Architecting for Secure Network Management

Rod Murchison
VP Product and Corporate Development
Ingrian Networks Inc.

Wednesday, January 29th 2003

Agenda

- Security Market Analysis: Trends and Indicators
- Top Security Threats to Corporate Infrastructures
- Deployment Examples:
  - Secure Web Acceleration
  - Web Application Protection
  - Web Data Protection
- Summary of Best Practices
- Q & A

Security Market Analysis

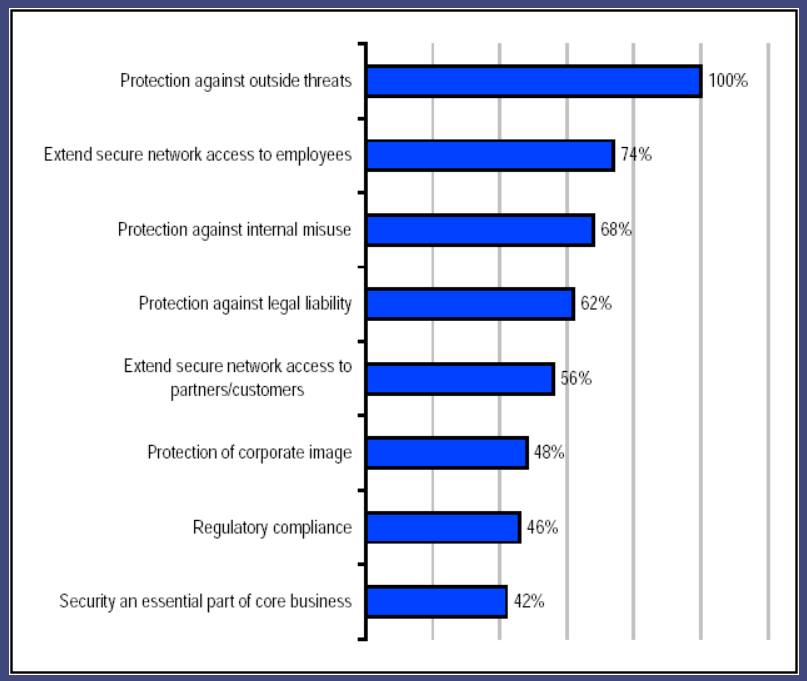
- "Security Software Market"
  - 2002 market size estimate at $9.8 B US [1]
  - Includes software, appliances, some hardware products
  - Expected to grow to $15 B US by 2006 [1]
- Security technology is moving up the stack from network layer to application / data layer
- Increasing concern over malicious activity within the infrastructure rather than the perimeter
- Emergence of a myriad of SSL/TLS-based web applications… and problems deploying them

1 - Source: "Security Software In-Depth Report – Merrill Lynch – Oct. 30th 2002

Security Market Analysis (cont.)

- Merrill Lynch Survey of 50 CIOs
- Showing surprising contradiction… 80% of attacks internal, but key concern is external threats
- Corporate policy changes on internal threats are driving new deployments
- SSL/TLS still one of the fastest growing application data transports

What are the key factors in your decision to purchase security software?



SOURCE: ML Survey of 50 CIOs

Security Market Analysis (cont.)

- 85% of IT managers: “Security is the most important issue”
  - $21 Billion spent on Internet security by 2005
  - 80% of all breaches are internal
  - Significant hacking attacks more than doubled in past year (20k to 50k)
- Secure web traffic (SSL/TLS) up from 5% to 33% by 2004
  - Exceeds 75% in financial services sector
- 5% of online consumers have experienced credit card fraud
- Internet-based B2B transactions up to $70 billion by 2003
- New attacks focus on compromising stored data, not transmitted data
  - Nimda, Code Red, SQL injection attacks, etc.

Security Market Analysis (cont.)

- Legislation and mandates emerging across most verticals worldwide for data security and privacy
- Integral components of:
  - US - Health Insurance Portability and Accountability Act of 1996 (HIPAA)
  - US - Gramm-Leach-Bliley Act of 1999 (GLBA)
  - UK - Data Protection Act 0f 1998 (DPA)
  - Many others…
- Across the board, most mandates are specifying best practices and guidelines, but not specific details on technical implementation
- Many companies are forming their own policies for data protection and protection, but realizing the push to web-enablement of key services can be very risky

The 5 Biggest Threats

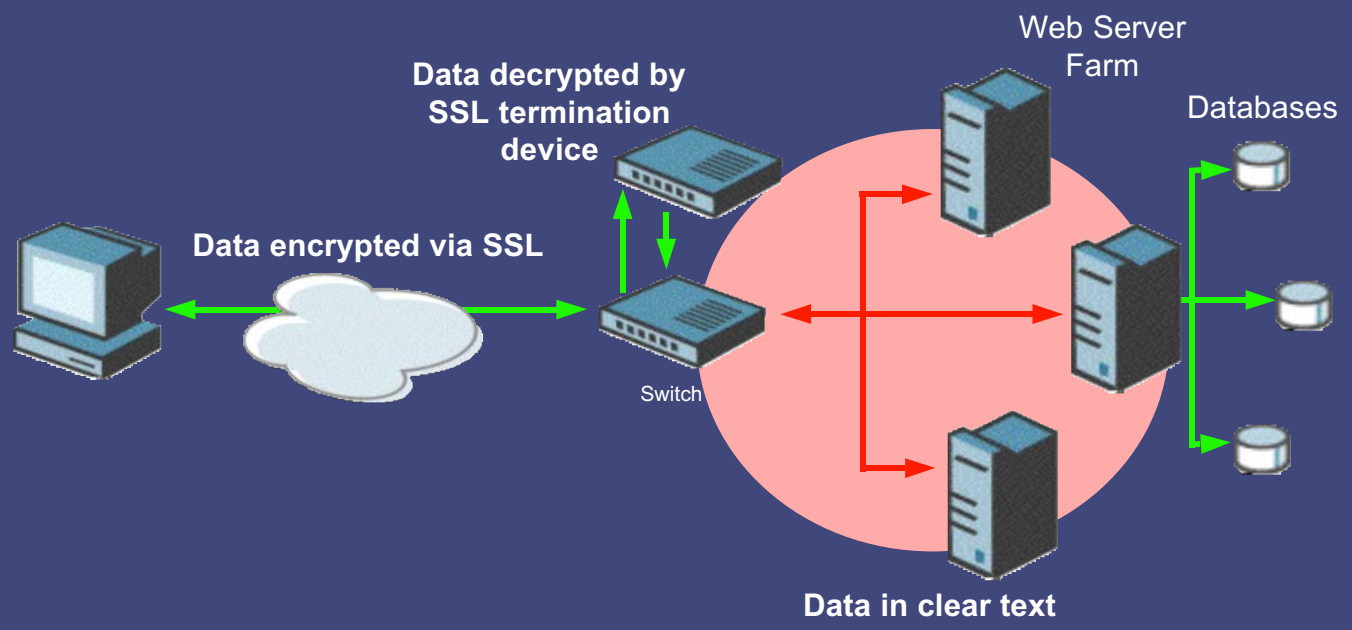
- Most significant threats to network security:

1. Compromise of Unencrypted Data
2. System Intrusion via Application Level Attacks
3. Theft of Private Keys
4. Unauthorized System Access
5. Administrative Errors

Web Data Security and Privacy Objectives

1. Ensure data is encrypted, as required, in transit from the client to the data store
2. Provide selective data encryption
3. Ensure data remains encrypted once it is finally stored
4. Protect cryptographic keys / identity from theft
5. Protect stored data against unauthorized access
6. Separation of data management roles and responsibilities with full audit capabilities
7. Enable a 3rd party trust model – a receiver can handle / process stored data that can only be decrypted by a partner

Threat 1: Compromise of Unencrypted Data (Transit Vulnerability)

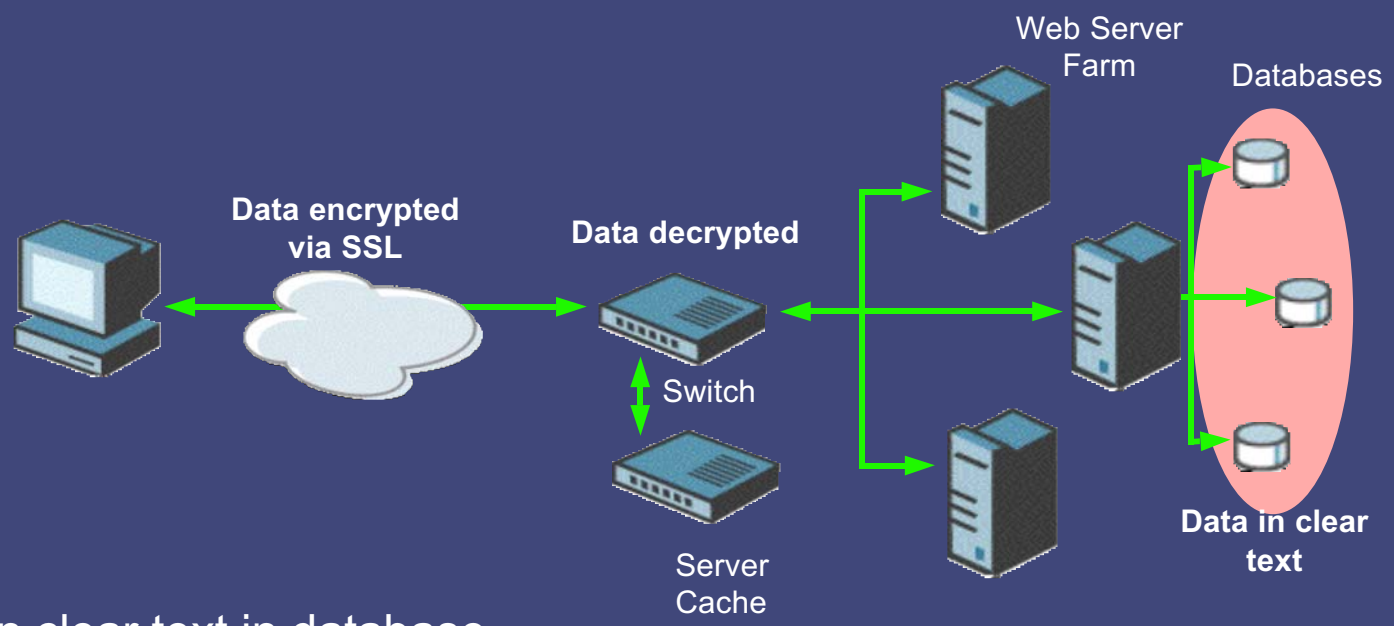


- Encryption stripped off inside network
- Data in clear text – easy to misuse
- Traditional switches, firewalls, etc. can't fully process secure data

Data Infrastructure Attacks

- How is this possible?
  - Latest web and security attacks are designed to get at your core data, and they are working
  - Most breaches are internal, and poor controls are in place for administrative data access
  - Push to open Web Services model without considering security impacts
- What can you do
  - Adopt data encryption methods that ensure sensitive data is never used or stored in the clear
  - Employ stringent controls on administrative access to sensitive data

Threat 1: Compromise of Unencrypted Data (Storage Vulnerability)



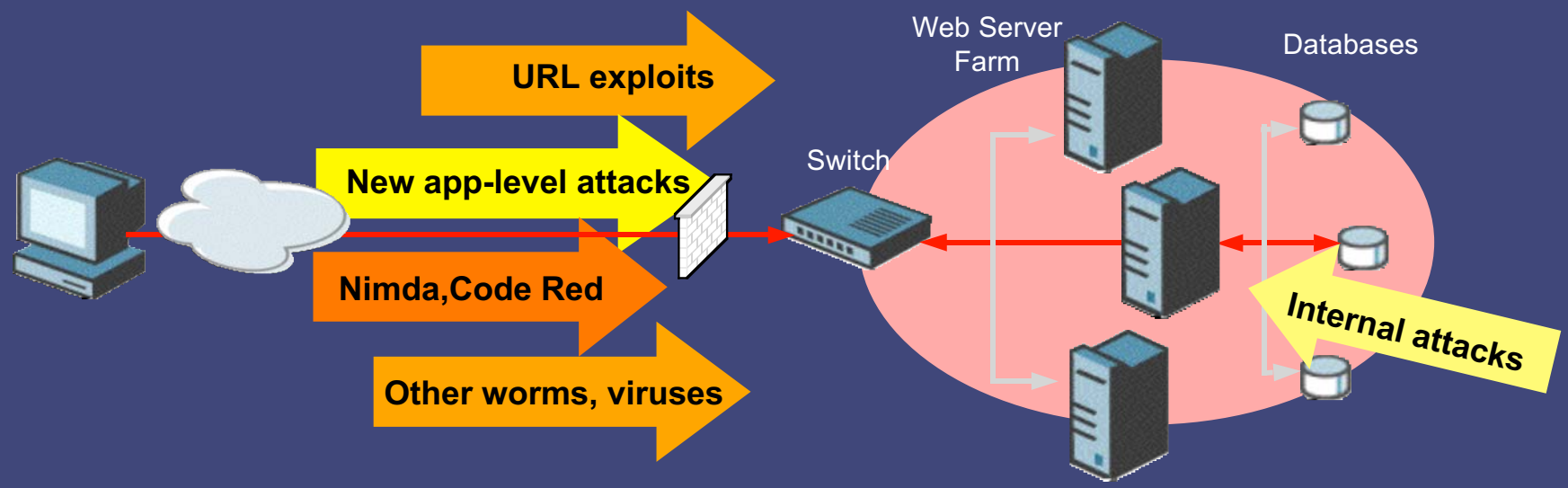
- Data in clear text in database
  - Passwords and cookies
  - Credit card and Social Security numbers
  - Personal data: financial, medical, etc.
  - Corporate data: plans, strategies, price lists, etc.

Threat 1: Compromise of Unencrypted Data (Storage Vulnerability)

Consequences of leaving information unprotected can be catastrophic

- Business Costs
  - Organizational financial loss
  - Client/Customer financial loss
- Credibility Costs
  - Reputation damage
  - Public embarrassment
- Productivity Costs
  - Operational disruption
  - Opportunity costs
- Legal Costs
  - Potential violation of government laws

Threat 2: System Intrusions via Application-Level Attacks



- SSL is a direct tunnel to Web servers
- Firewalls don't stop new threats to Web server-based applications
- Internal and external breaches can access entire network

Web Application Infrastructure Attacks

- What is “Code Red” and “Nimda”?
  - Specific attacks that exploit errors in the way URLs are processed on webservers
  - Successful attack opens up your webserver to the possibility of executing code delivered by the hacker
  - Foothold on the webserver can provide the hacker a means to infiltrate backend systems (app servers, databases, etc.)
- What can you do?
  - Ensure that any system that provides web services is fully protected with software / hardware
  - Plan for scalable network performance
  - Prepare for going even deeper in the *ML to find attacks with Intrusion Prevention & Application Protection solutions
  - Don’t forget about SSL…

What is Cookie Poisoning?

- What is Cookie Poisoning?
  - Manipulating the cookie text or forging session cookies to create an impersonation attack (Identity Theft).
  - Manipulating the cookie text to alter the Web session for other reasons (e.g., slashing prices on eCommerce purchases if the price is encoded in the cookie [eShoplifting] or reassigning charges to another user [eFraud]).
- Why does Cookie Poisoning happen?
  - Cookie content is often not generated in a secure or protected way, leaving them vulnerable to inspection and manipulation
  - Cookie content is easily accessible to the client

Who is Vulnerable to Cookie Poisoning?

iVillage
Identity Theft
August 2002

Each time users logged onto iVillage.com, they saw a different person's inbox, complete with these other people's private messages.

Barnes & Noble.com
Identity Theft
August 2002

Personal information of on-line shoppers, collected in cookies and transmitted insecurely, can be accessed by hackers.

msn Hotmail
Identity Theft
April 2002

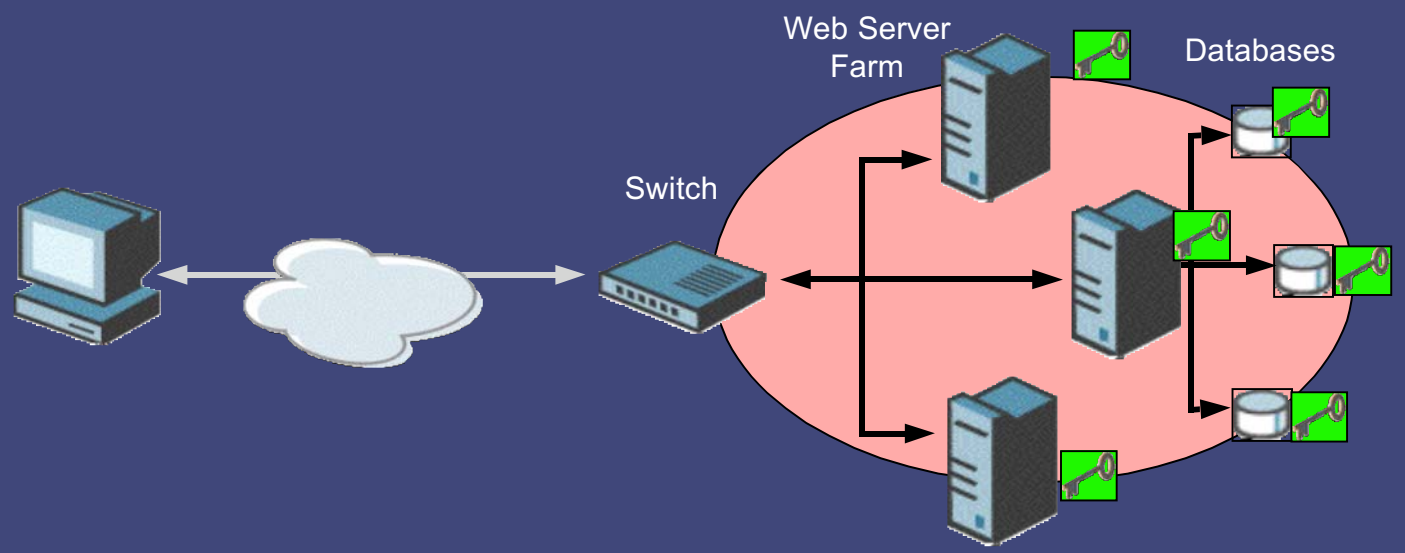
When a victim's cookie was stolen, the thief had access to the victim's e-mail account forever, despite the victim repeatedly changing her password.

amazon.com
eShoplifting

Hackers discovered that the list price of books placed in their "shopping cart" is included, unencrypted, in their cookie. Editing the cookie.txt file allowed them to purchase items at 90% off.

Anyone using unencrypted & decipherable cookies for authentication, affinity, or Web tracking is vulnerable to Cookie Poisoning.

Threat 3: Theft of Private Keys

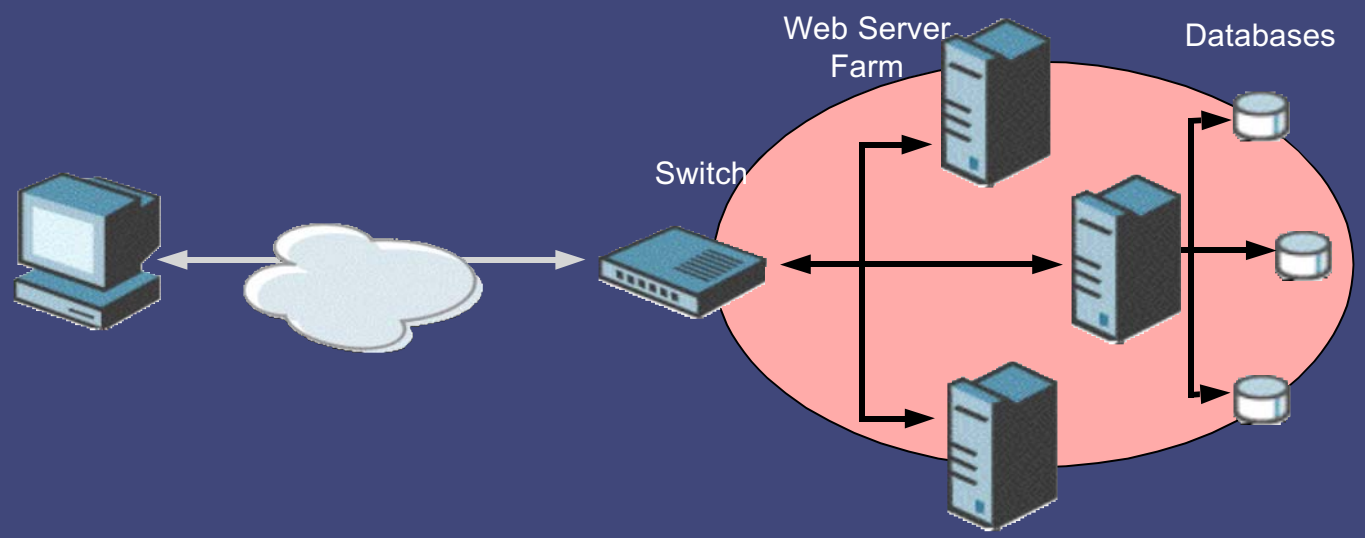


- Private keys kept in clear text
- Keys stored on Web servers and in databases
- Vulnerable to internal and external compromise
- Theft of corporate identity

Security Infrastructure Attacks

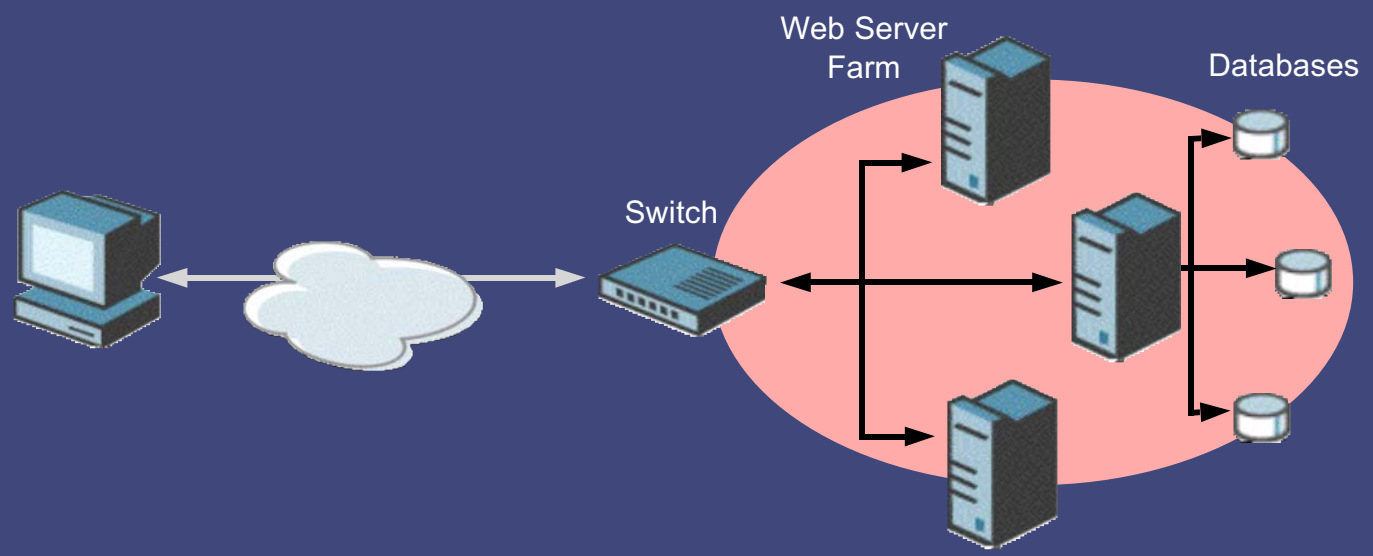
- Why is private key theft so damaging?
  - With your private key, a hacker could decrypt your data, transactions, or even spoof your identity
  - Significant liability being associated with key theft
  - Loss of partner / consumer trust can be fatal
- What can you do?
  - Fully assess your security environment, and audit who is capable of what
  - Embrace FIPS 140-1/2 Level 2/3
  - Embrace SSO

Threat 4: Unauthorized System Access



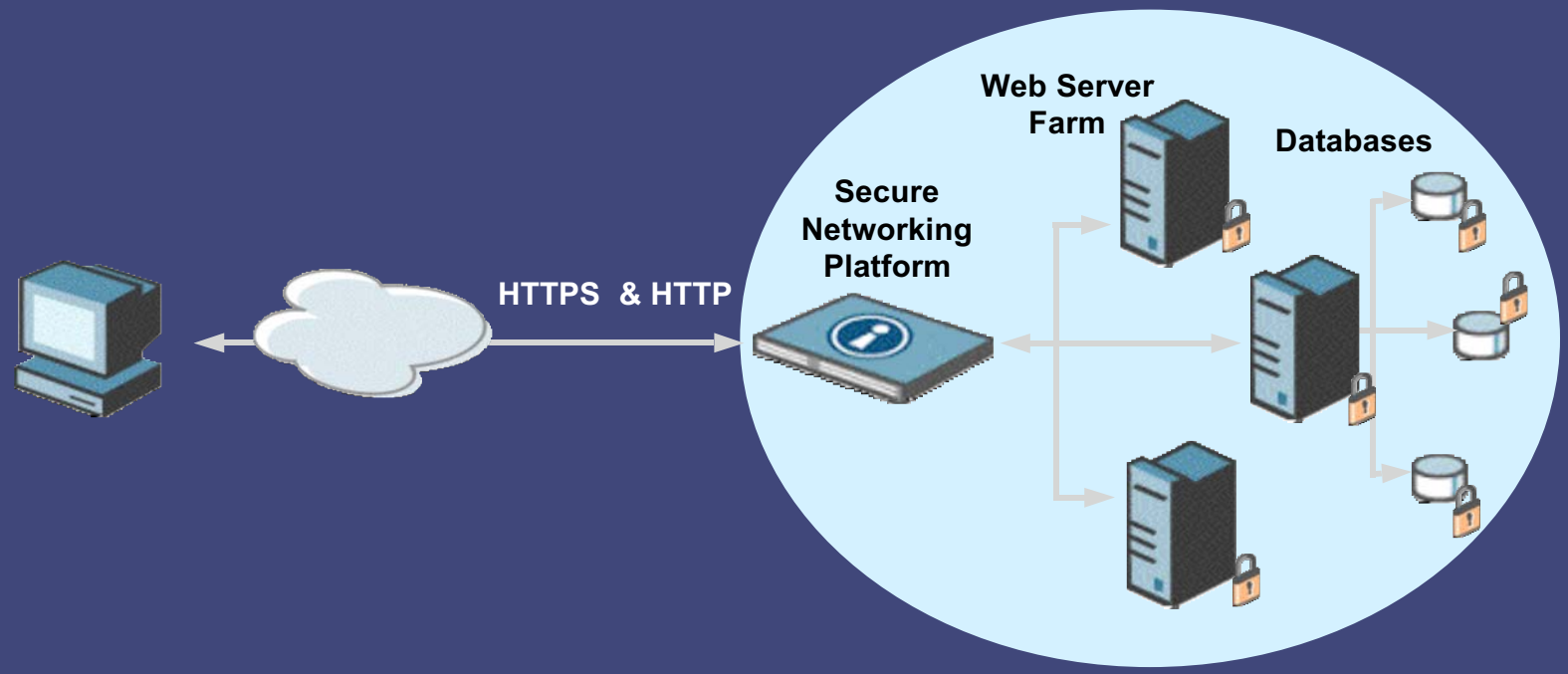
- Inadequate access controls on sensitive data is big threat.
- Fine-grained policies for administration often not in place
- Inadequate administrative action logging or audits
- Remember… most breaches are internal

Threat 5: Administrative Errors



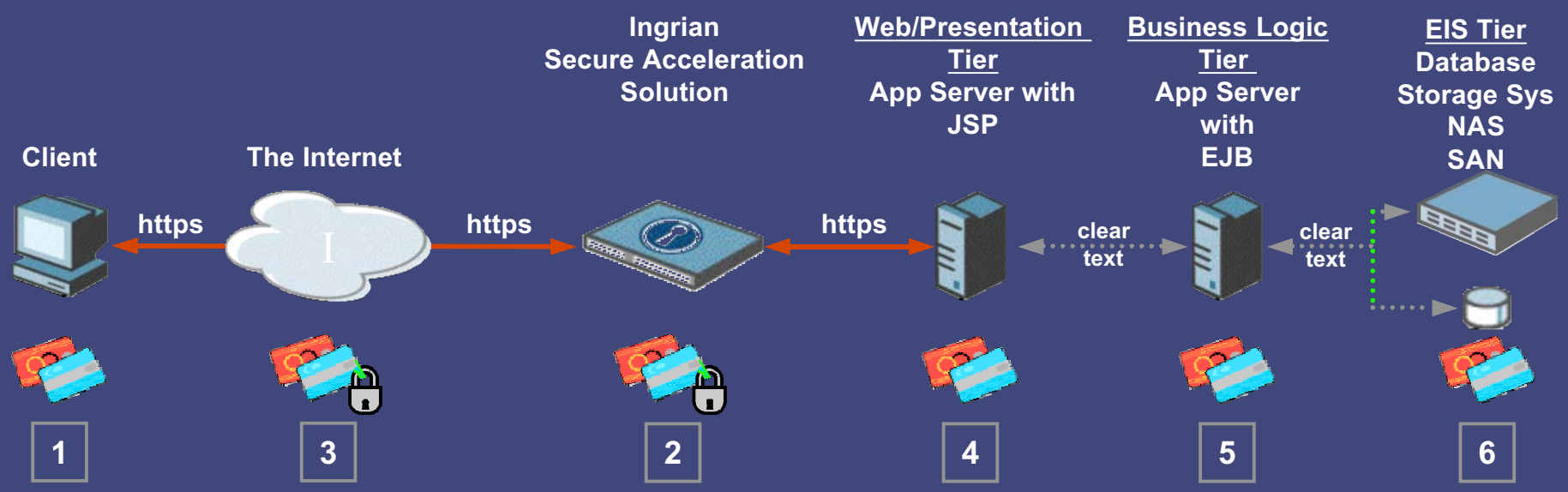
- Mis-configuration of security parameters
- Network-based attacks have blurred the line of control between network and security managers
- Many administrators do not even know they have inadvertently caused a security problem

Solutions for Threat 1: Compromise of Unencrypted Data



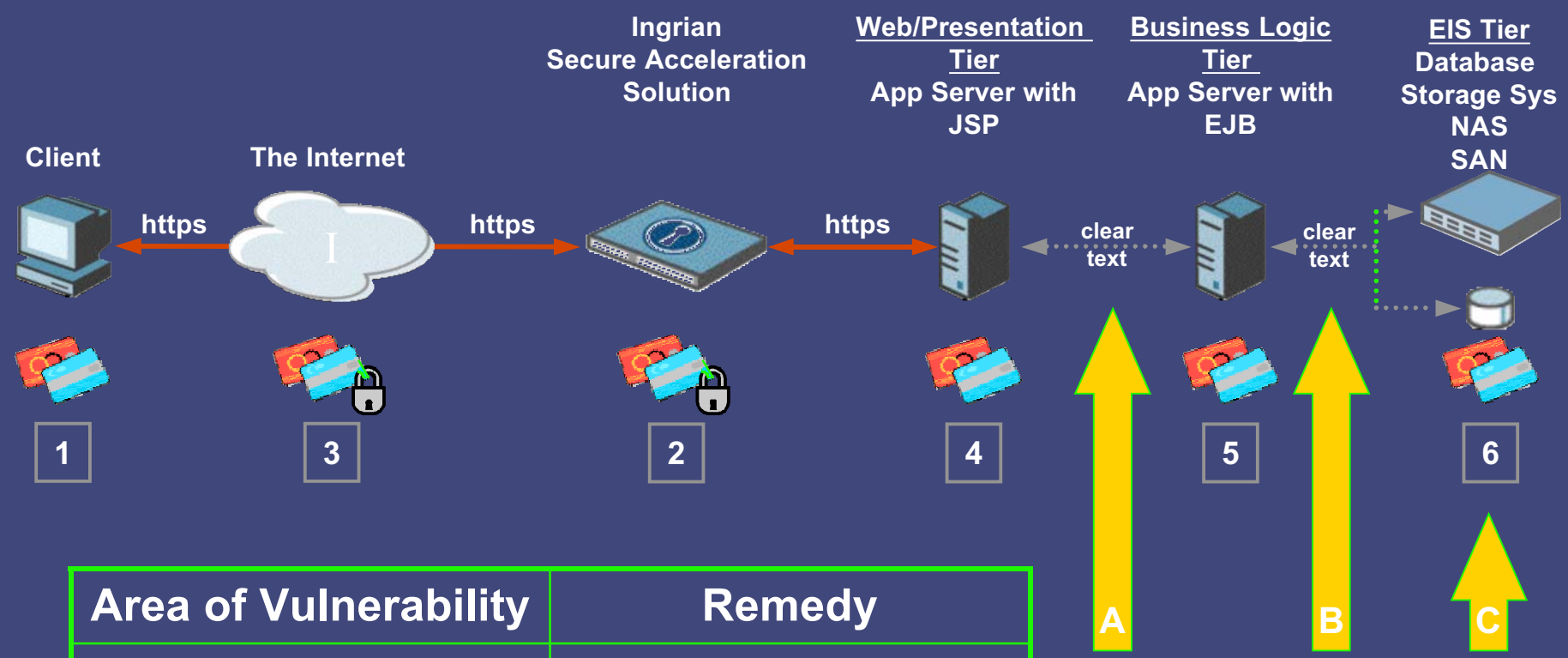
- Leverage new data encryption technologies in the network and on the server
- Develop data exchange models that ensure sensitive information is not accessible in the clear
- Other vendors: F5, Cisco, RSA, Oracle, Protegrity, and IBM

Know The Typical Sensitive Data Processing Architecture



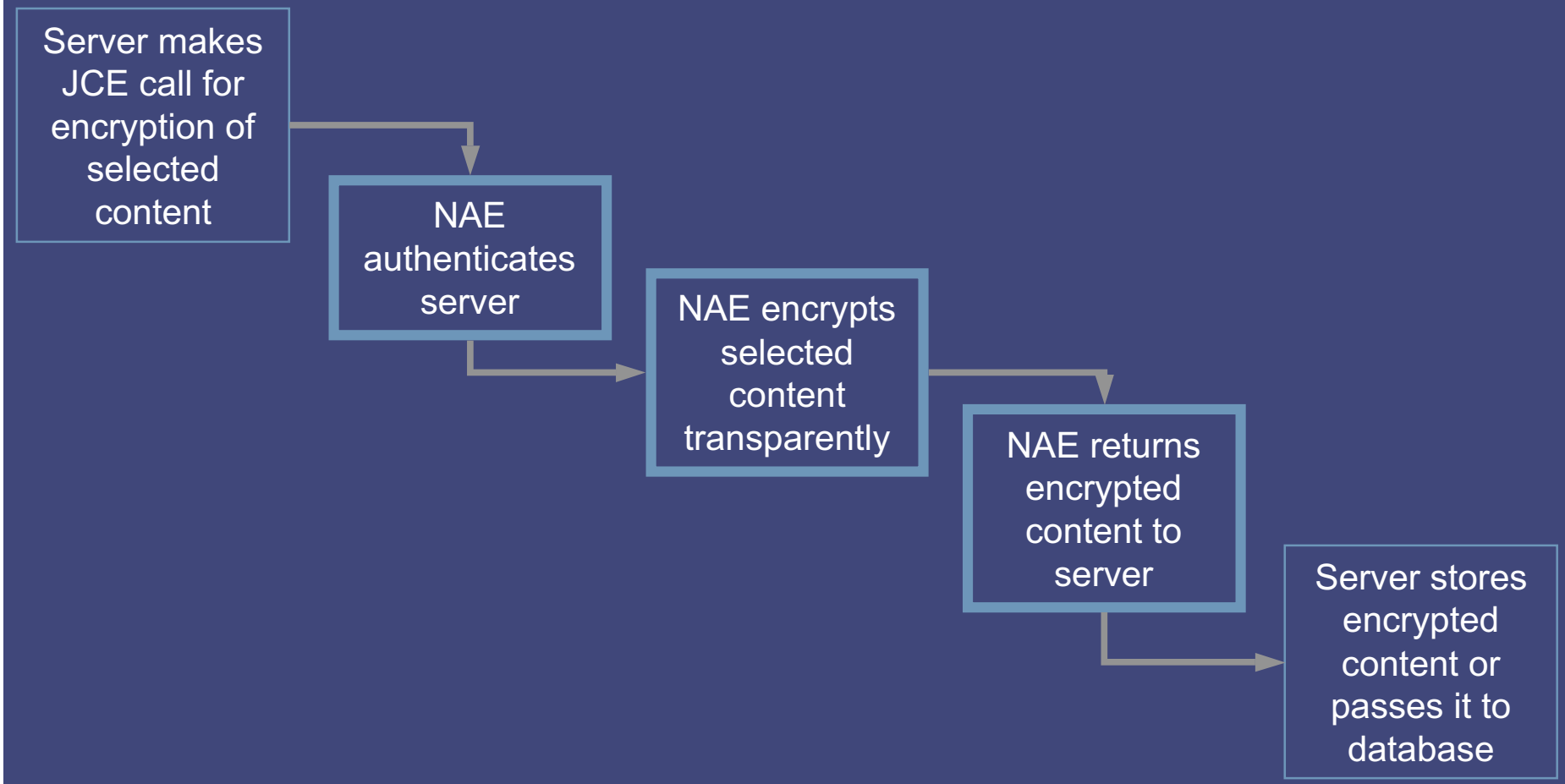
1. A client enters confidential information (e.g., credit card number) in a web form and submits it to a "secure" web site
2. The Ingrian AAS platform accelerates the SSL traffic and establishes a back end SSL connection to the Tier 1 server
3. The CC# is secure in transit through the SSL tunnel
4. The Tier 1 Server terminates the SSL connection from the Ingrian platform
   The Java Servlet Page (JSP) on the Tier 1 Server performs cursory verification on the CC#
   If verification fails, the JSP returns a failure message to the client.
   If verification passes, the JSP forwards the CC# ***in clear text*** to the Tier 2 Server
5. The Enterprise Java Bean on the Tier 2 Server performs further business logic and verification on the CC#
   The EJB forwards the CC# ***in clear text*** to back-end storage
6. The CC# resides ***in clear text*** in storage (database, NAS, SAN, or other storage system)

Know the Vulnerabilities In the Data Processing Architecture



Area of Vulnerability	Remedy
A. Transport	Encrypt / MAC
B. Transport	Encrypt / MAC / hash
C. Persistent Storage	Encrypt / MAC / hash

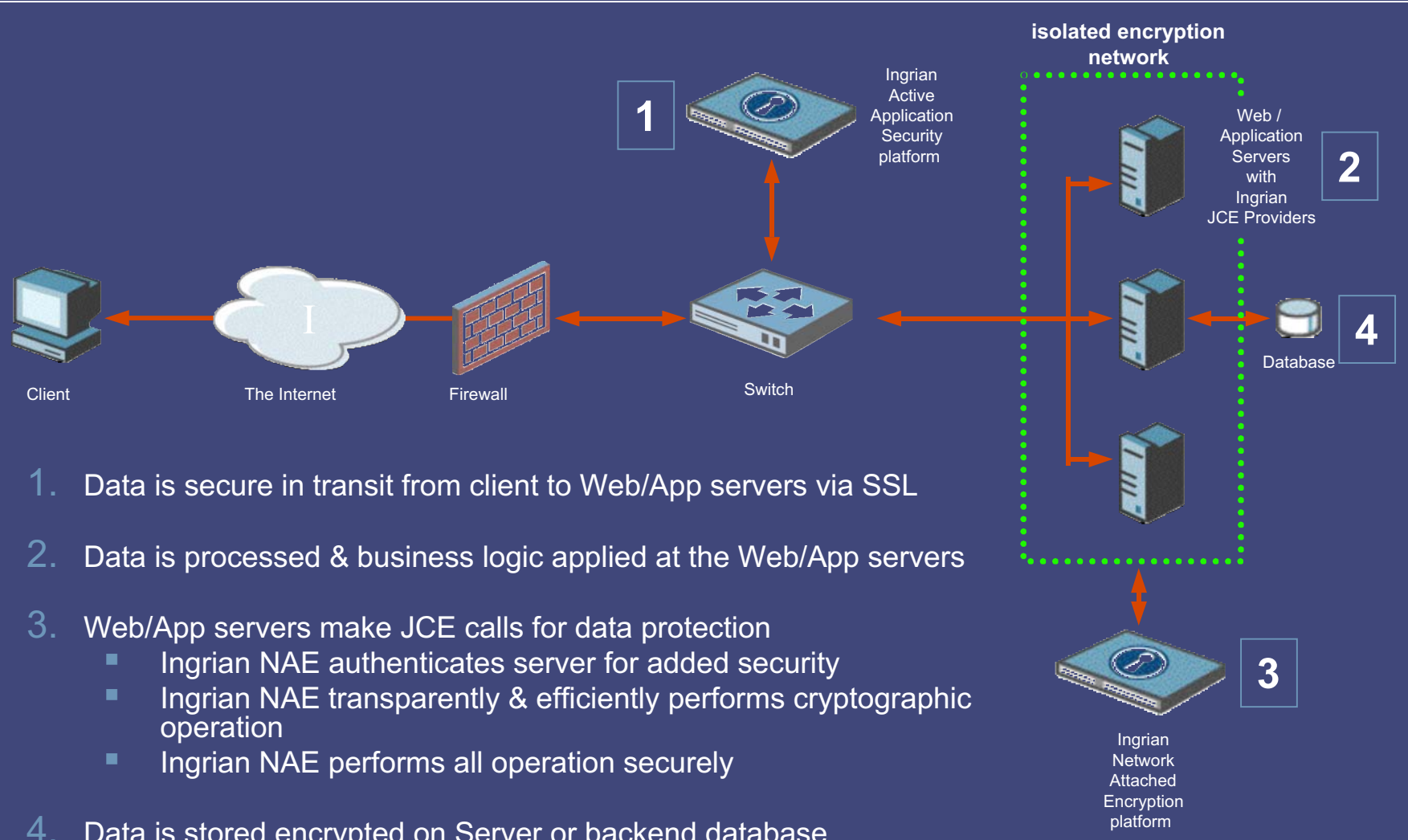
Example of leveraging J2EE & J2SE compliant applications for fine-grained data encryption



Advantages Of Network Attached Encryption

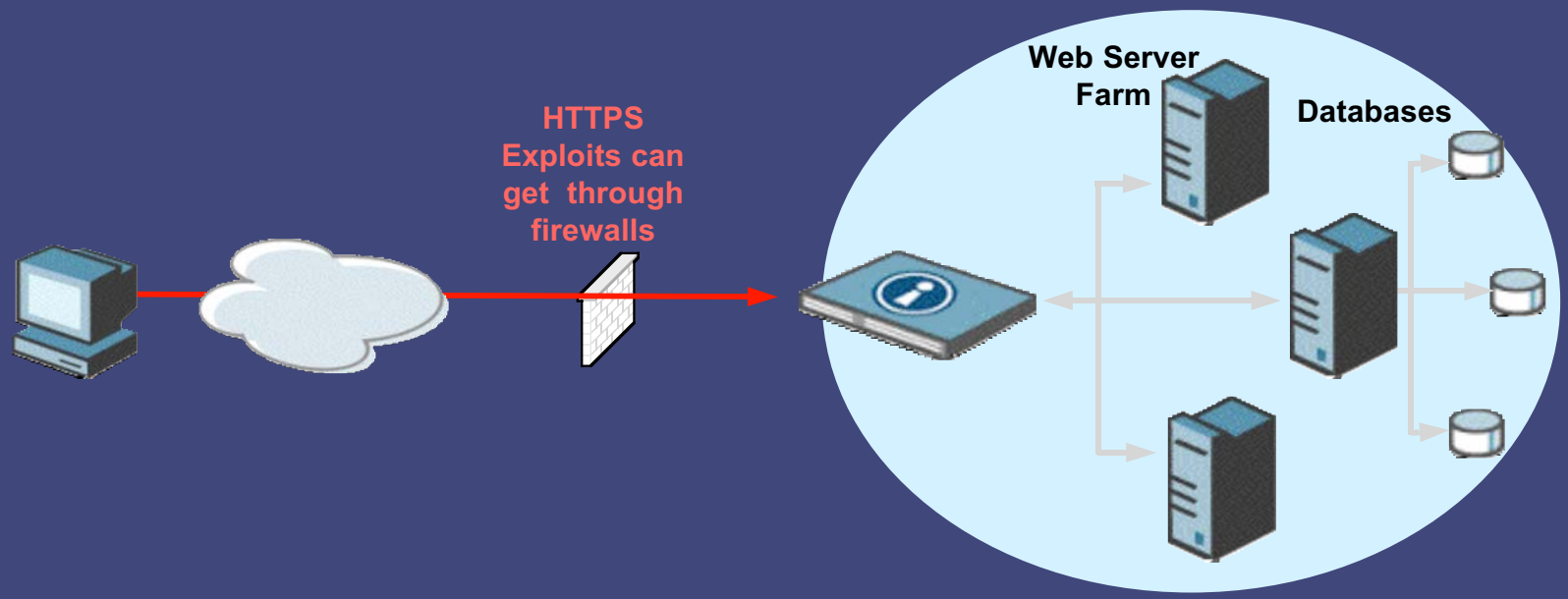
Network Attached Encryption		"Per-Server" Based Architecture
❖ Cryptographic keys live on a single, secure platform	vs.	❖ Cryptographic keys reside insecurely on each and every web/app server
❖ Key management (creation, deletion, replication, etc.) performed in one location	vs.	❖ Key management (creation, deletion, replication, etc.) performed laboriously and repetitively on each and every web/app server
❖ Administration and management access is controlled by fine-grained, multi-factor authentication	vs.	❖ Administration and management access is controlled by flimsy server-based authentication
❖ Logs, statistics, and crypto information aggregated centrally and stored securely	vs.	❖ Logs, statistics, and crypto information scattered among servers and stored insecurely
❖ Scalability for additional encryption capability is horizontal with one-click replication	vs.	❖ Scalability for additional encryption capability is vertical and labor-intensive

Example Deployment of Network Attached Encryption



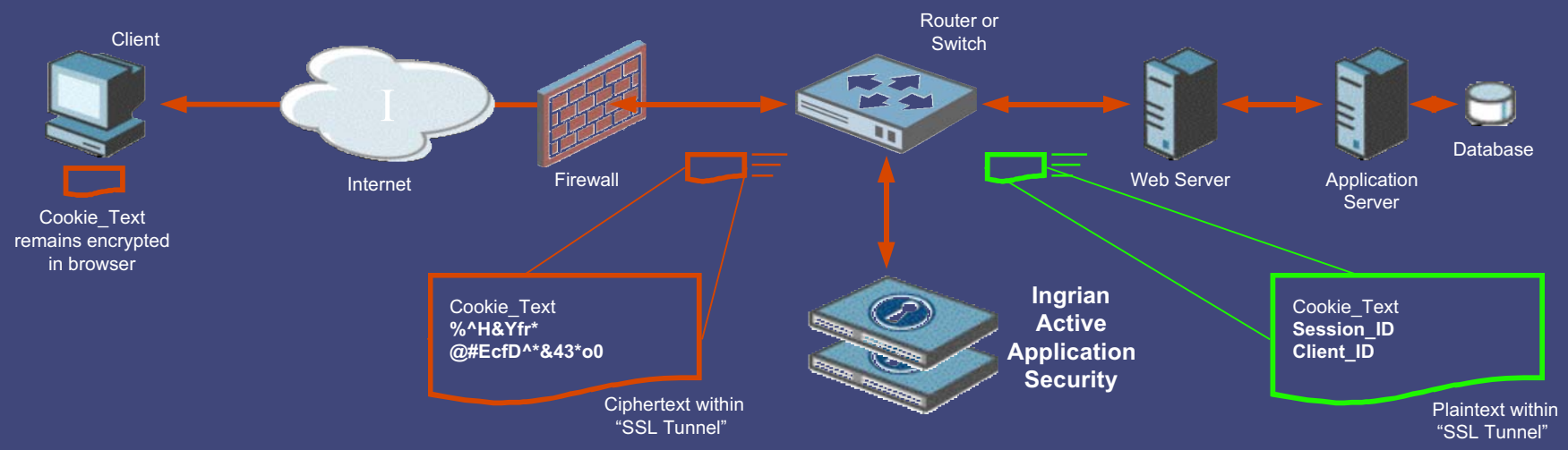
1. Data is secure in transit from client to Web/App servers via SSL
2. Data is processed & business logic applied at the Web/App servers
3. Web/App servers make JCE calls for data protection
   - Ingrian NAE authenticates server for added security
   - Ingrian NAE transparently & efficiently performs cryptographic operation
   - Ingrian NAE performs all operation securely
4. Data is stored encrypted on Server or backend database

Solutions for Threat 2: System Intrusions via Application-Level Attacks



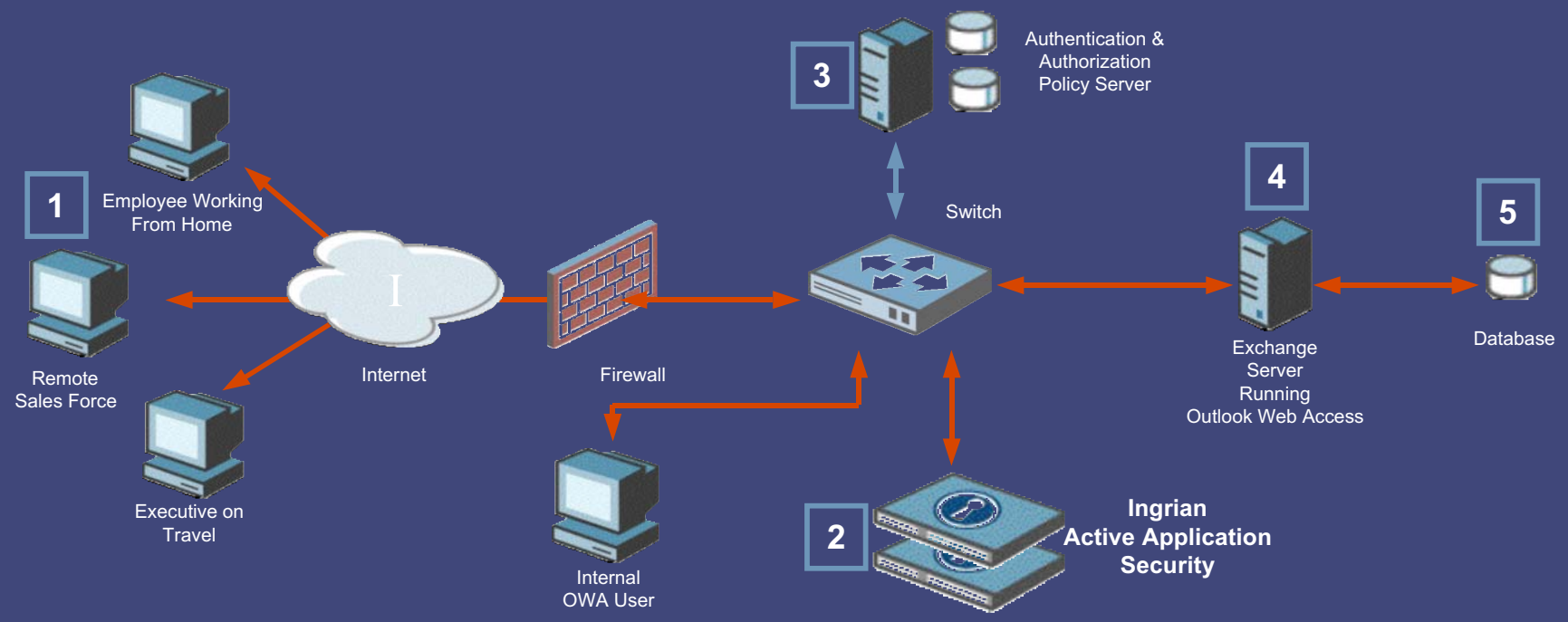
- Ensure that you can protect against HTTP and HTTPS attacks (Nimda, CodeRed, etc.)
- Most traditional firewalls good for HTTP, but ensure you have enough horsepower
- Other vendors: Netscreen, Checkpoint, Cisco, Symantec, Kavado, etc.

Cookie Protection



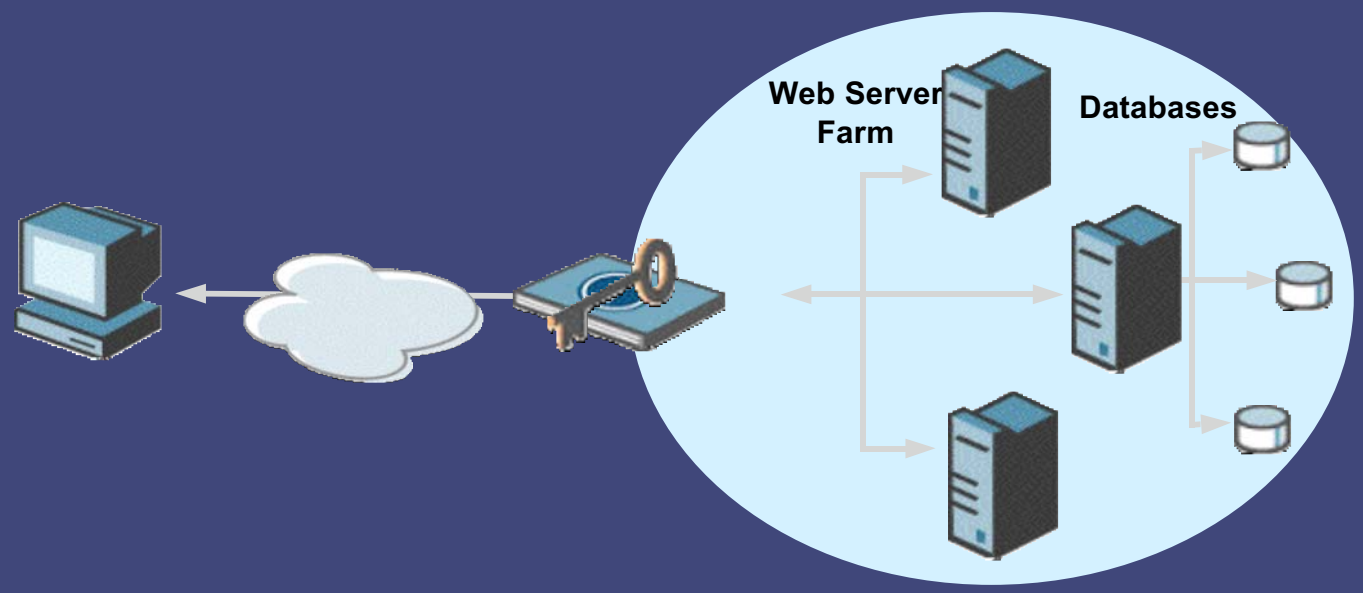
- Often done with ISAPI filters, or inline data encryption devices like Ingrian
- Encrypts and digitally signs cookies sent from Web server back out to client
  - Cookie contents are protected by the 3DES encryption
  - Cookie modification is prevented by the digital signature
- Cookies sent back by the client are verified by Ingrian before being sent to backend servers
  - If the Cookie data has been tampered with, the connection is terminated before going to backend servers
- Eliminates vulnerabilities of identity theft, eShoplifting, and other cookie poisonings

Microsoft Exchange Outlook Web Access Protection



1. Microsoft OWA client launches e-Mail application through the Internet
2. Ingrian Active Application Security platform negotiates secure SSL connection with client
3. Once connection is made, Ingrian Active Application Security platform running Netegrity SiteMinder Service Engine routes connection request to AAA Policy Server for authentication and authorization
4. Once authenticated, client gains access to e-Mail through the Exchange server
5. If the Ingrian Active Application Security platform is running Content Encryption Service Engine, selected sensitive e-Mail fields are further encrypted, even while stored in backend databases

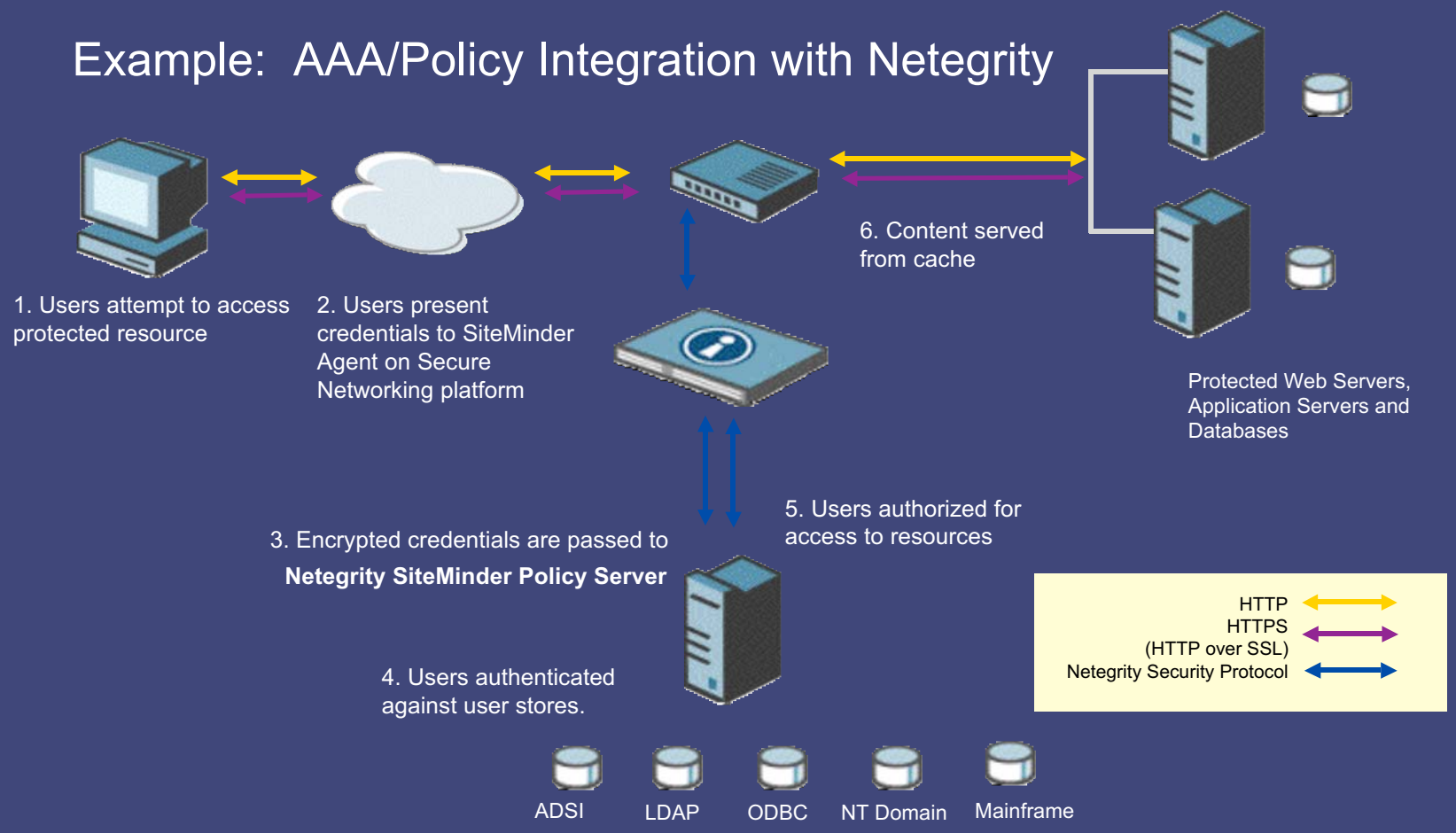
Solutions for Threat 3: Theft of Private Keys



- What to look for:
  - Private Keys always encrypted – never in clear text
  - Certified to FIPS 140-1 Level 2 and above
  - Secure configuration, backup and recovery
- Other vendors: nCipher, Compaq, IBM, Sun

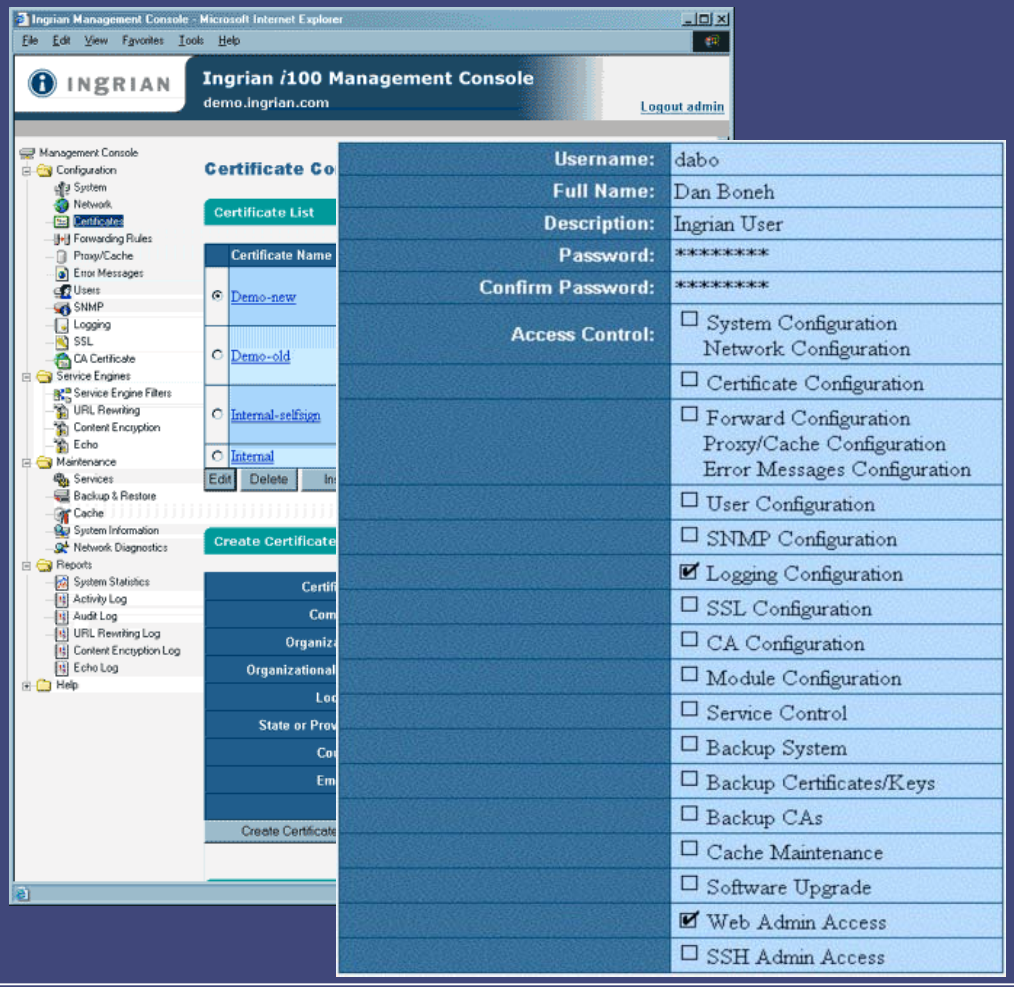
Solution for Threat 4: Unauthorized System Access

Example: AAA/Policy Integration with Netegrity



Solution for Threat 5: Administrative Errors and Abuse

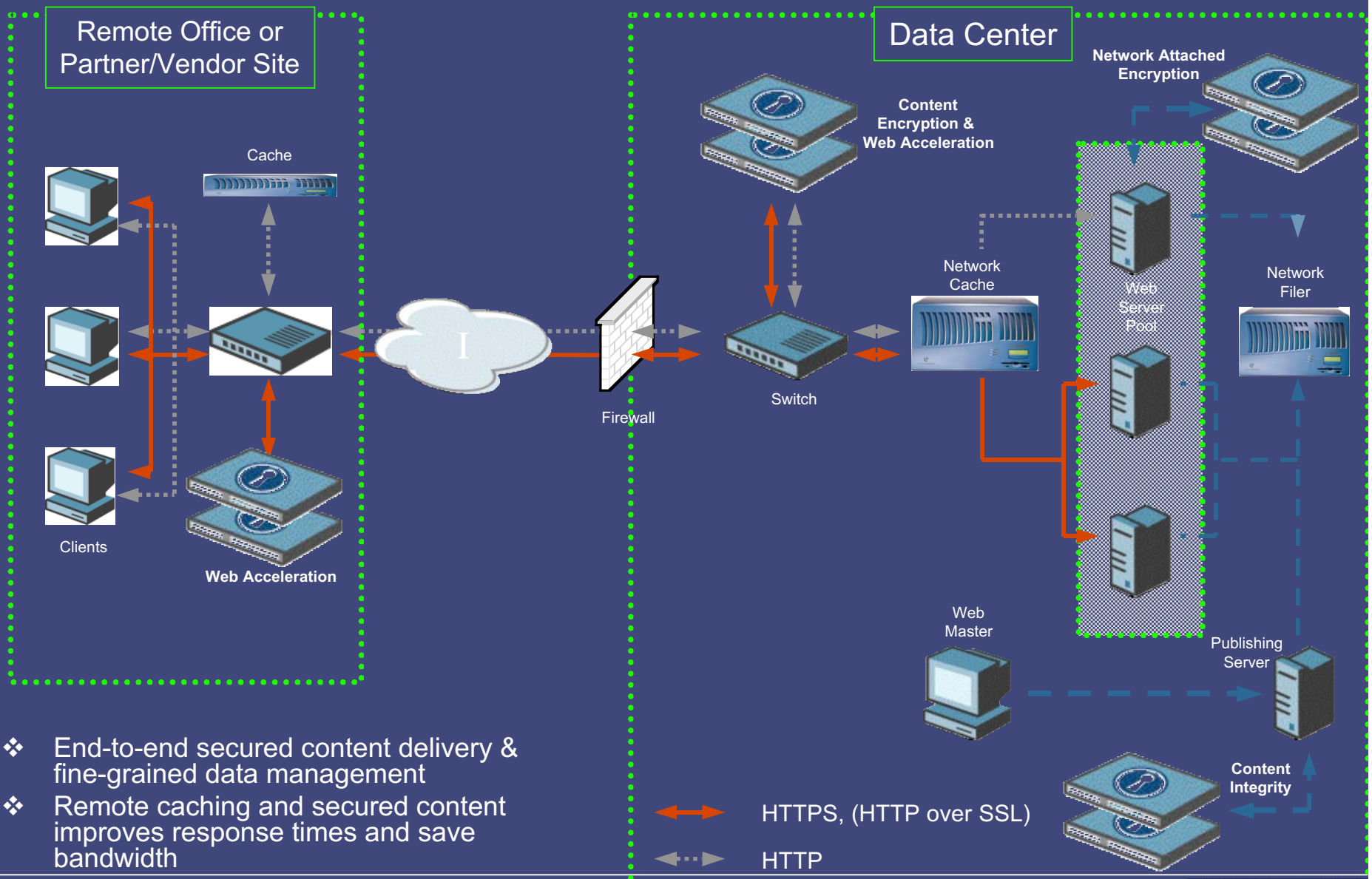
Example: Ingrian Management Console



What to look for:

- Intuitive GUI
- Ease-of-use to reduce configuration errors
- Full audit and activity logs
- Redundancy and Recovery mechanisms
- One-button addition of devices

Distributed Enterprise Data Architecture



- End-to-end secured content delivery & fine-grained data management
- Remote caching and secured content improves response times and save bandwidth

Selected Best Practices for Secure Network Management

- Keep security patches up to date
  - OS loads / updates like a router
- Encrypt stored sensitive data
  - No private keys may leave platform in the clear
- Encrypt data sent across open networks
  - SSL/TLS is not a solution by itself
- Assign unique ID to each person with computer access to data
  - Fine-grained management interface
- Track and audit access to data by unique ID
  - Ensure you 100% know and can track customers AND administrators
- Restrict physical access to nonpublic information
  - FIPS 140-2 L3 validation for protection of security context

Summary

- Creative new methods emerging for data privacy and security… leverage cryptography!
- Must always be concerned with storage AND transit of sensitive data to ensure privacy
- Authentication and authorization will play a key role going forward… look into “Single Sign On” solutions
- Intelligent auditing and administrative tracking expands
- Push hard on increased efficiency without compromising security or extensibility

Q&A

Questions & Comments Welcome!

Rod Murchison
rod@ingrian.com
Office: 650-261-2476