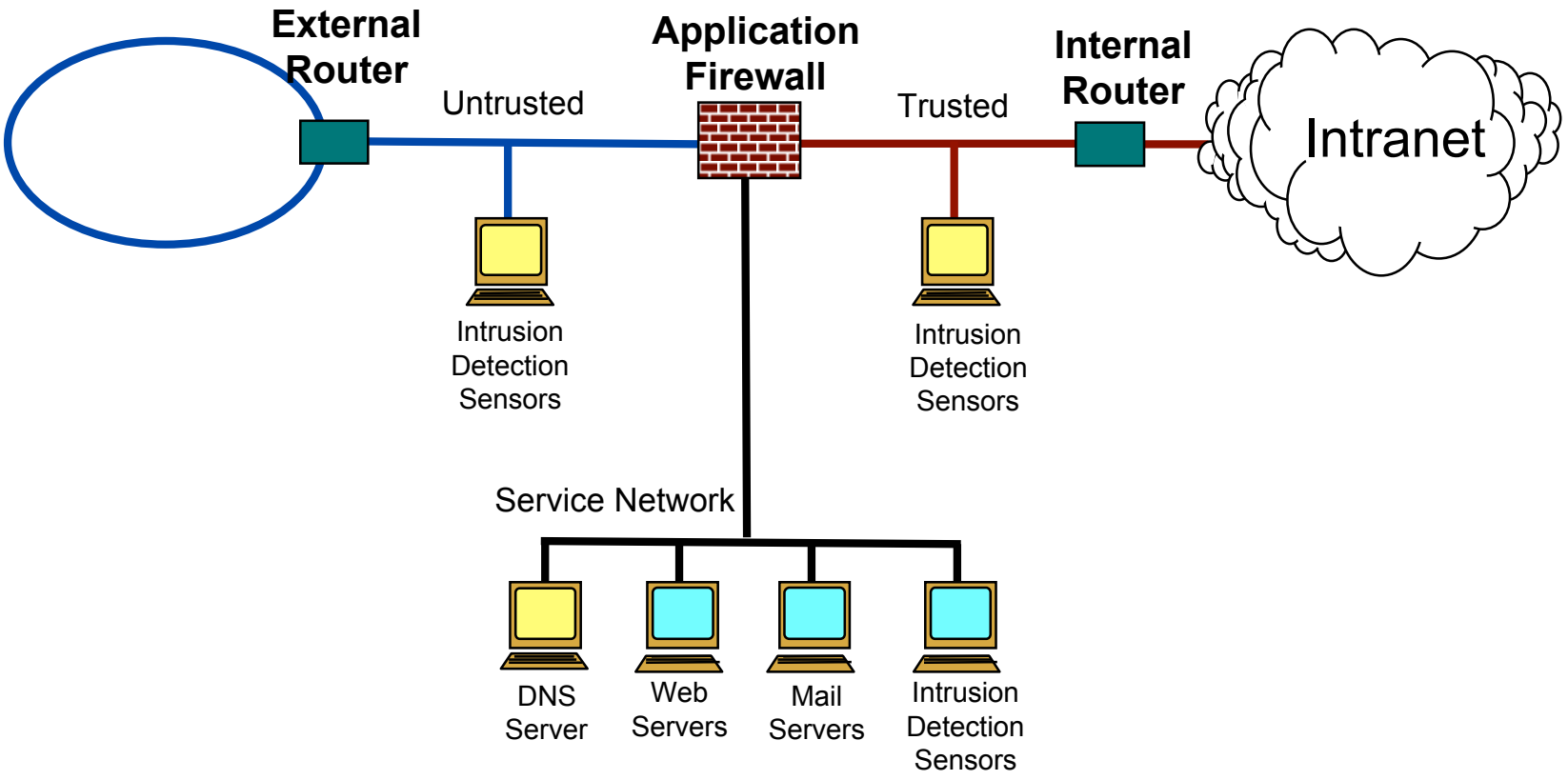
NORTHROP GRUMMAN

Enclave Enterprise Applications



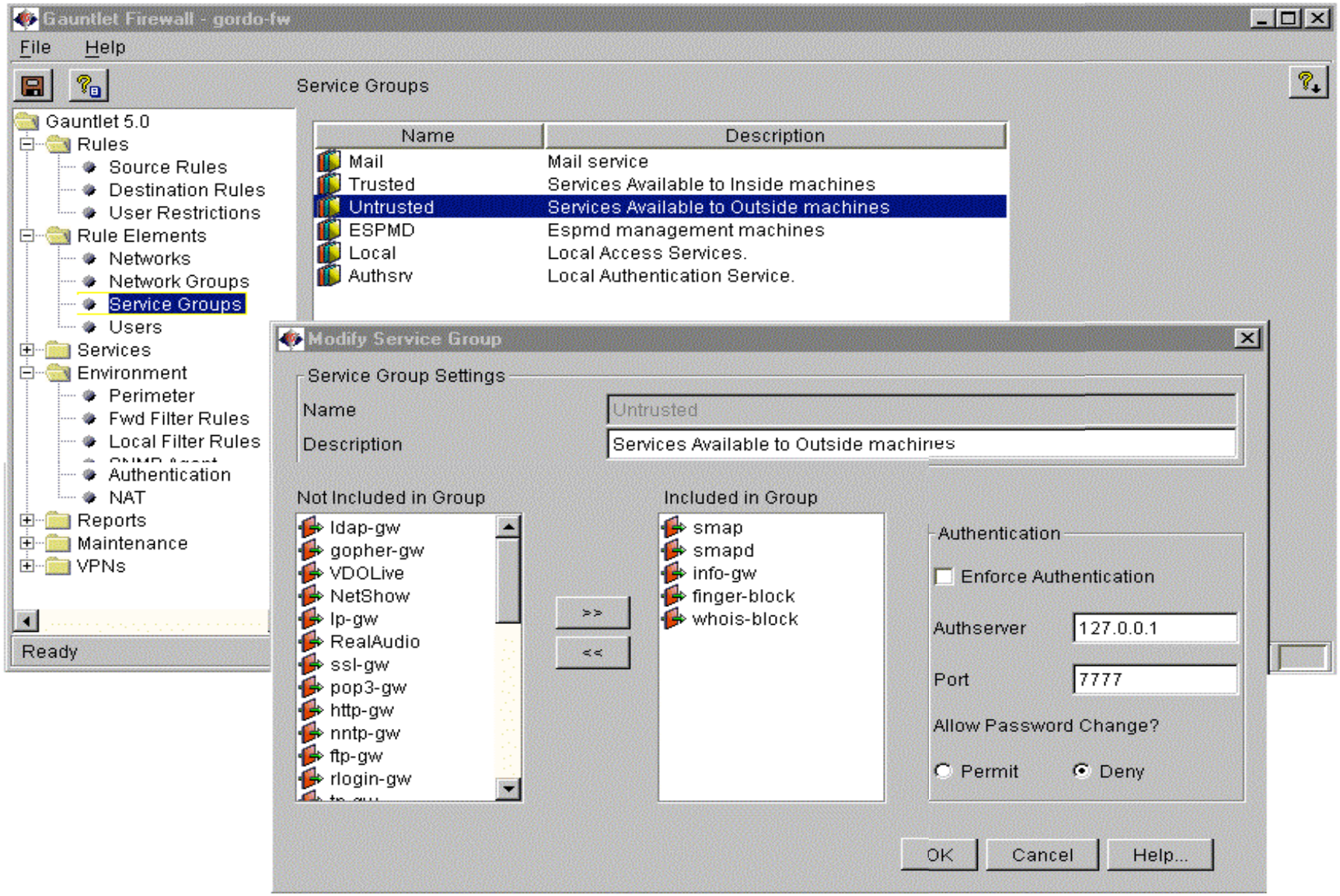
NORTHROP GRUMMAN

DMZ Design



NORTHROP GRUMMAN

Typical Firewall Filter Screen



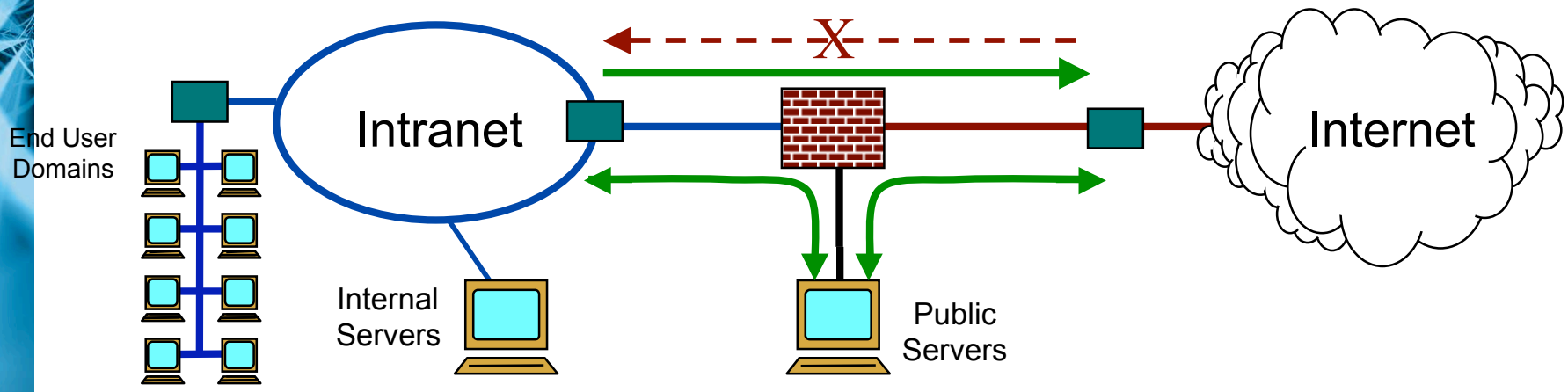
NORTHROP GRUMMAN

Application Firewall Capabilities

- Transparency: internal users have access to the internet through the firewall which proxies outgoing requests and manages sessions
- Proxy: firewall accepts incoming connections for the intranet, and proxies outgoing sessions; allowed services are proxied to the actual destinations
- Aliasing: firewall represents the entire public address space
- Separation: firewall separates the trusted internal network from the untrusted external network; service network separates public servers from internal hosts
- Security Policies: firewall enables security policies for incoming and outgoing connections on all interfaces
- Logging: firewall provides detailed logs of inter-network activity to support investigations and analyses
- Mail Exchange: firewall has the option of providing mail exchanger services for he protected domain; includes anti-spam, anti-relay, content inspection options
- Domain Name Service: firewall has the option of providing external DNS service for the domain

NORTHROP GRUMMAN

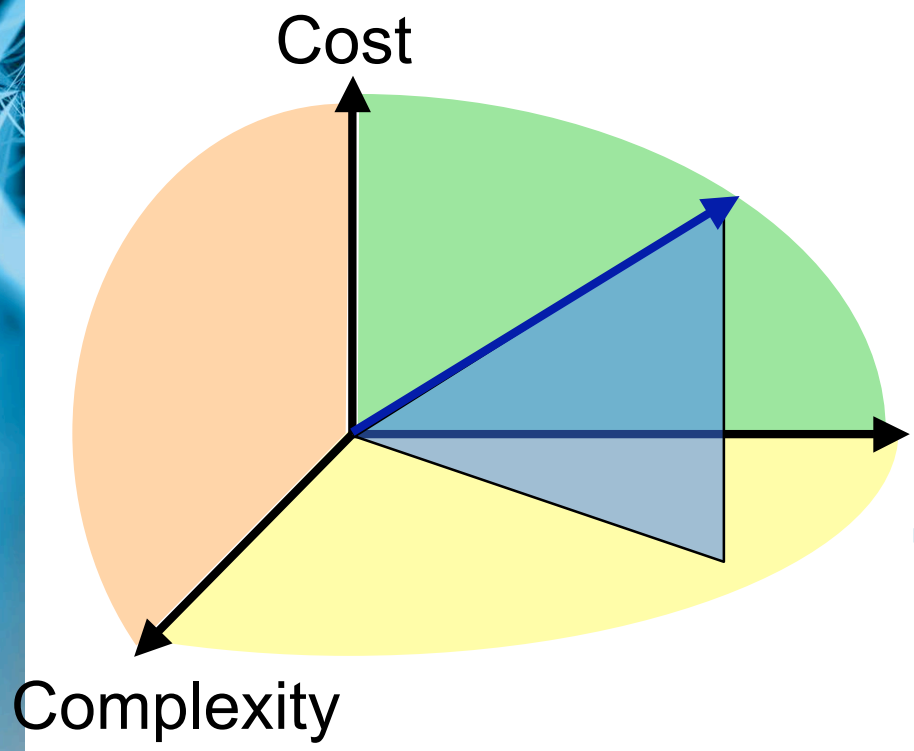
Security Policies



- **Firewall provides many networking options**
- **Example of policies:**
  - External to internal: generally not permitted except as allowed by plug-proxies or filters
  - Internal to External: unrestricted except as specifically blocked
  - Internal to Service Network: unrestricted
  - Service Network: permitted except as blocked

NORTHROP GRUMMAN

Solution Space



- **It is rare that assurance can be increased while decreasing cost and complexity, but it might be possible**
- **Most changes made to move up the assurance axis increase cost and complexity, then the change must be justified**

NORTHROP GRUMMAN

Mechanism Strength

- **Measured by "Work Factor" – the amount of effort required to break their security**
- **Best evaluated against objective technical criteria:**
  - Common Criteria - Evaluated Assurance Levels (EALs)
- **Experience of information security professionals**
- **Wrong ways to compare products strength:**
  - User surveys
  - Journalist's articles in magazines
  - Popularity

NORTHROP GRUMMAN

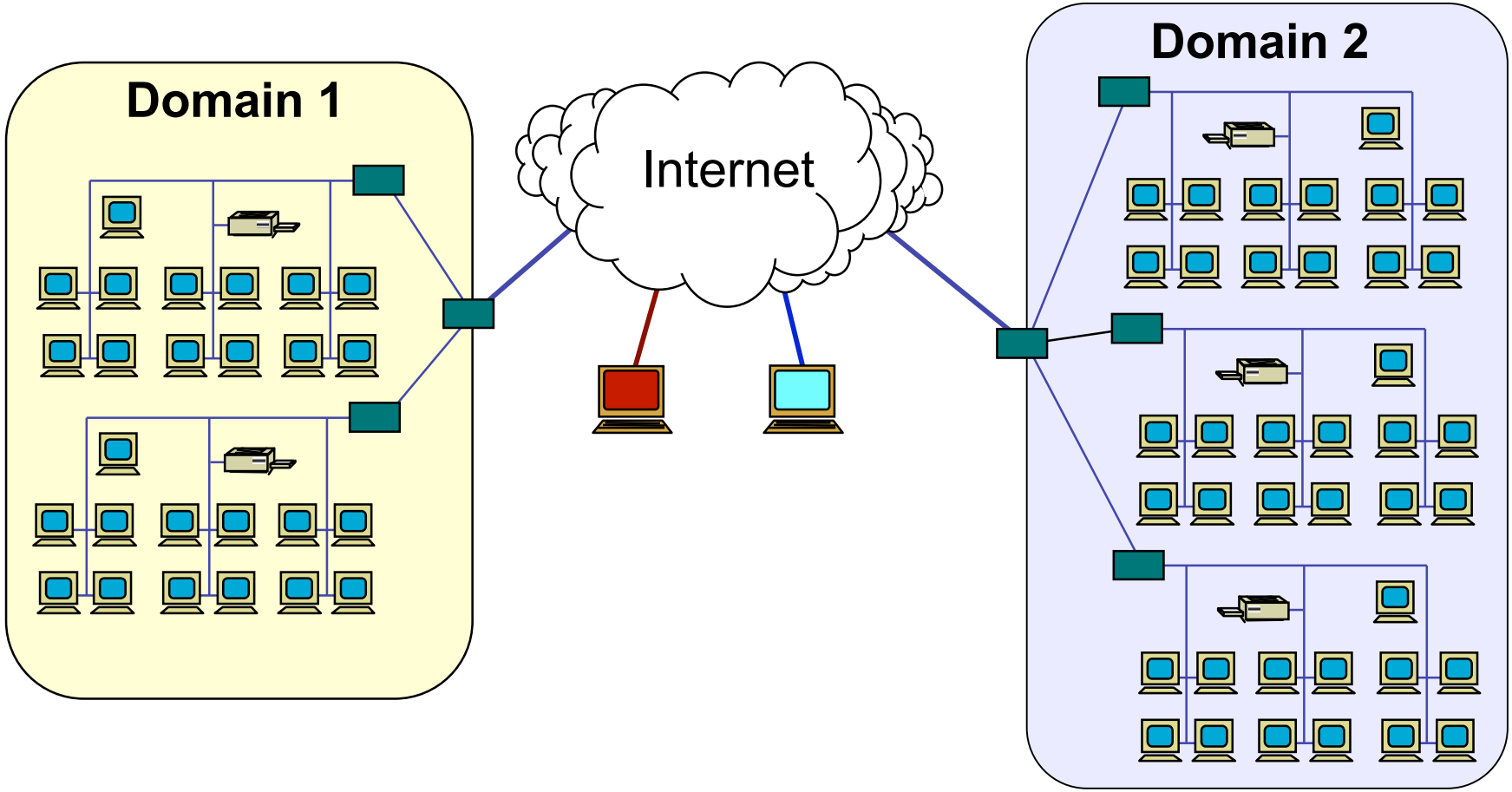
Cross-Domain Problem

- Collaboration across multiple organizations
- The “need to share” information outside of an organization’s domain
- The need to integrate applications across multiple organizations

NORTHROP GRUMMAN

Typical Problem

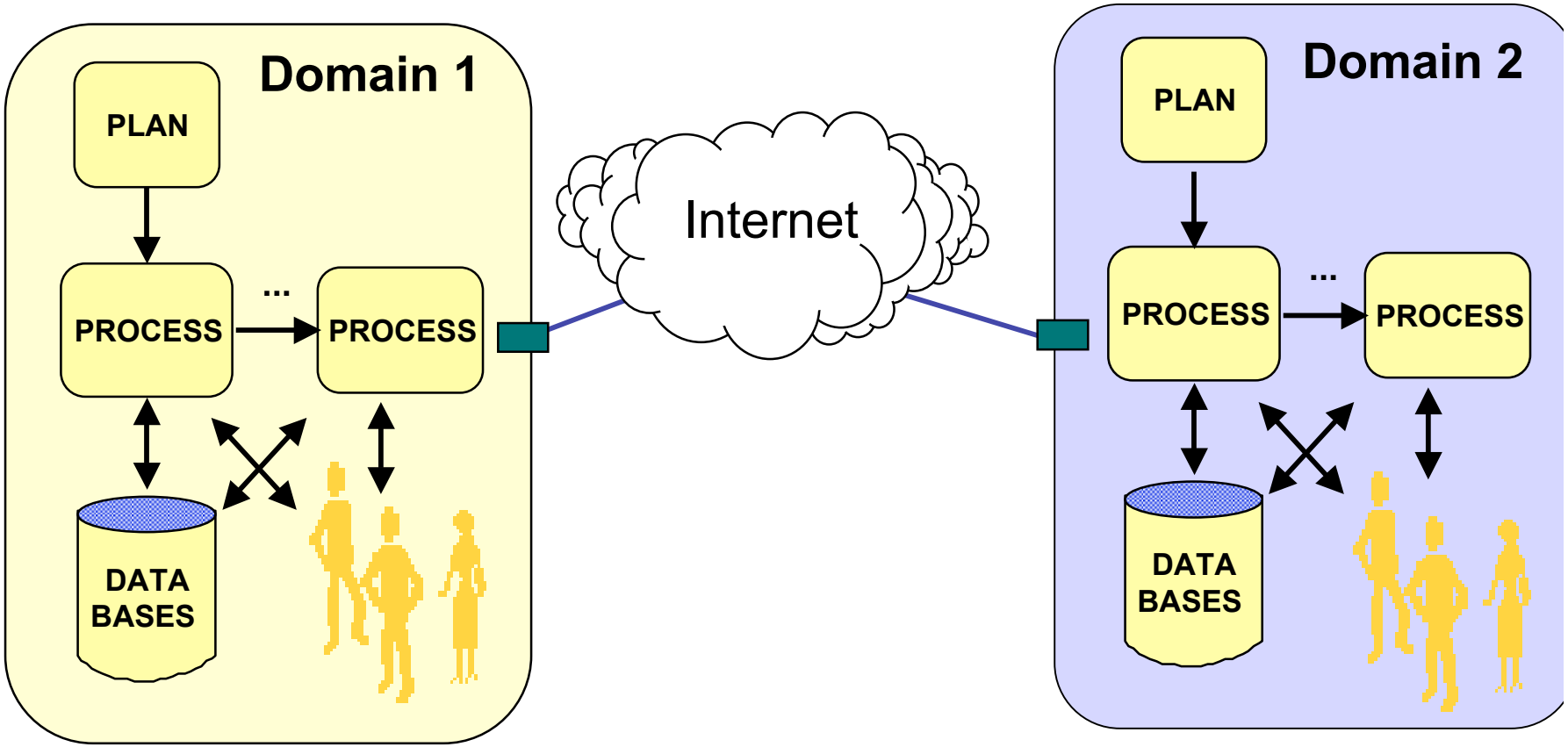
- Multiple Communities of Interest
- Need to share information and applications



NORTHROP GRUMMAN

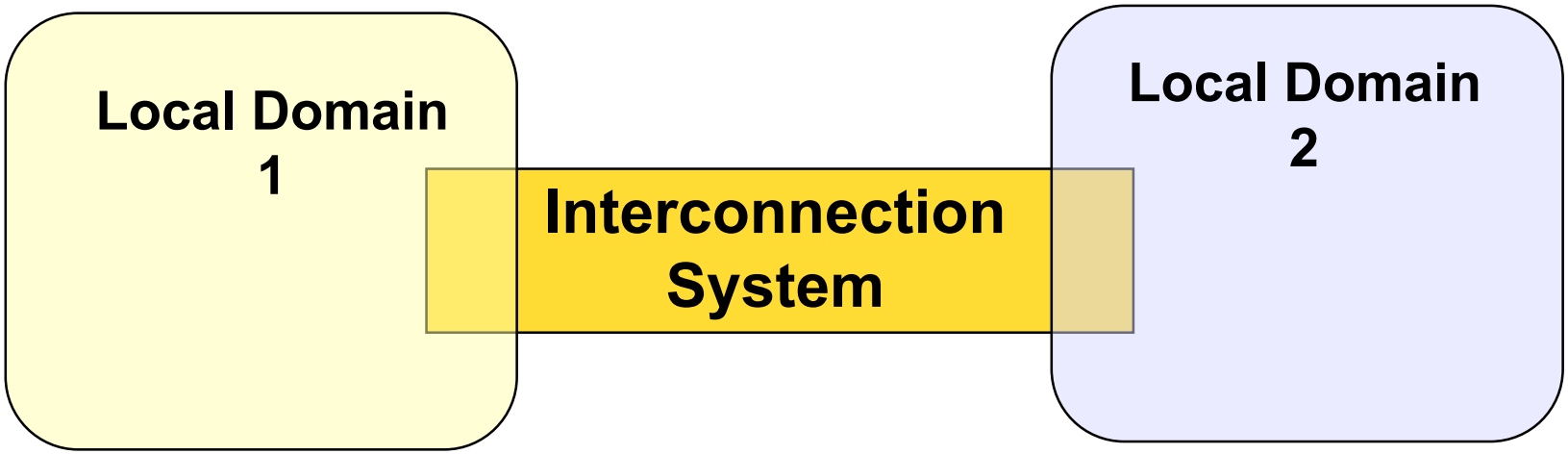
Information Domains

- Information, Processes, Information Technology, Users, connected by a common security policy
- Communities of Interest can span Domains



NORTHROP GRUMMAN

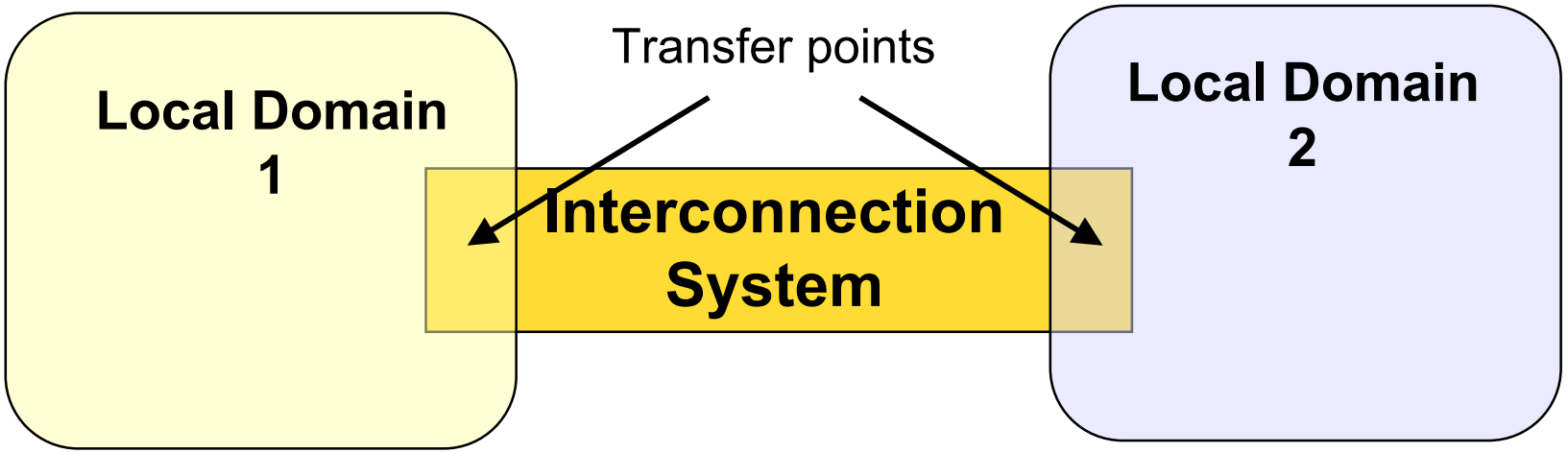
Domains



- Each Local Domain and the Interconnection system are separate jurisdictions
- Each Domain and the Interconnection system have their own Security Policies

NORTHROP GRUMMAN

Transfer Points

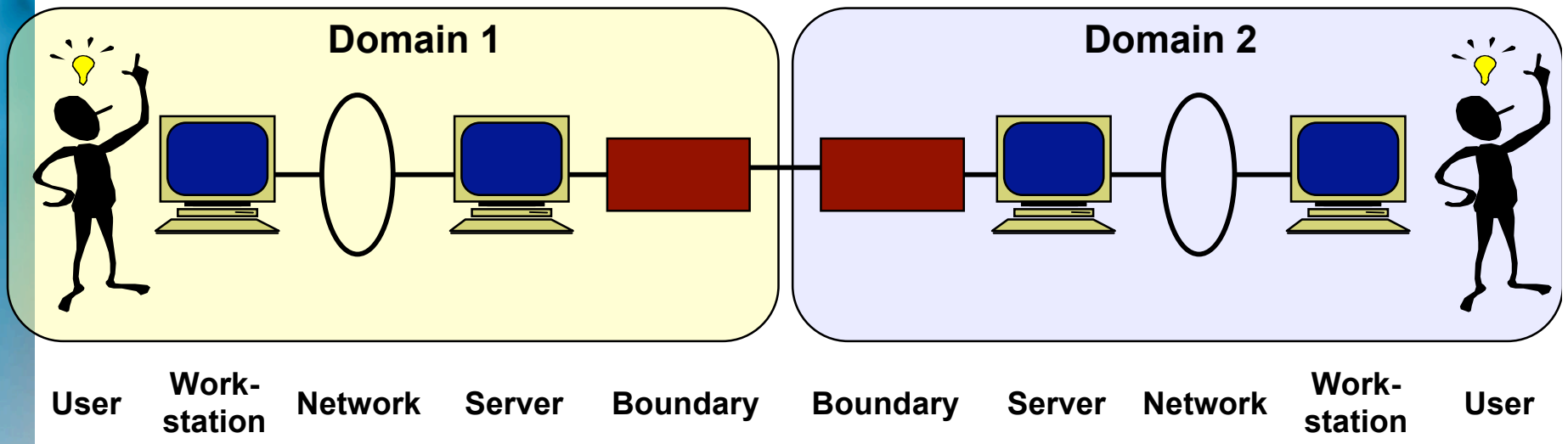


- Transfer Points must maintain requirements through the transfer process
- Security requirements (e.g., confidentiality) must be satisfied in each Domain and in the Interconnection system
- Transfer points are defined where security responsibility is transferred from the Local Domain to the Interconnection System

NORTHROP GRUMMAN

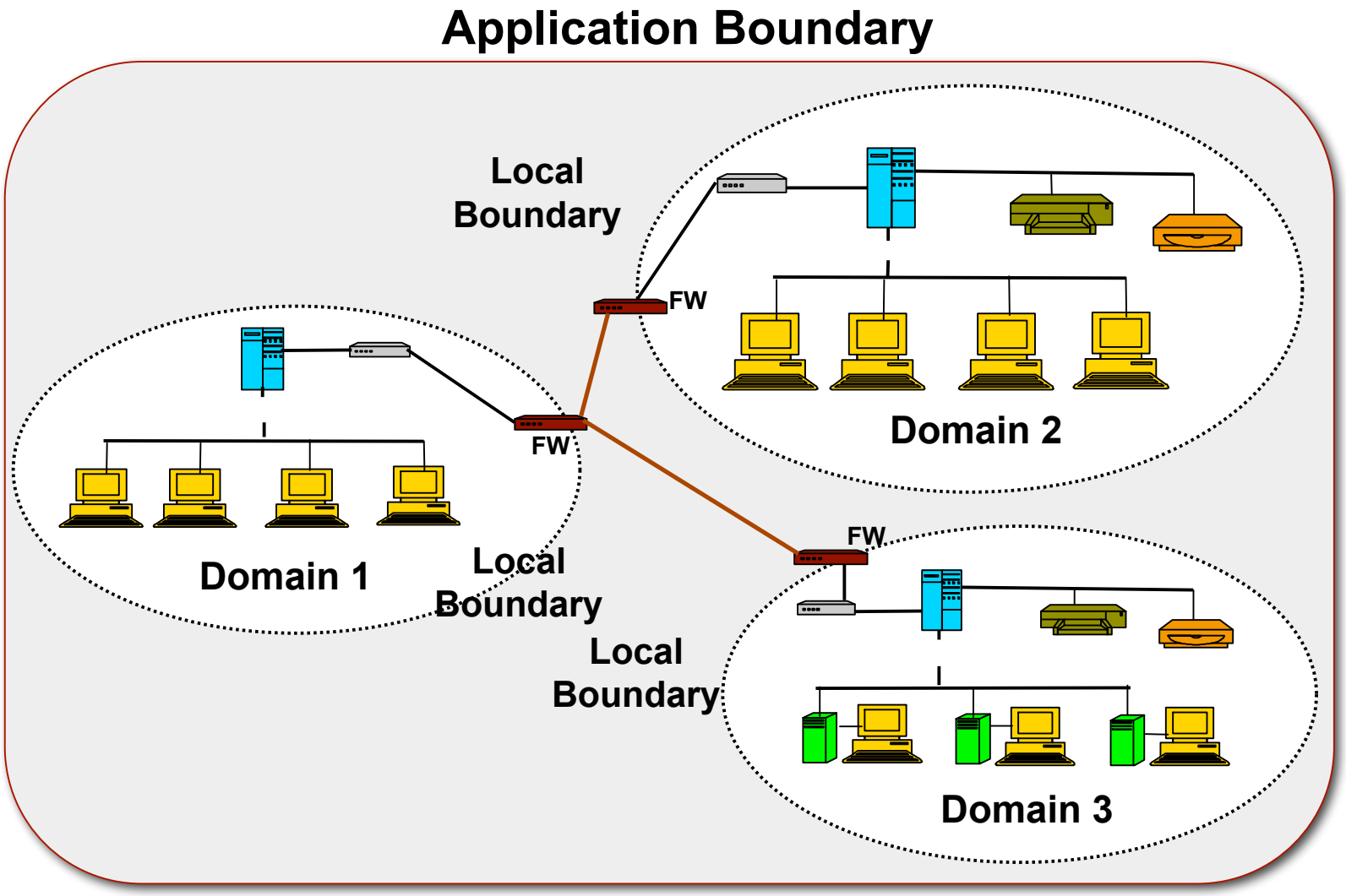
Cross-Domain Model

- **Security responsibility is shared among each component in functional regions**



NORTHROP GRUMMAN

Integrated Information Systems



NORTHROP GRUMMAN

Web Services

- Service Oriented Architecture for application sharing
- Enables “net-centricity”

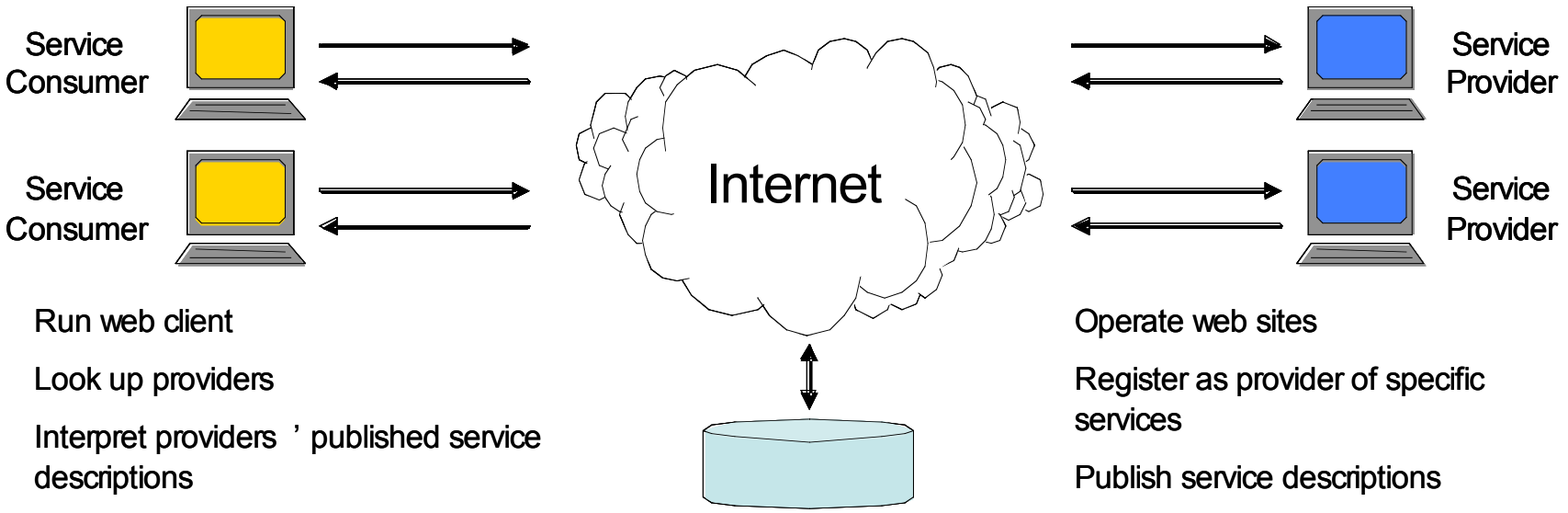
NORTHROP GRUMMAN

Evolution of Internet Technologies

Development	Description	Limitation
Command-Line Hypertext 1991	Scientists developed the original Web servers to assist scientific researchers. Linked hypertext documents were published electronically using the HTTP protocol. Users accessed these documents through command-line browsers. Browsers reference the user-provided host IP addresses or host names in order to retrieve the information.	Users need to know commands. Users need to know location of servers, directories, and file names. Users need to manually connect to servers, receive, store, and process information from unformatted text.
Graphical Browser 1992	The advent of graphical browsers allowed users to point and click to follow embedded hypertext links. The first popular Mosaic graphical hypertext browsers from NCSA popularized the World Wide Web (WWW). These browsers allowed users to enter a URL such as http://www.ncsa.edu to jump to the home page of a requested site. The Home Page at this site would provide a list of links available.	Users need to know location of servers, directories, and file names. Users need to manually connect to servers, receive, store, and process information from unformatted text.
Web Portals 1993	Popular Home Pages quickly evolved into Web Portals, offering lists or directories of other sites available on the WWW. Some portals, e.g., Yahoo, provided searchable directories of sites and methods for new sites to register themselves into a structured taxonomy of information resources.	Users need to know location of the Web Portal that they wish to use. Users need to manually connect to the Web Portal. Users need to navigate the lists of links on the Web Portal to manually select the source they want. Users need to open the link to connect to Web servers, receive, store, and process information from unformatted text.
Web Search Engines 1994	Web searching applications evolved to proactively search and index Web servers into large databases based upon text key words. When new sites or updated Web pages are created, the search engines must rediscover them and update their databases. Users must then search for and find the new information.	Users need to know the location of the Web Search Engine that they wish to use. Users need to manually connect to the Web Search Engine. Users need to enter the search terms into the search window of the selected Web Search Engine. Users need to navigate the lists of links provided by the search engine to manually select the source they want. Users need to open the link to connect to Web servers, receive, store, and process information from unformatted text.
Web Services 2001	The XML standard allowed documents to be exchanged containing embedded data descriptions along with text. As related standards developed these capabilities provided for distributed applications across the Internet. A client application can dynamically locate and link to current information and service resources. New servers and services dynamically register themselves.	Users need to have client applications that are enabled for XML and Web Services.

NORTHROP GRUMMAN

Web Services Architecture

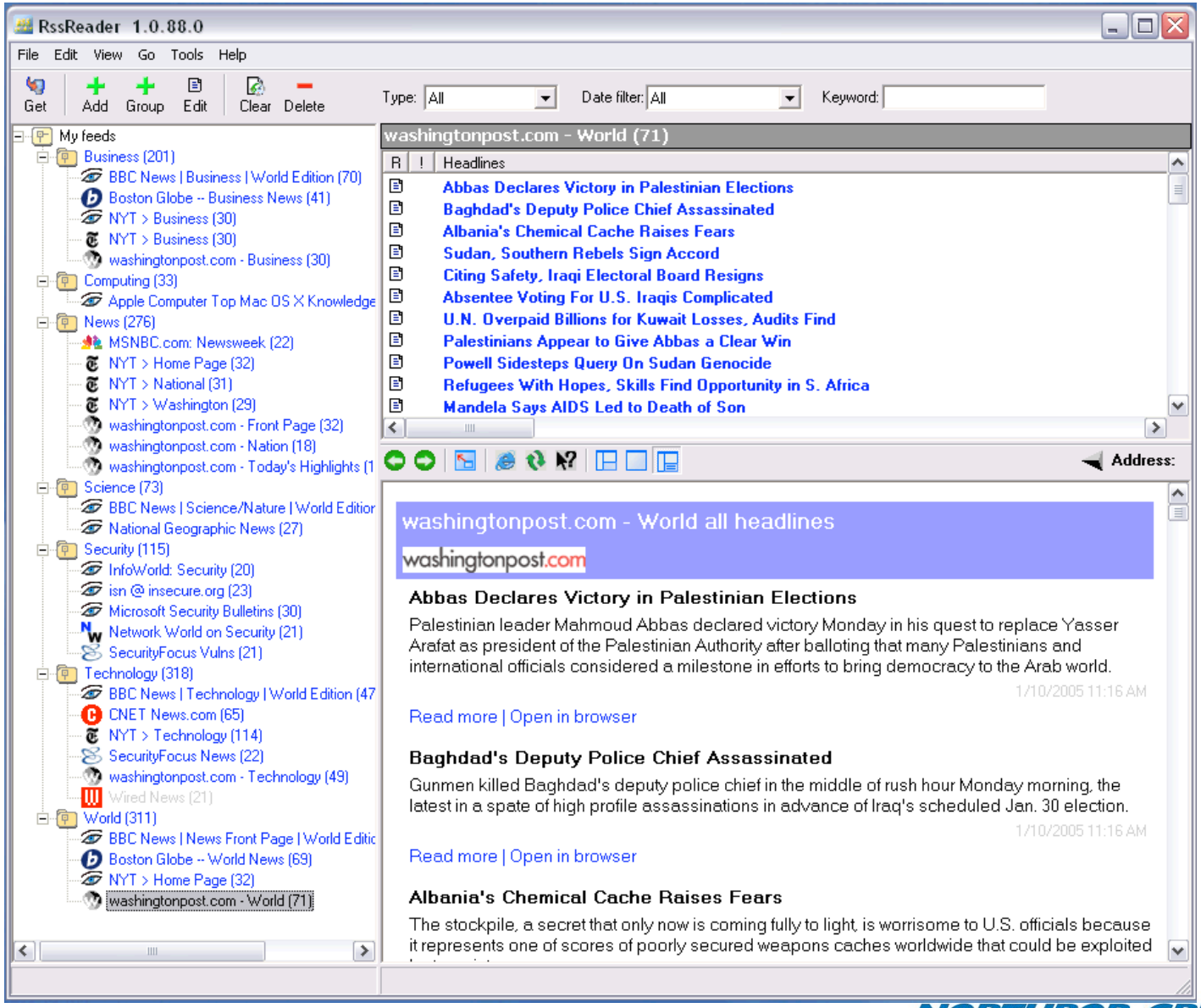


- Run web client
- Look up providers
- Interpret providers ' published service descriptions
- Transfer data from providers
- Process and display integrated information

- Operate web sites
- Register as provider of specific services
- Publish service descriptions
- Transfer requested data to consumers
- Store and publish XML formatted data

NORTHROP GRUMMAN

Really Simple Syndication (RSS)



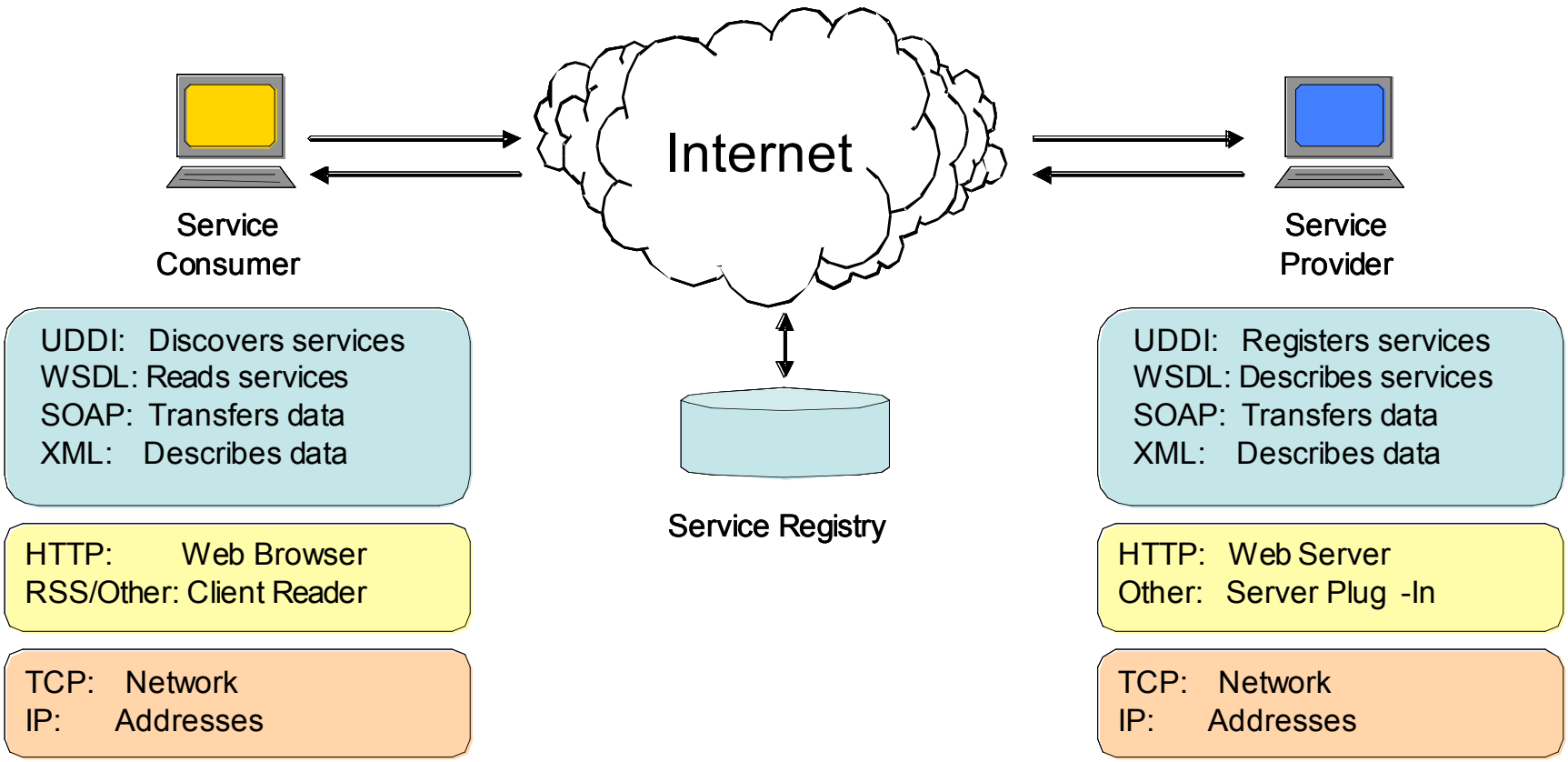
NORTHROP GRUMMAN

XML Protocols

- **Data Representation**
  - Extensible Markup Language (XML)
- **Data Communication**
  - Simple Object Access Protocol (SOAP)
- **Service Description**
  - Web services Description Language (WSDL)
- **Service Discovery**
  - Universal Description, Discovery, anad Integration (UDDI)
- **News**
  - Really Simple Syndication (RSS)

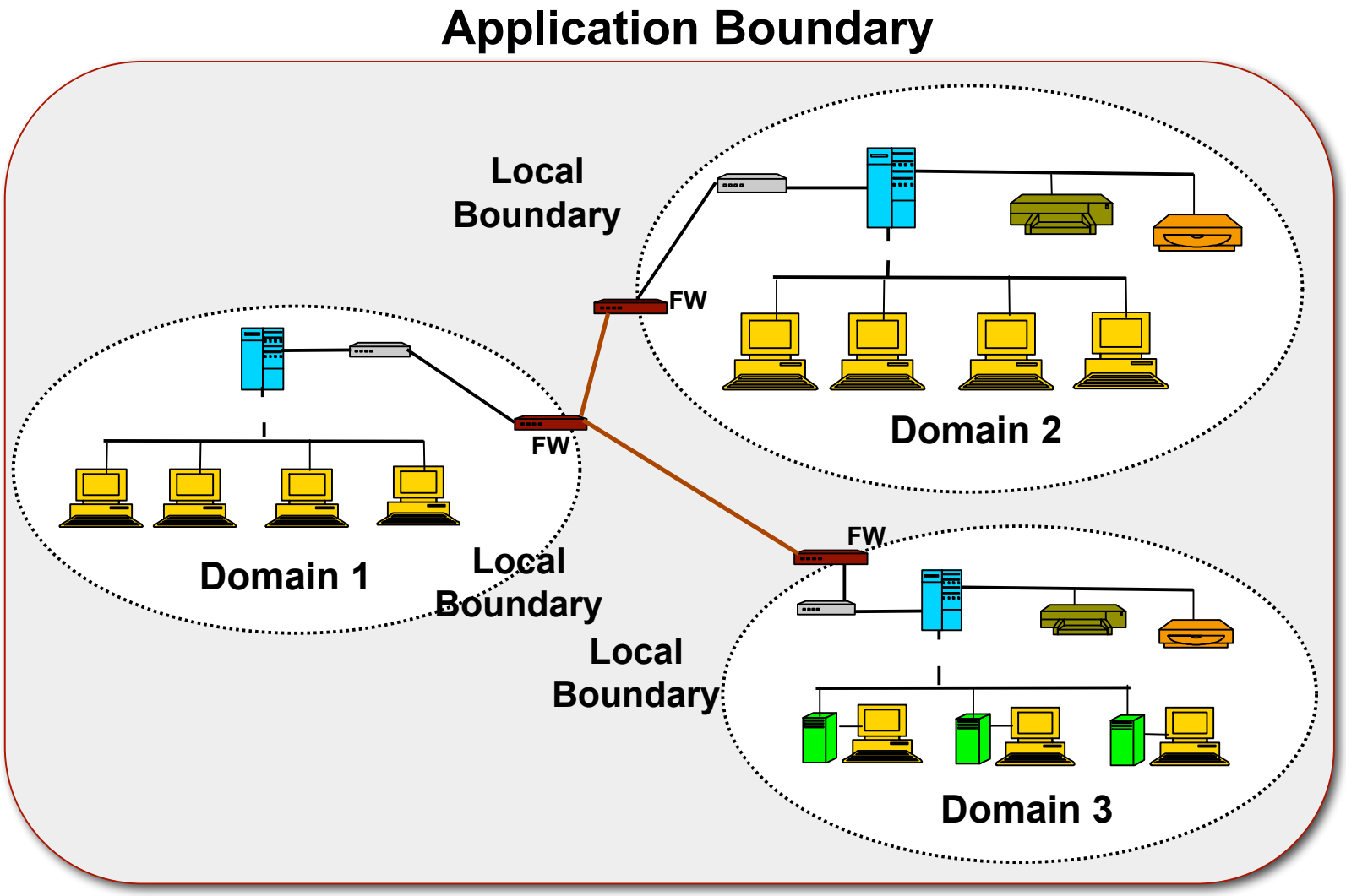
NORTHROP GRUMMAN

Application Architecture



NORTHROP GRUMMAN

Integrated Information Systems



NORTHROP GRUMMAN

Solution Technologies

- New technologies offer additional approaches to the cross-domain information sharing problem

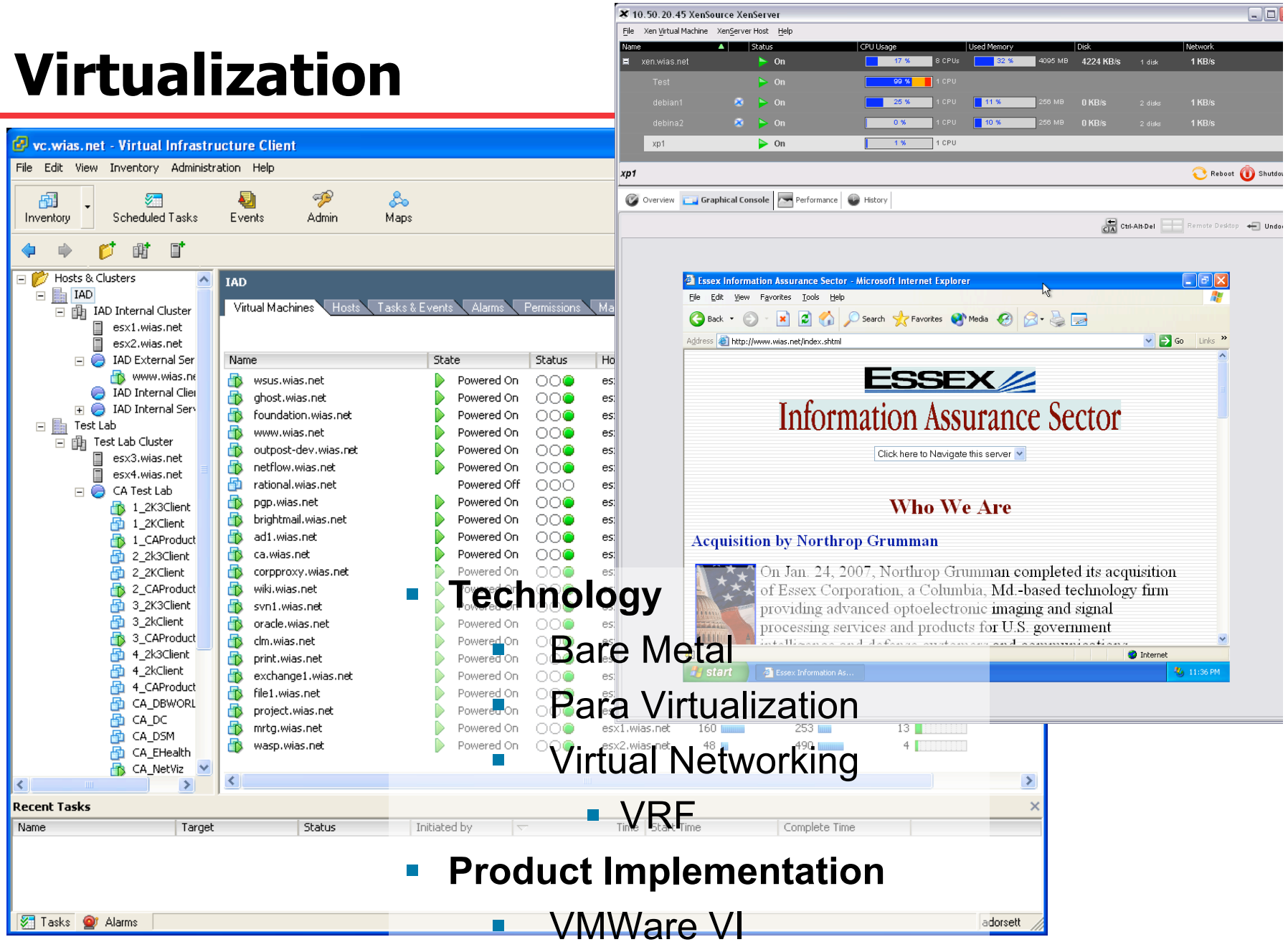
NORTHROP GRUMMAN

Computing Technology Evolution

Centralized Data Centers

Centralized Data Centers

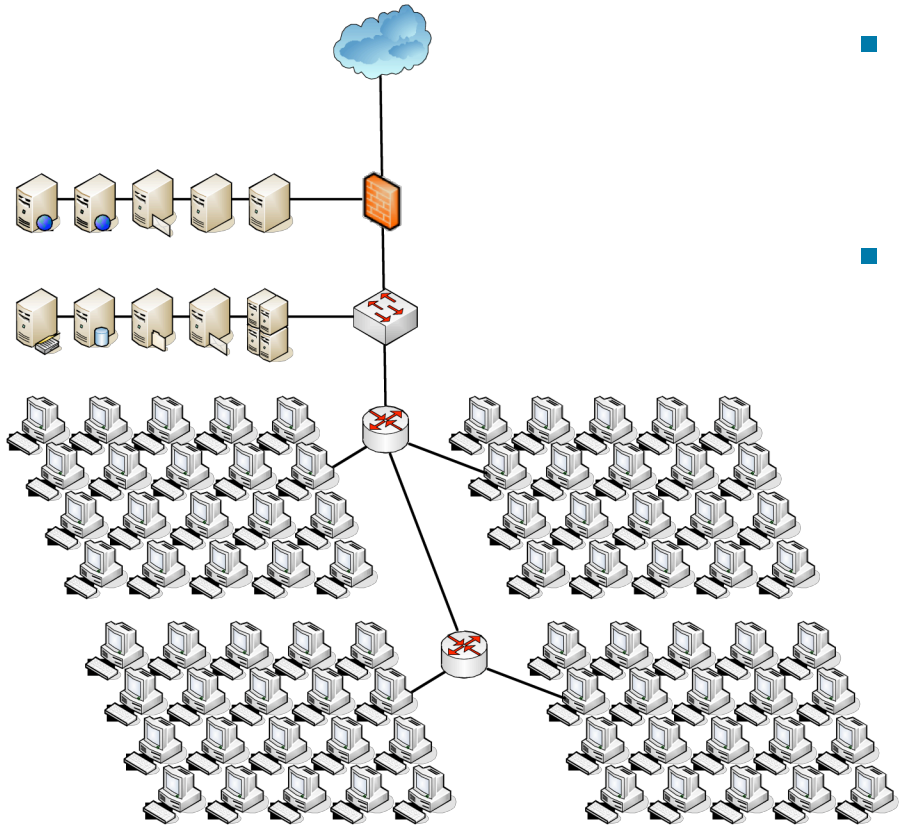
Virtualization



- **Technology**
  - Bare Metal
  - Para Virtualization
  - Virtual Networking
    - VRF
- **Product Implementation**
  - VMWare VI
  - XenSource Enterprise

NORTHROP GRUMMAN

Going Beyond the Enclave



- **Physical Model**
  - The enclave concept is physical
- **Virtual Implementations**
  - Enclaves are often implemented in virtual components, VLANs, Virtual hosts

NORTHROP GRUMMAN

Security Implications

- Physical components are now logical
- Converges Physical Infrastructure
- Converges Network Components
- Integrates IA Monitoring components into single in-band capability
- Shares memory spaces among Virtual Machines
- Reduces separation

NORTHROP GRUMMAN

Protecting Virtualized Infrastructure

- Confidentiality of Virtual machines
- Integrity of Virtual Machines
- Availability of Virtual Machines
- Use of Non-Persistent File Systems
- Refreshing Virtual Machines
- Virtual Firewalls
- Virtual Switches
- Integrity of Virtual Security Systems
- Detectability of Virtual Infrastructures

NORTHROP GRUMMAN

Summary

- **Problem**
  - Conventional Enclave architecture does not easily support collaborative information sharing, web services, or other needs
- **Solution**
  - Apply architectural concepts and models
  - Apply new information technologies
  - Develop New security solutions
- **Assumptions**
  - Cross-domain information sharing requirement
  - Web services information infrastructure

NORTHROP GRUMMAN