Change Management and Security for the Everyday SAN

AJ Casamento
Solutioneer, Brocade Communications

Who really needs change management or security?

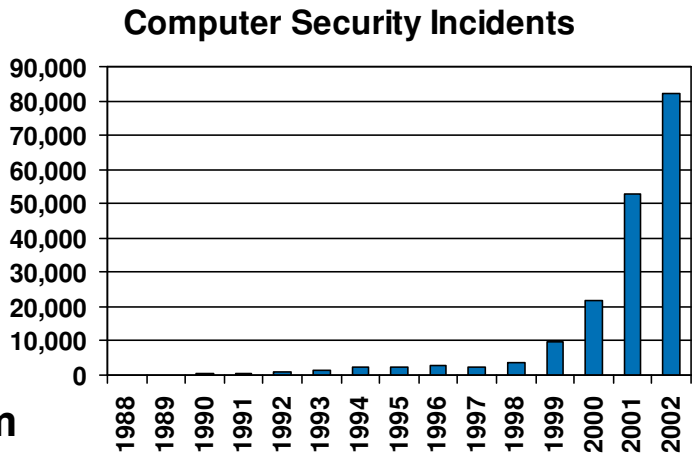
SAN and General Security Landscape

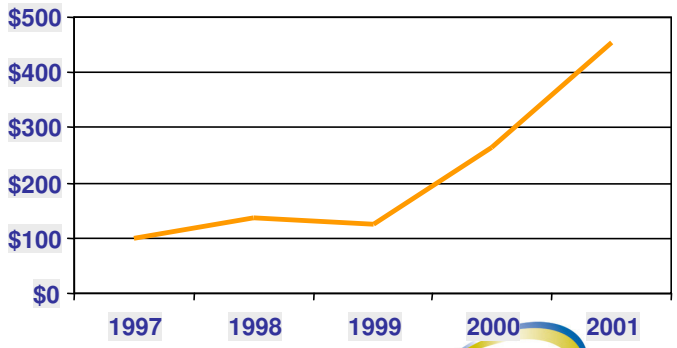
- **Storage Security became an essential aspect of customers' deployment strategies** *(Yankee Group, 2002)*

- **Security Threats are Growing in Numbers and Sophistication**
  (Source: www.cert.org/stats/cert_stats.html)
  - 2000 incidents = 21,756
  - 2001 incidents = 52,658
  - 2002 incidents = 82,094

- **Eighty percent of all network security managers claim their biggest security threat comes from their own employees.** *(Source Gartner, May 2002)*

- **The financial impact of security breaches has escalated dramatically**
  (Source: PWC\ASIS\U.S. Chamber of Commerce, 2002)
  - Estimated losses totaled $59 billion in 2001
  - Average cost per incident was $404,000
  - Greatest impacts were increased legal fees, company embarrassment, loss of revenue and competitive advantage.





Painful Examples

Dec 2002 - TriWest Healthcare

Stolen disks contained medical records on 500,000 military personnel

Jan 2003 – IBM Global Services

IBM notifies customer, Co-operators Life Insurance, that a disk containing personal and financial information on up to 180,000 customers is missing, presumed stolen

Feb 2003 – Visa, Amex, MasterCard

Hacker breaches 8 million credit card accounts through a third-party processor

Sep 2003 – Canadian Customs & Revenue Agency

CCRA loses unencrypted data on 120,000 Canadians in server theft from regional office. Leads to “literally millions of calls and checks within our system"

Jan 2004 – GMAC Financial Services

Stolen equipment containing customers' names, addresses, dates of birth, Social Security numbers, credit scores, marital status, and gender for over 200,000 customers

Painful Outcomes

July 2003
Ricoh Executives Bow in Apology
for Losing Backup Tape
with Customer Data

2003 Storage Market Survey

Theme: Flexibility, Data protection, and Cost control

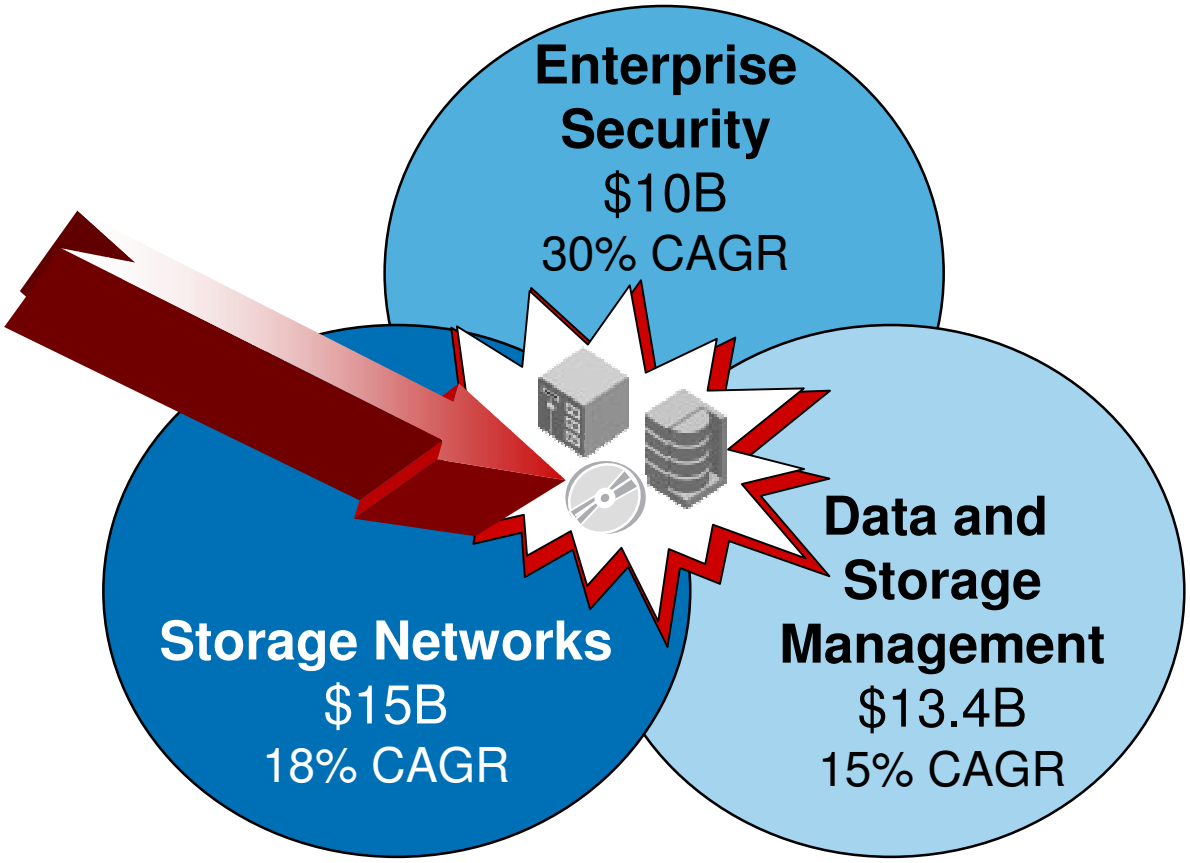
Cost	71%
Reliability	61%
Compatibility with existing systems	54%
Security	**54%**
Maintenance	51%
Scalability	41%
Interoperability	41%
Other projects have higher priority	20%
Recruiting talented employees to manage technology	19%
Integration of products from multiple vendors	17%

Source: *InfoWorld 2003 Storage Survey*

Why Secure SANs … Drivers …

- Security is a fundamental requirement for enterprise SANs, just like any other network
  - Many entry points into the SAN (users, devices, apps)
  - SANs interconnected over WANs / MANs (DWDM, SONET, IP etc.,)
  - SAN management applications
- SANs require change management controls (configuration integrity) to prevent disruption, network downtime, and improve availability
- New regulations and compliances
  - HIPAA (healthcare)
    - Health Insurance Portability & Accountability Act of 1996 (August 21), Public Law 104-191Act.
  - Graham-Leach-Bliley Act, Financial Modernization Act, November 1999
    - Financial Privacy, Protection of borrower data (encryption etc.)
  - Sarbanes-Oxley Act (Corporate financial integrity, January 2002)
  - California SB 1386 (Personal Information Breach Disclosure, July 2003)
- Multi-tenant environments have new security requirements
  - Security enables sharing of SAN resources among multiple customers securely
  - Reduces multi-tenant network infrastructure costs and enables economies of scale

Growth Opportunity



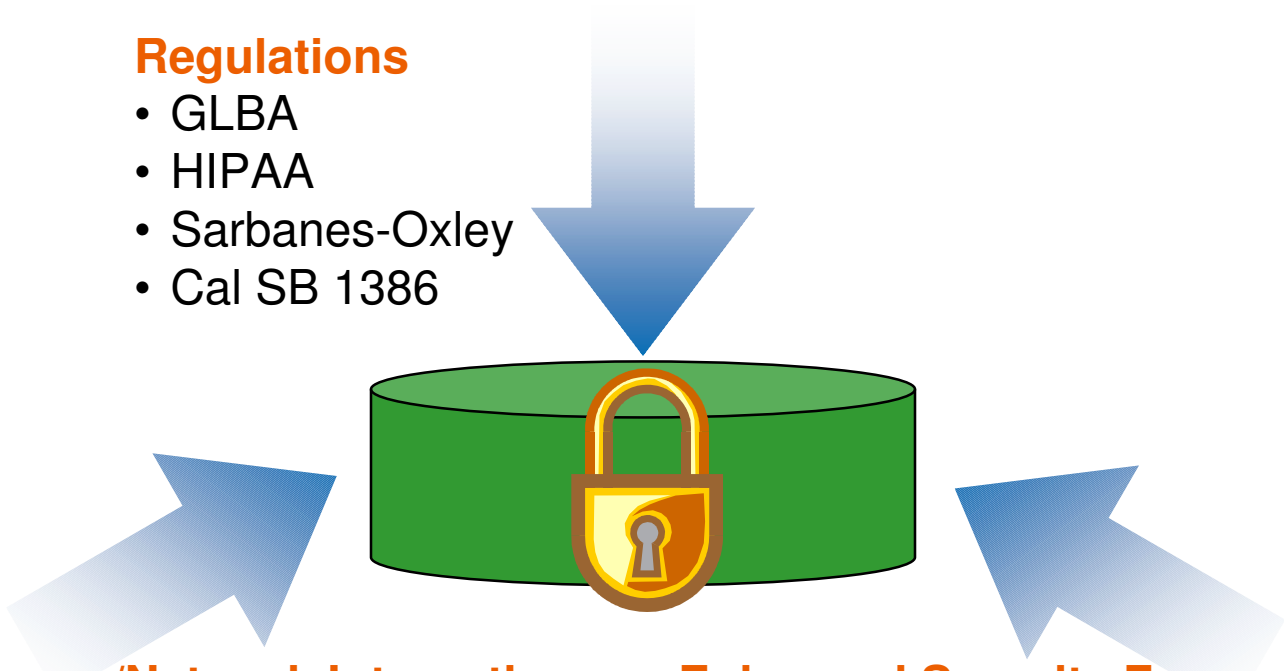
Storage Security Available Market $1B+ 2006*

*Estimates based on IDC Research Reports: #27477, #26380, #28144, #28584

What are the issues?

Storage Security Drivers

Regulations
- GLBA
- HIPAA
- Sarbanes-Oxley
- Cal SB 1386



Storage/Network Integration
- iSCSI
- FCIP
- Remote applications
- Data replication
- Distributed filesystems…

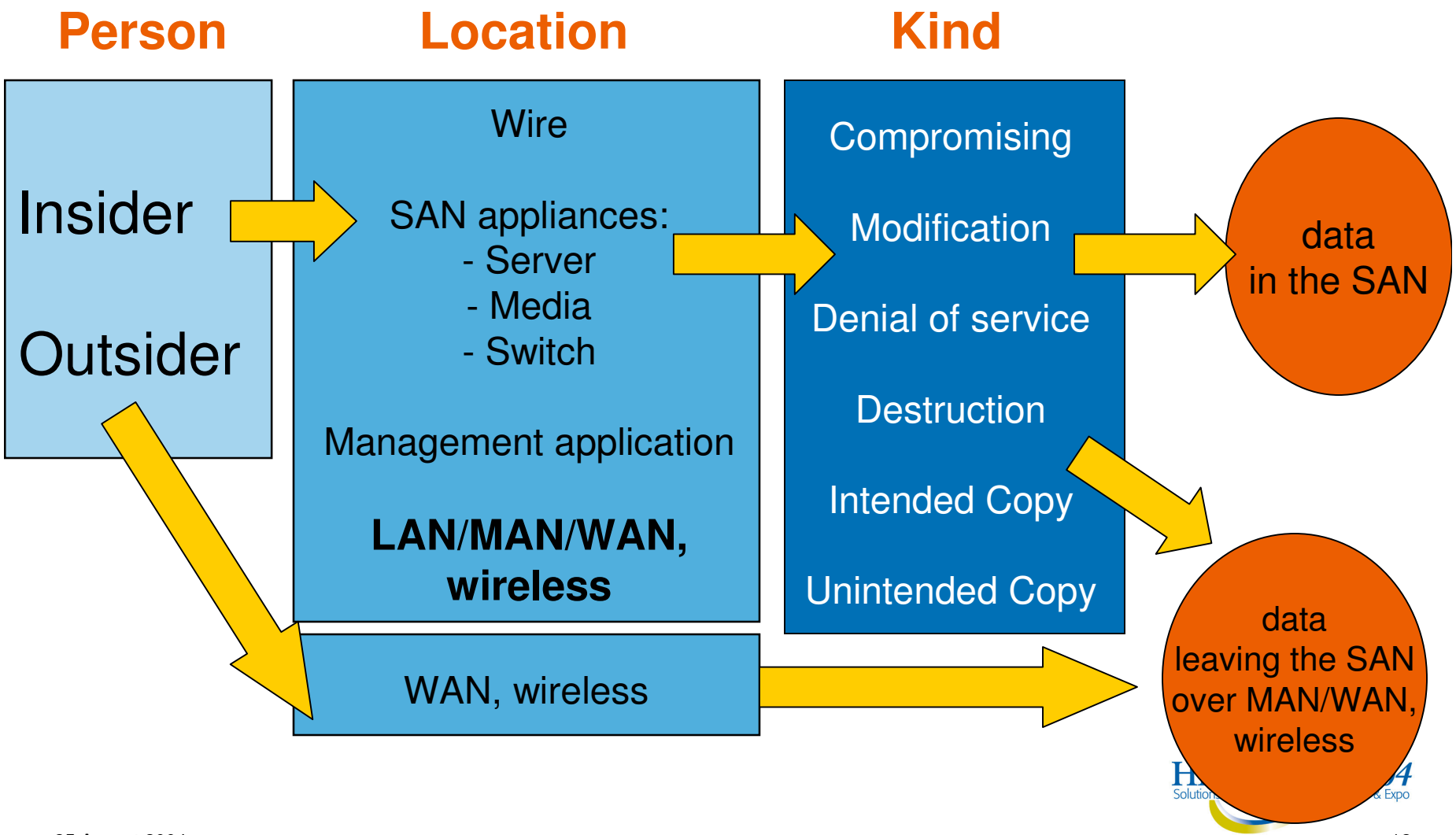
Enhanced Security Focus
- Application security
- Internet-based business processes
- Internal controls
- Intrusion prevention
- Growing staff and budgets
- Board Level participation…

HP WORLD 2004
Solutions and Technology Conference & Expo

Layered Security Model

- **Most attacks are internal!**
- **Down time caused by errors and poor change management controls**

Types of Threats
(ANSI T11.3 FC-SP & IETF IPstorage)

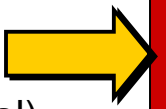


Level of Threats against SANs (ANSI T11.3 FC-SP)

- T11.3 Security Working Group has identified 17 threats
- Classification of possibility of appearance: High (1) , medium (15) , low (1)

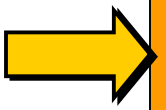
Persons

Insider & Outsider
(intentional or unintentional)



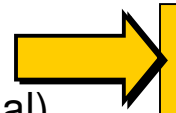
*** High: Use of management applications (Local, MAN/WAN, & wireless)

Insider and Outsider



** Medium: Use of server, switch and direct access to media

Insider
(intentional or unintentional)

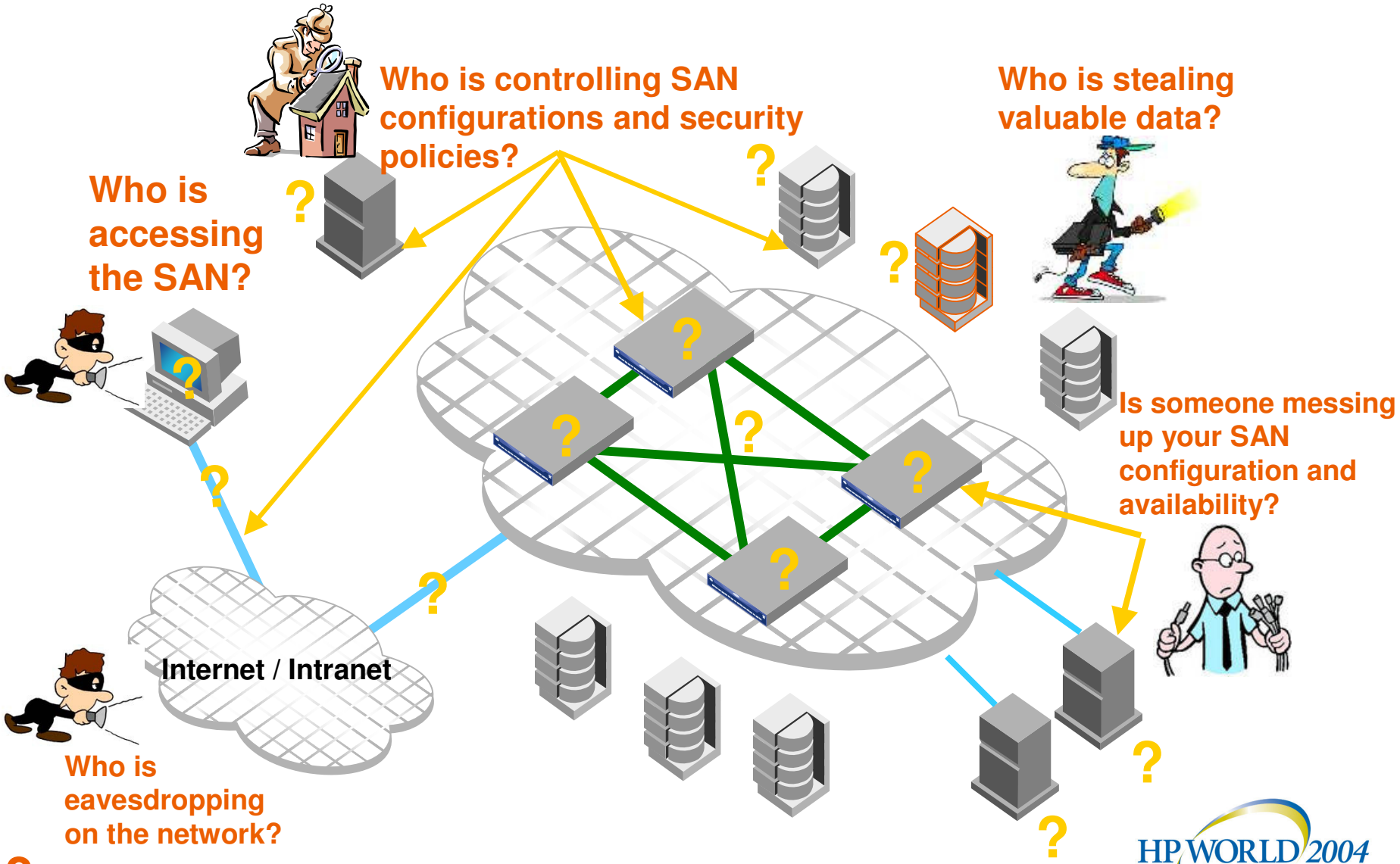


* Low: Direct access to the wire

What security problems are we addressing? Threats!

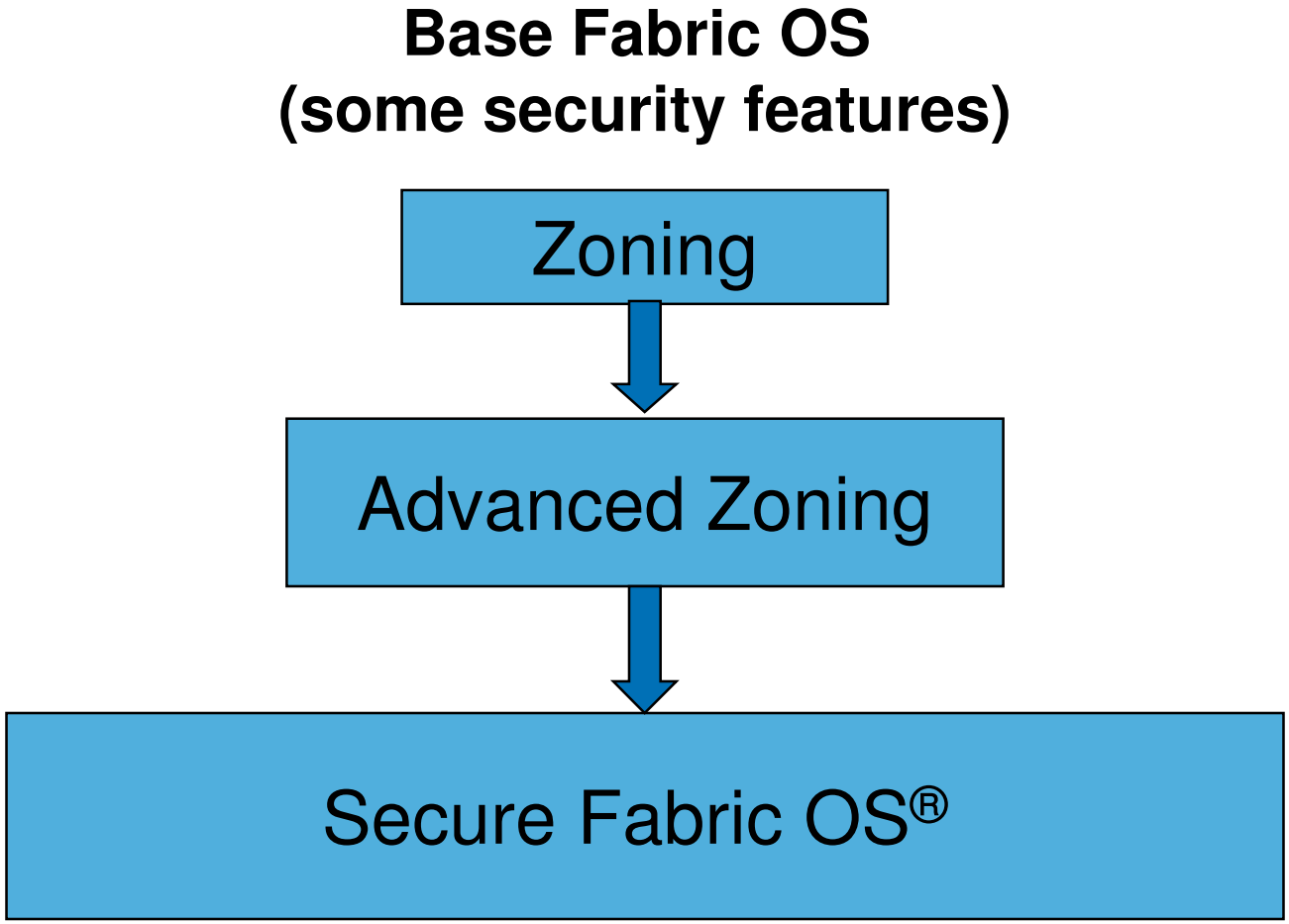
- Lack of adequate (or granular) administrator and user access control and authentication
  - Threats: The most common attack. Unauthorized access by individuals to sensitive data or SAN security parameters.
- Lack of strong or binding authentication and authorization among SAN devices (switches and servers)
  - Threats: IP or WWN spoofing. Masquerading. Unauthorized access by devices or other switches.
  - Unintentional changes, errors, and misconfigurations - network disruptions
- Inadequate controls and granularity in SAN Management access and security policy distribution
  - Threats: Management access from uncontrolled sources. Denial of Service (DOS) attacks through open management ports.
  - Unintentional changes, errors, and misconfigurations– network disruptions
- Lack of privacy for sensitive management data such as passwords as well as files etc.
  - Threats: Eavesdropping. Ability to view or intercept sensitive data such as passwords or data files.

How secure is your SAN?



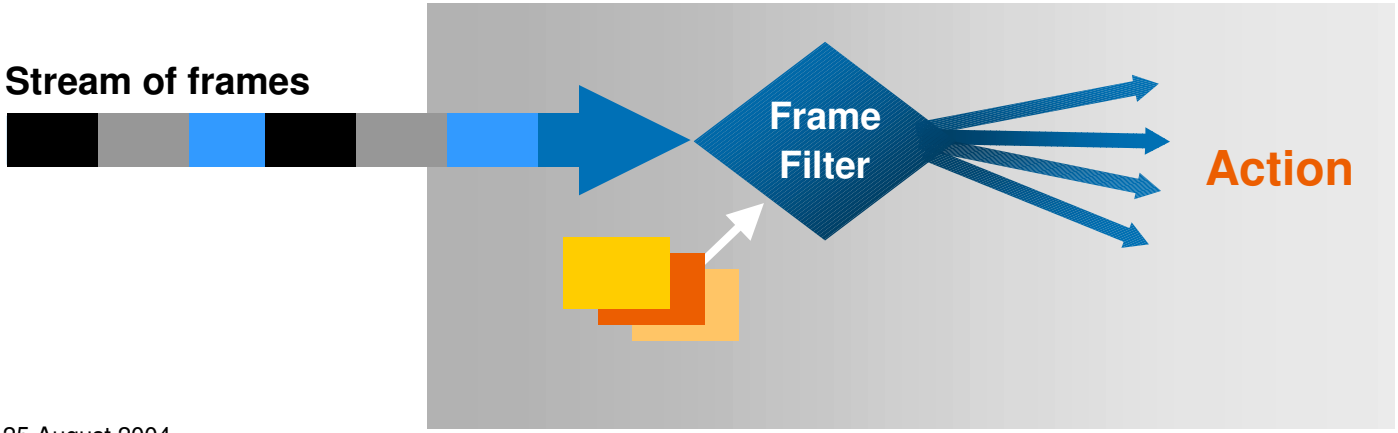
What does HP bring as a solution?

HP Enterprise-Class Security



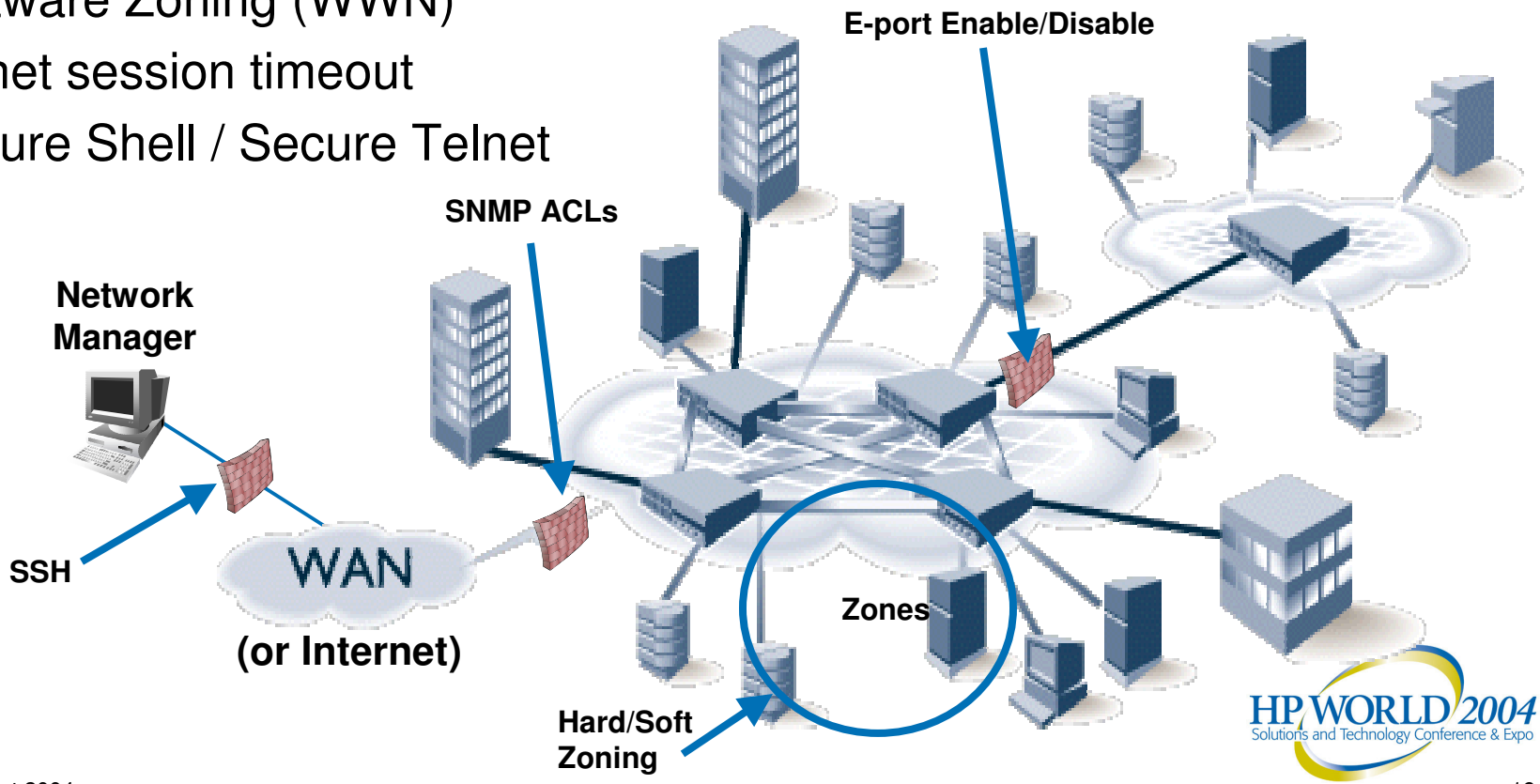
Advanced Zoning - Hardware-Enforced Port and WWN Zoning

- It Starts with Intelligence in the ASIC…
- Zoning tables are loaded directly into the ASIC
  - Intentional or accidental WWN changes on the HBA will not fool the system
- No reliance on the Name Server for zoning information
- Unauthorized frames are rejected at the destination port
- "Blocked vs. unlisted phone number…"



Security Features in the Base Fabric OS Today

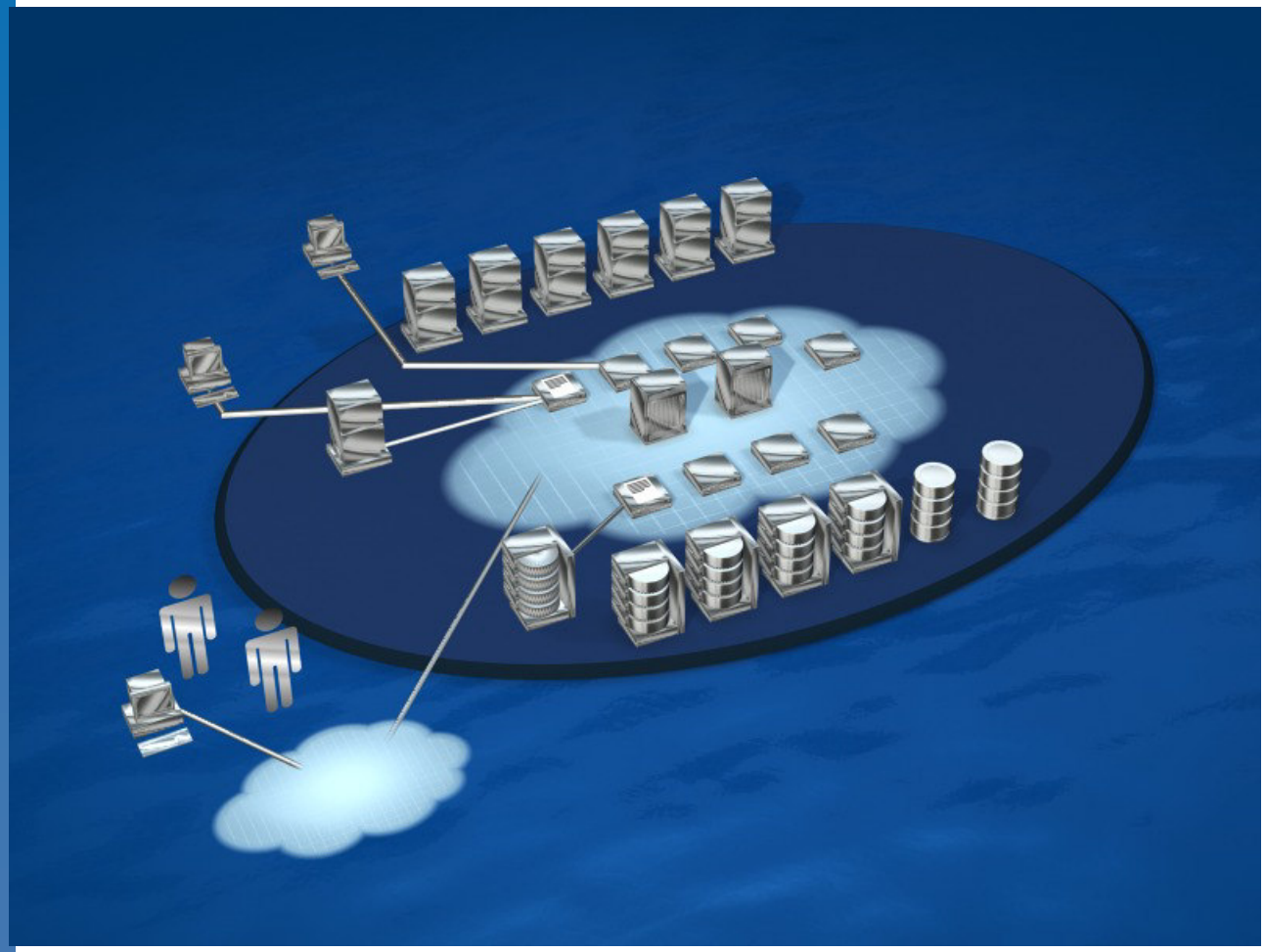
- SNMP / MGMT SRVR ACLs
- E_Port enable/disable
- Hardware-Enforced Zoning (Port and WWN)
- Software Zoning (WWN)
- Telnet session timeout
- Secure Shell / Secure Telnet



Introducing Secure Fabric OS

- Brocade Secure Fabric OS is a licensed software product that provides a complete set of security capabilities within Brocade fabrics.
  - Centralized security management (trusted switches)
  - Fabric-wide security policies to control all access and to maintain 'configuration integrity'
    - Port level access control
    - Switch level access control
    - Management access controls (Telnet, SNMP, HTTP, API, Serial port etc.)
  - Encryption of management data such as passwords and logins (Secure Telnet, Secure Shell)
  - Strong and non-repudable authentication between switches (using digital certificates and signatures)

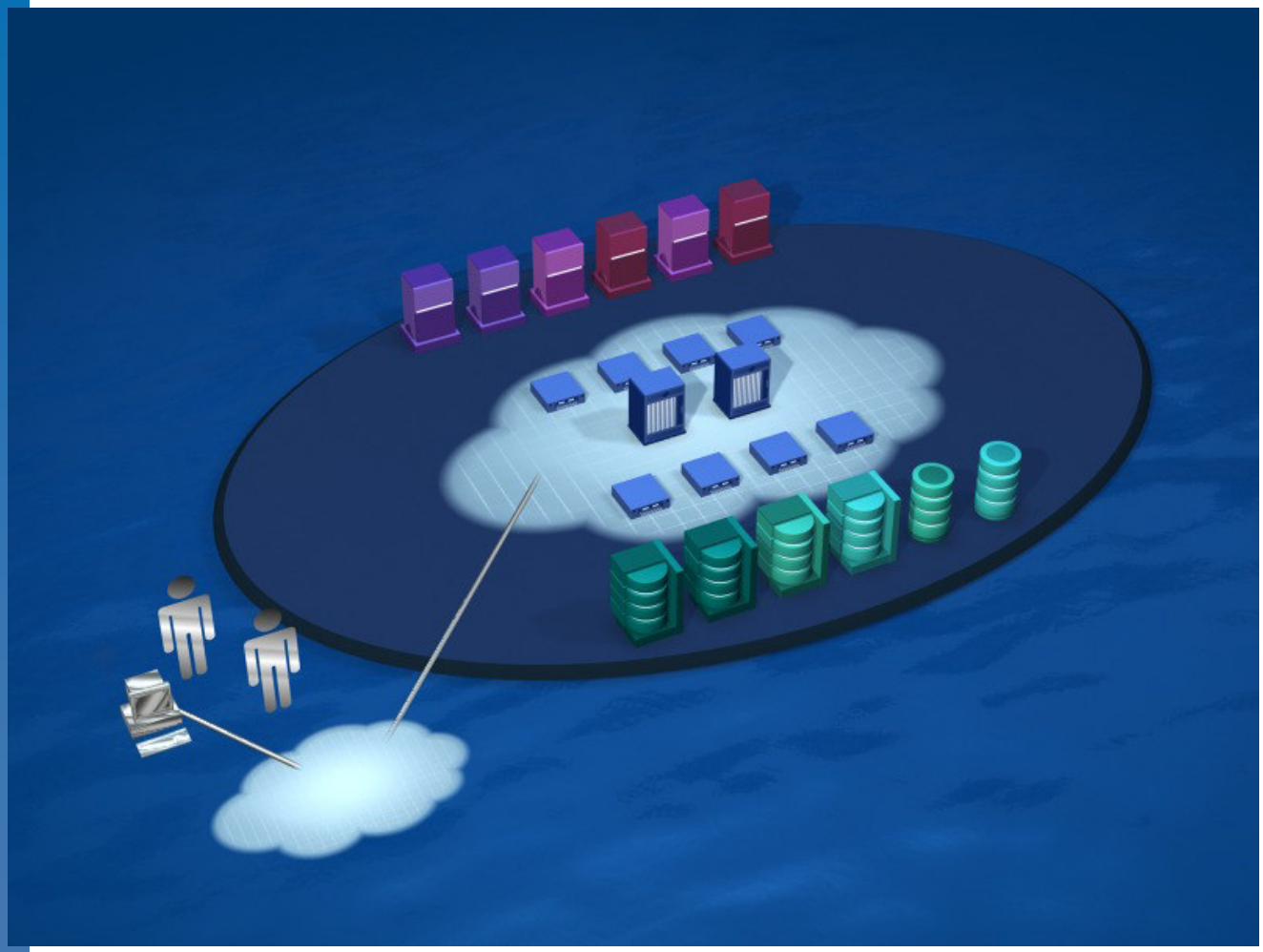
HP Secure Fabric OS Provides …



- Comprehensive *fabric* based security
- Assured Configuration Integrity
- Active Change management
- Protection from unauthorized access, loss or corruption
- Reduced system downtime
- Strong Authentication and Access Control
- Policy-based Management

HP Secure Fabric OS

Management path encryption ensures secure access to your SAN

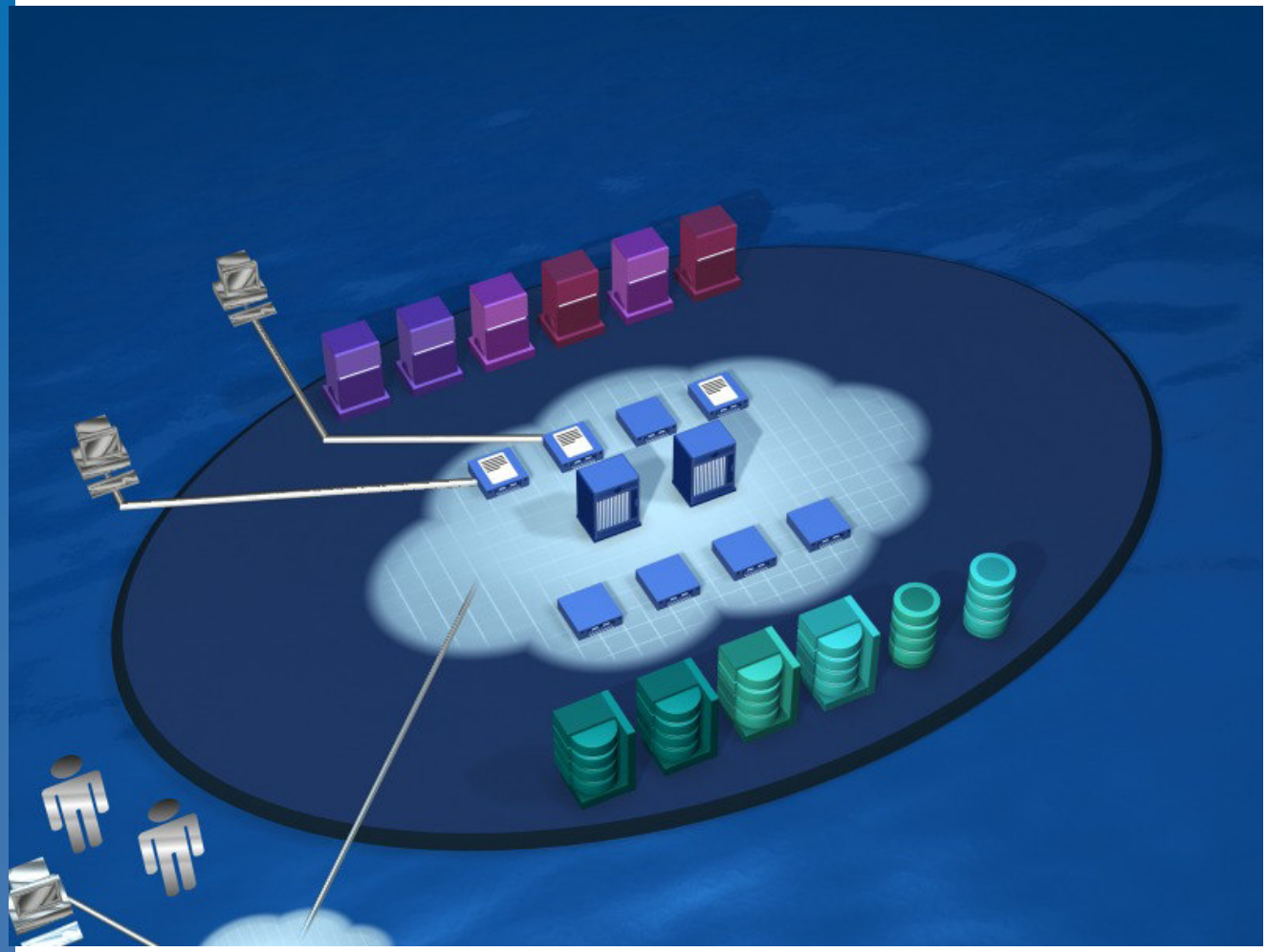


- Secure Management Communications *Channels*
- Encryption of Admin IDs and passwords
- Protects passwords over public or internal networks
- Secures unprotected log-ins to the SAN
- Prevents Eavesdropping on sensitive data

HP WORLD 2004
Solutions and Technology Conference & Expo

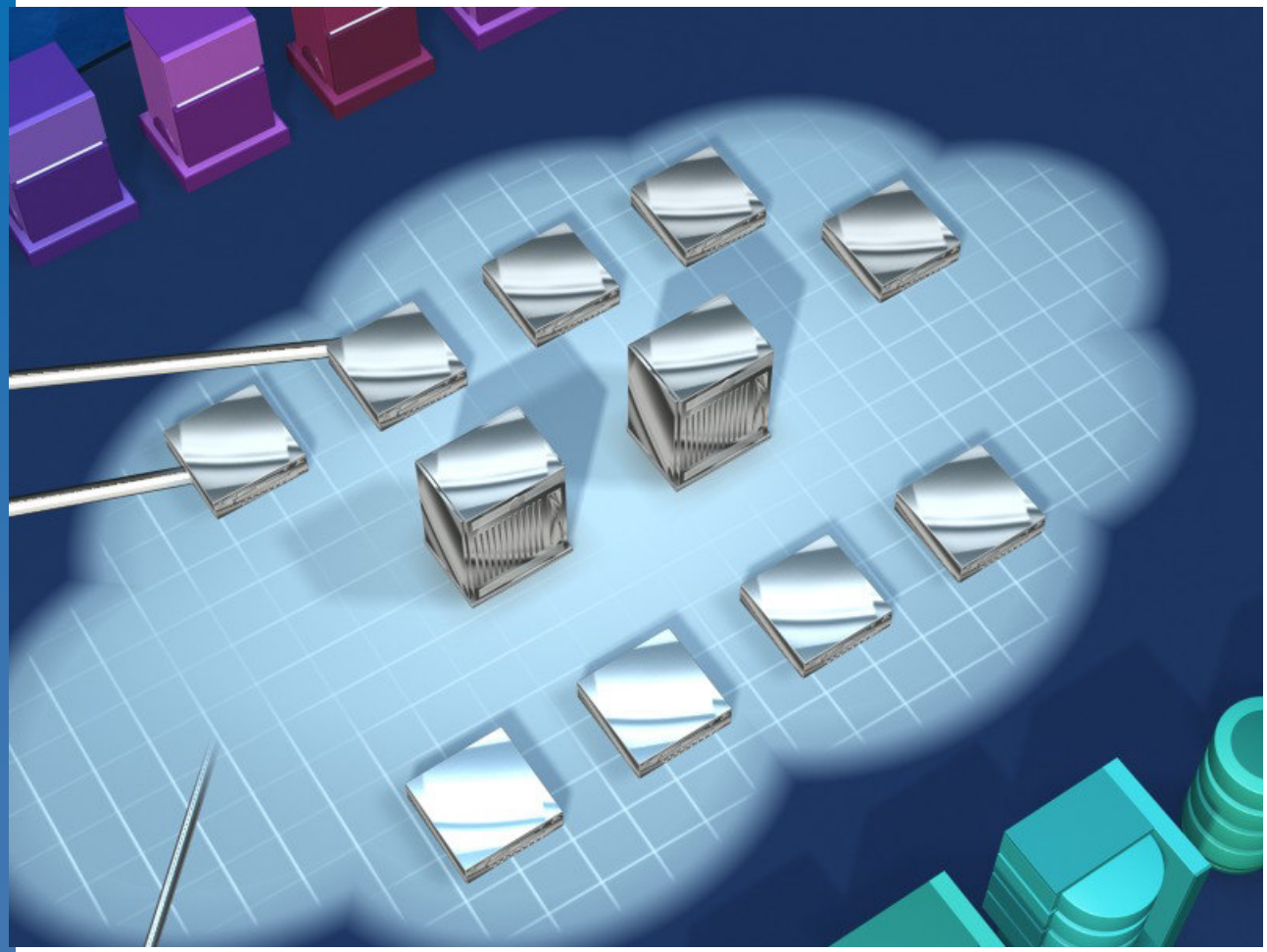
HP Secure Fabric OS

Control management and administrative access



- Management ACLs control access to the fabric from different sources
- Policy-based Infrastructure with centralized control
- Passive or active control allowed to admins

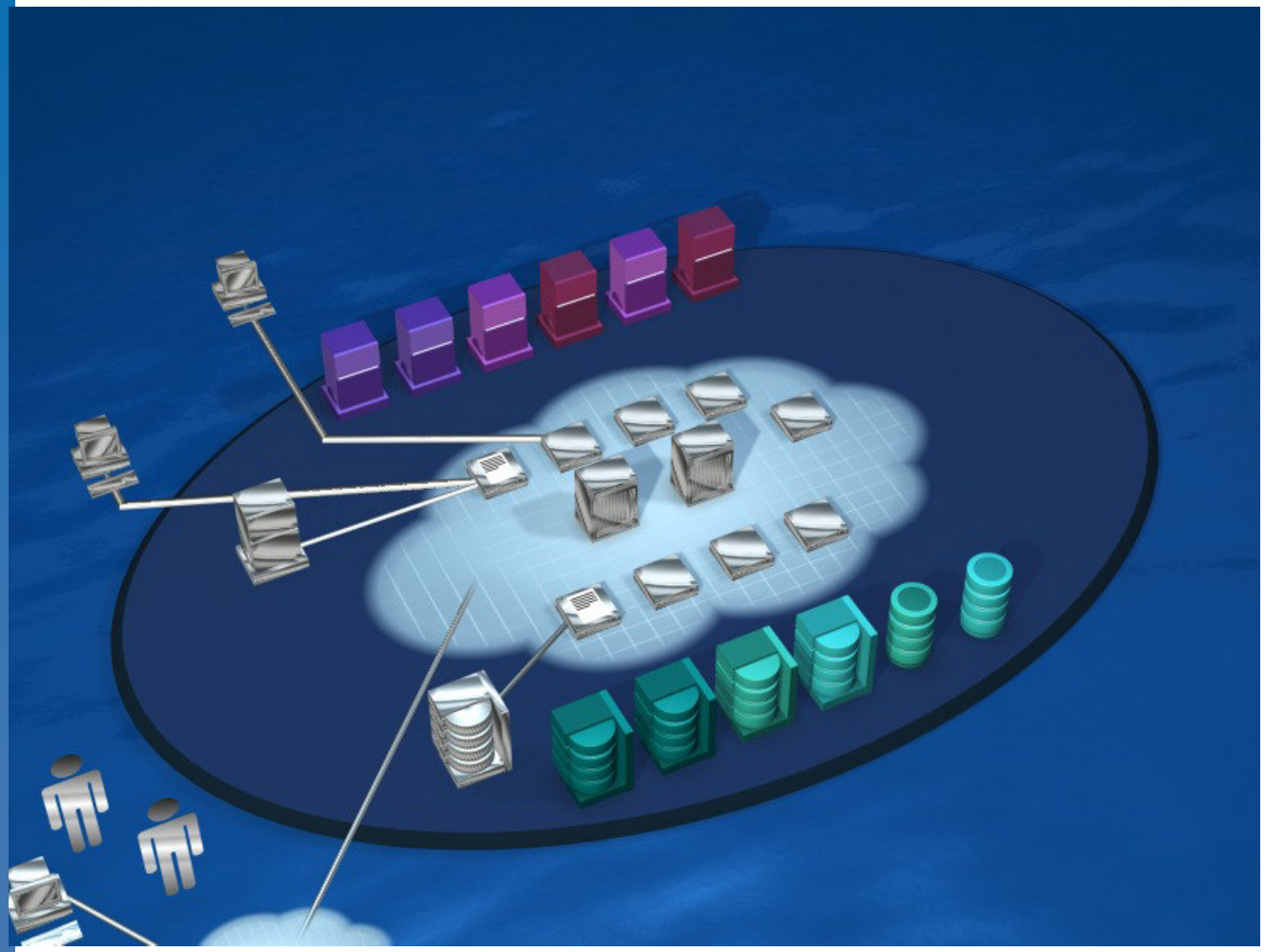
HP Secure Fabric OS
Authenticate switches and infrastructure



- Digital certificates within the switch provide the strongest authentication for new switches
- Ensure a new switch is authorized to join the fabric

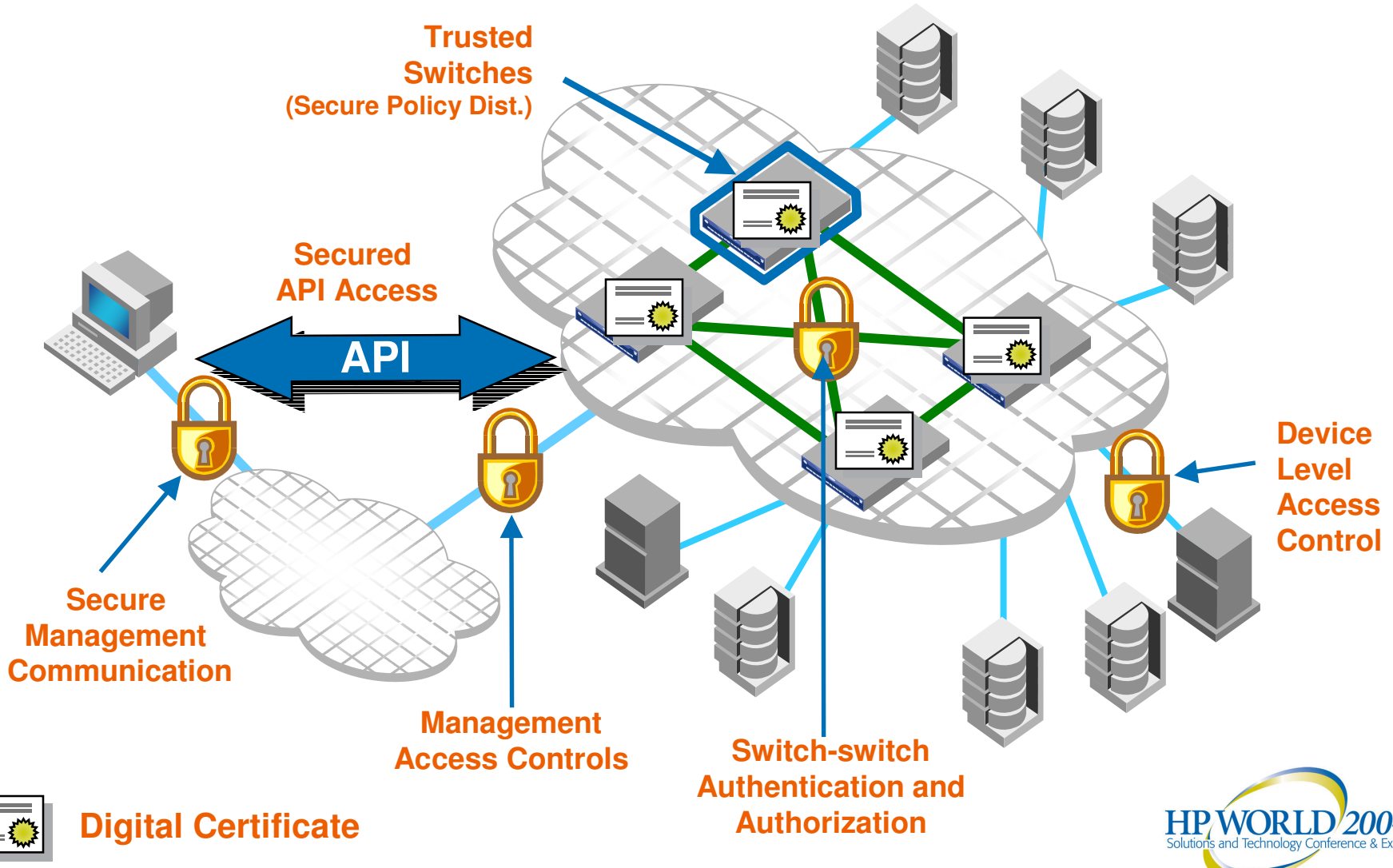
HP Secure Fabric OS

Assure configuration integrity and change management



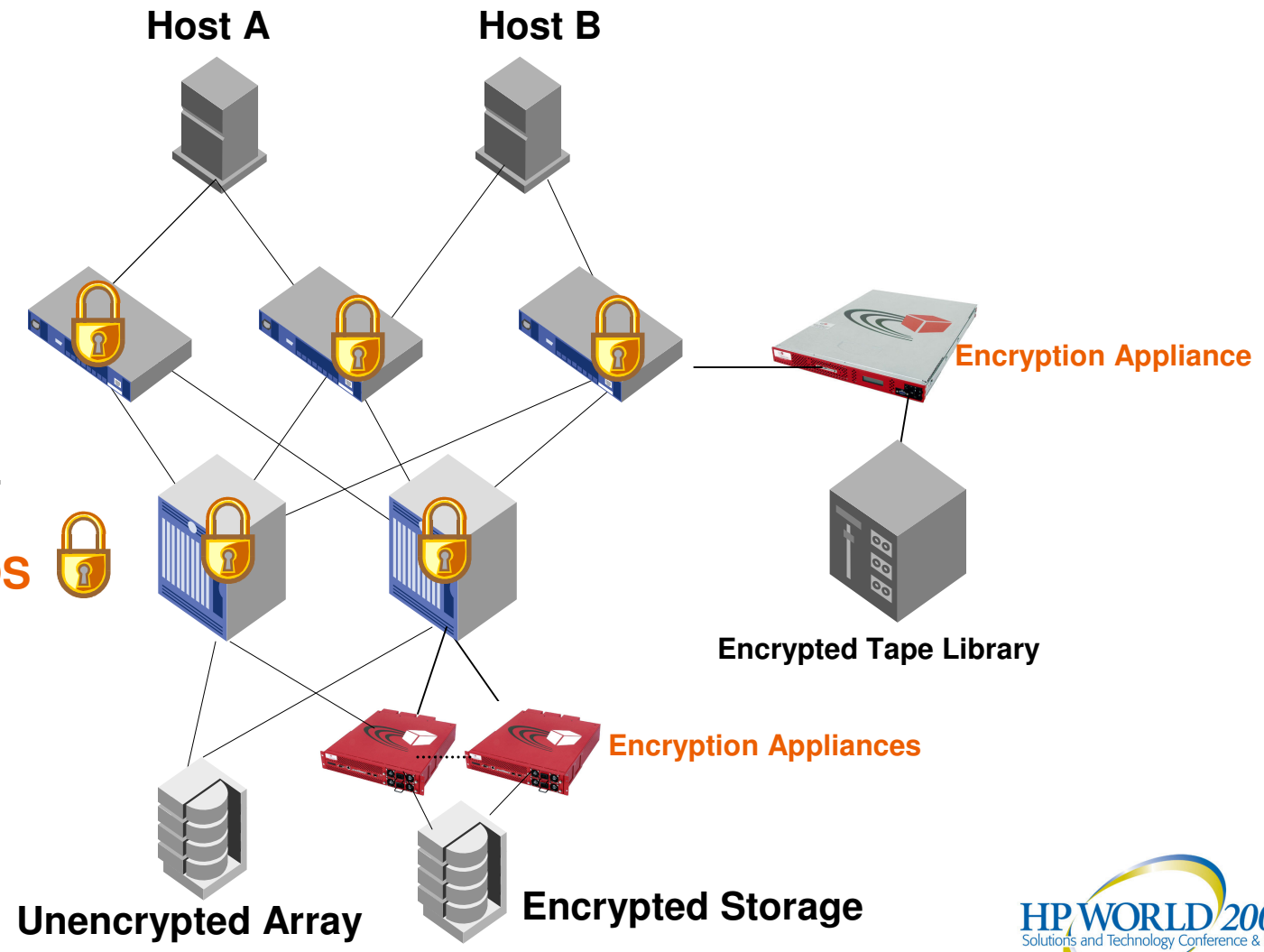
- Device connection controls (port levels ACLs)
- Port-level access policies tightly control server access to the fabric
- Access Control Lists lock Hosts/Servers by WWNs to specific physical ports

HP Secure Fabric OS, Securing The SAN infrastructure

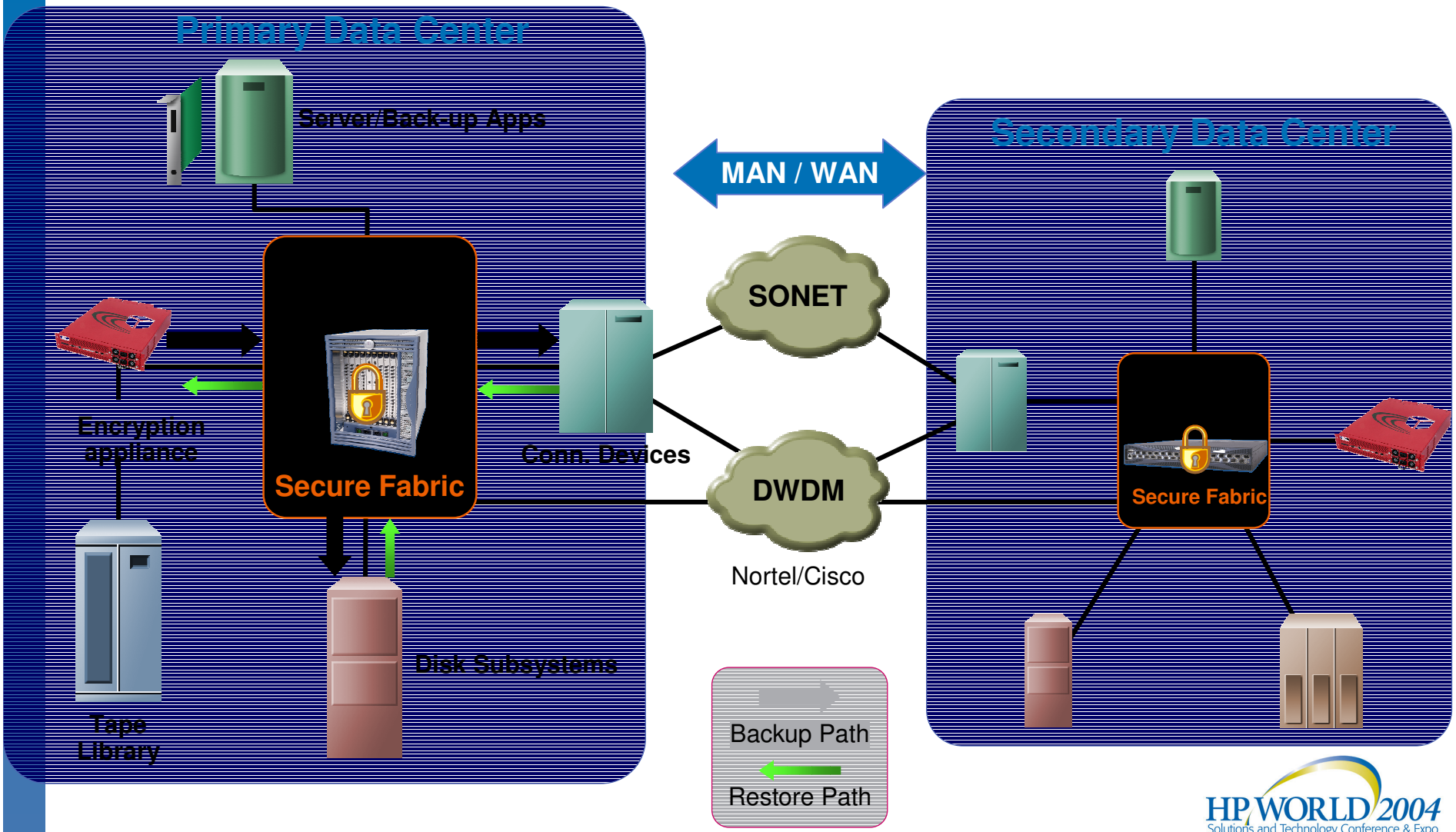


HP Secure Fabric OS and Encryption Appliances for Data Content Security

HP B-Series 2x3
Core-edge fabric.
With
Secure Fabric OS

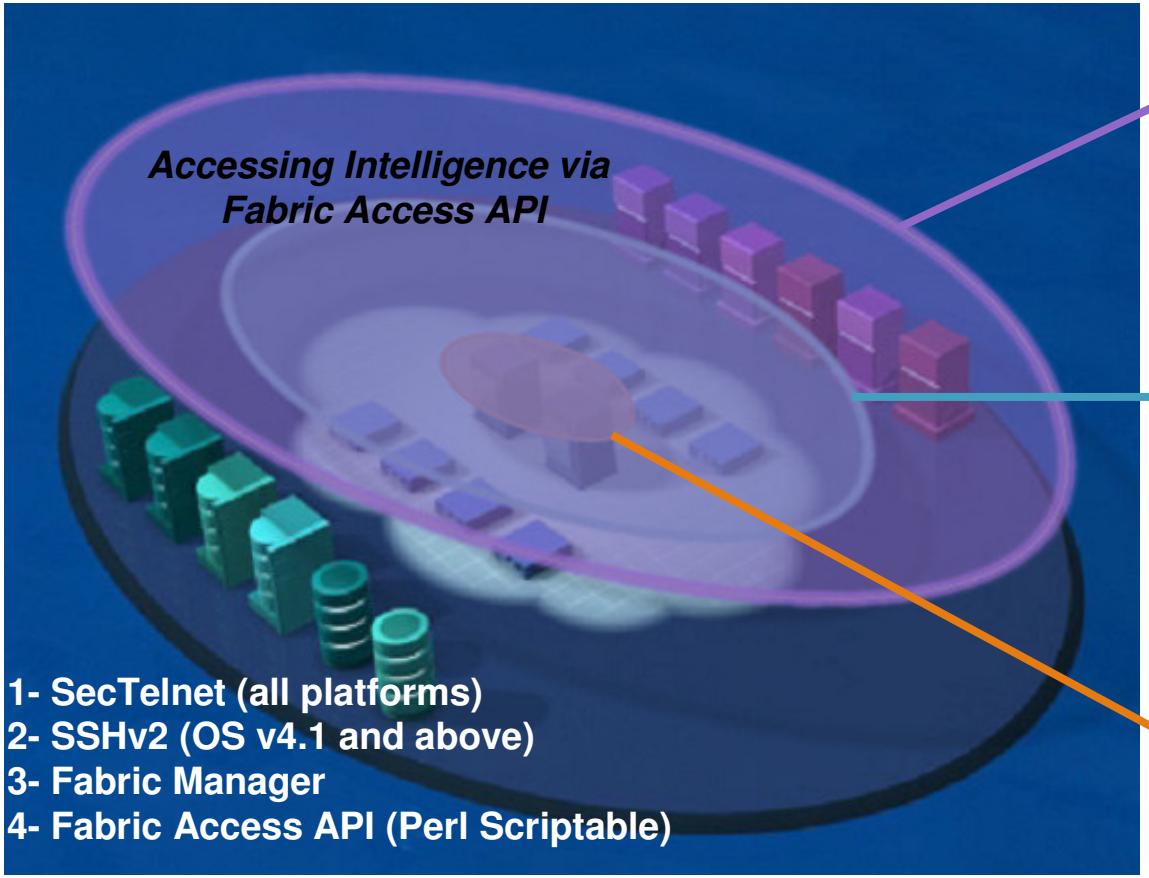


Secure Tape Backup and Recovery



Manage Security

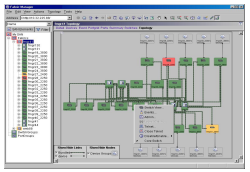
Integrated Fabric Management Applications



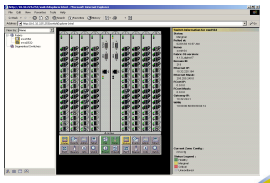
3rd Party Applications

hp invent
Computer Associates
EMC²
CreekPath SYSTEMS
INTERSAN Pioneering Storage Area Management
Sun microsystems
IBM
VERITAS

Fabric Manager

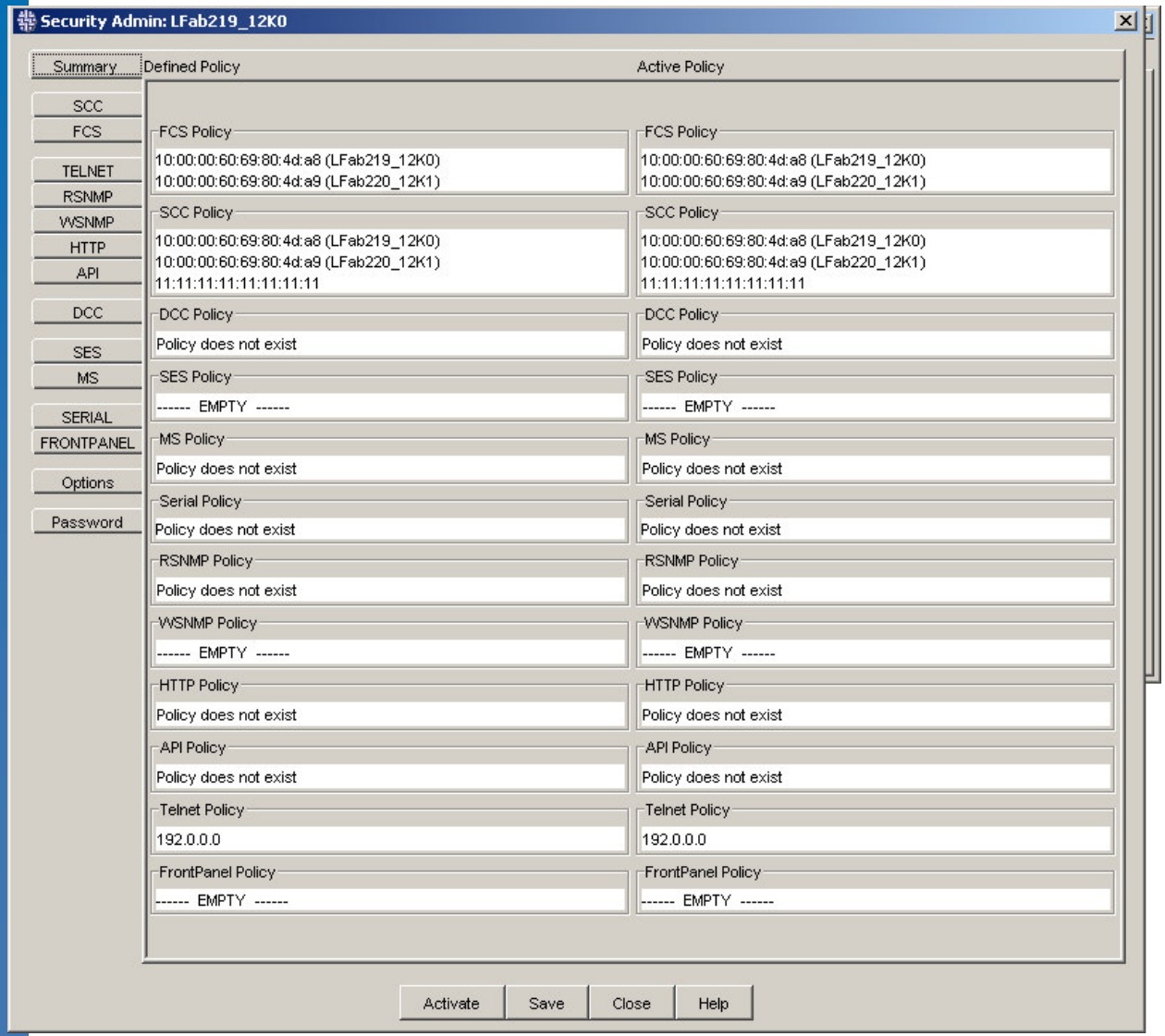


Command Line



HP WORLD 2004
Solutions and Technology Conference & Expo

Fabric Manager - Security Policy Administration



- **Secure Fabric OS management**
- **Security Policy control**
- **Security audit & reporting**
- **Multi personality (manage secure & non-secure Fabrics from a single console)**

Security/Cryptographic Mechanisms in HP Secure Fabric OS

Authentication:

- Fibre Channel Authentication Protocol (FCAP) – PKI-based security
  - Switch Link Authentication Protocol (SLAP) – subset of FCAP
  - Protocol used to authenticate switches (E_Ports) within a fabric

Privacy:

- RSA Public Key Encryption (1024-bit keys) as well as Secure Shell (SSH)
  - For encrypting passwords between the manager and the switch
  - MD-5 for hashing passwords within the switch
- Advance Encryption Standard (AES)
  - For encrypting the switch's private key used in digital signatures and password encryption/decryption processes

Integrity:

- Digital signatures on security parameters distributed from the FCS (trusted switch)

Non-Repudiation:

- RSA digital signatures
  - For authentication of switches
  - SHA-1 hash algorithm for the signature process
  - ITU X.509 v3 certificates

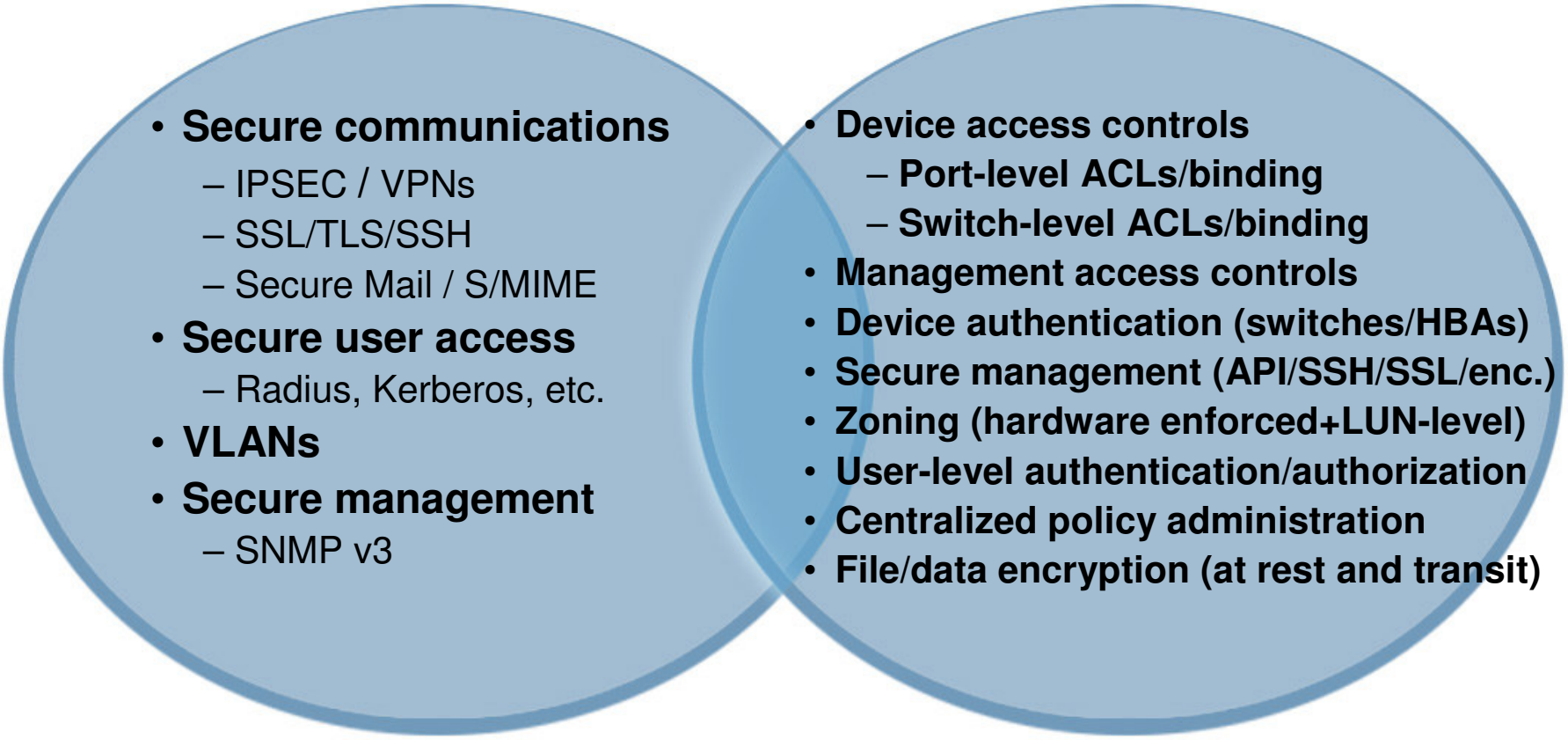
Access control:

- Comprehensive policies to control management and device access to the fabric

Fabric Security Architecture (ANSI T11.3 FC-SP)

Confidentiality	ESP (Encapsulating Security Payload)
Integrity	Policy Distribution (Signatures / HMACs / ESP)
Authorization (Access Control)	Fabric Asymmetry / Fabric-wide Security Policies (ACLs)
Authentication	FCAP // FCPAP // DH-CHAP
Security Infrastructure	PKI // Password Administration // Shared-Secret Administration

IP vs. SAN Security



Some overlap, but there are unique requirements!

Security Roadmap, Summary

- **Next Secure Fabric OS Release**
  - Non-disruptive SecMode Enable (3.x, 4.x)
  - SNMP V3 (in base OS)
  - SSL / HTTPS (in base OS)
  - SCP (SecureFTP) (in base OS)
    - Encrypt config upload/download – Encrypt image (later)
  - RADIUS integration – Fabric admins authenticated through RADIUS (in base OS)
  - Addition of authentication using DH-CHAP (Switch-switch only)
  - Additional admin accounts (more role based access controls)
  - Secure Fabric OS support across various SAN gateways
  - Usability enhancements (Mem increase, FM config wizard, CLI lock down command, keep password option..)
  - Continued switch hardening / threat analysis

Thank You!