



# Securing Your SAN



**Bob Nusbaum**

**Software Product Line Manager, Cisco Systems**

# Weave in Messages

- Services Oriented SAN
- Unified I/O
- Investment protection w/ FCoE & 16G roadmap

# Why Is SAN Security Important?

- Governments have enacted a variety of strict **security regulations mandating the privacy and integrity of sensitive customer and corporate data**
  - Health Insurance Portability and Accountability Act (HIPPA)
  - Gramm-Leach-Bliley Act (GLBA)
  - Payment Card Industry Data Security Standard (PCI DSS)
  - Sarbanes-Oxley Act (SOx)
  - European Privacy Directive
  - CA SB1386
- Many of the regulations and legislation require **'countermeasures against internal and external threats'**

# Securing Fibre Channel

- **'FC Zoning'** introduced to provide segregation between Storage devices
- **'Port Mode Security'** introduced to prevent edge ports coming up as ISLs
- **'Port Security'** / **'Port Binding'** introduced to help protect against WWN Spoofing
  - Locking WWNs to specific ports
- **Virtual SANs** (VSANs) introduced to provide segregation between (virtual) fabrics
- **FC Security Protocol** (FC-SP) is the final step required to secure FC
  - Device authentication, per message secrecy and integrity protection, policy management

# Securing Storage Management

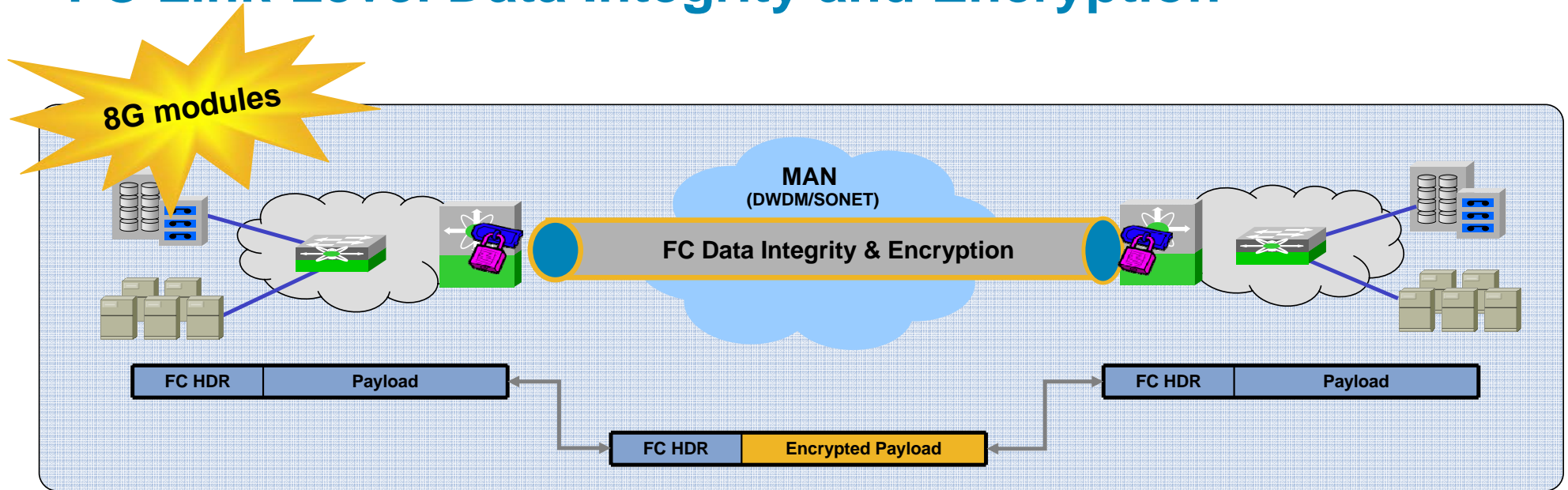
Storage Management Security includes:

- Authentication, Authorization and Accounting (AAA) of management actions
  - RADIUS/TACACS+
  - Syslog
  - SNMP Traps
  - Call Home (SMTP)
- Role-based management access control
- Secure transport of management actions
  - SSH, SNMPv3, SSL/TLS
- Access control to management interfaces
  - Secure design of the network management module
- Consistent Security Policy across all devices

# IP Storage Security: FC-over-IP (FCIP)

- FCIP allows for interconnection of SAN islands via IP networks
  - The FCIP standard doesn't provide for any in-band security mechanisms
  - Per message origin authentication, integrity, anti-replay protection, and privacy are provided, where required, by independent IPsec tunnels
- FCIP tunnel is a virtual ISL—can leverage existing FC Fabric security mechanisms
  - FC Port Security
  - FC-based FC-SP DH-CHAP switch-to-switch authentication

# FC Link-Level Data Integrity and Encryption



- Preserve integrity and confidentiality of FC traffic over MAN
- Integrated, high performance functionality
- No change to existing SAN, enable functionality only on edge switches

# Encryption Solutions

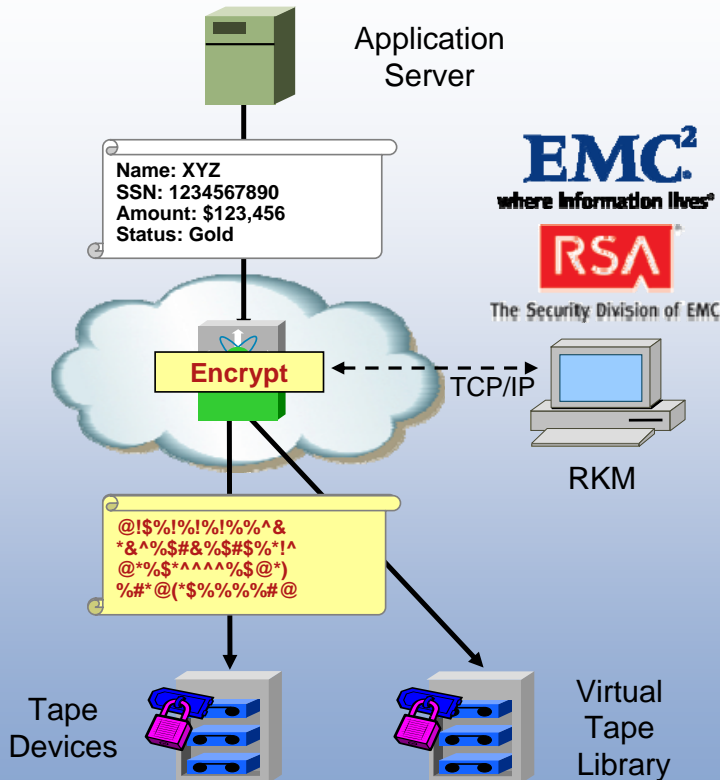
- **Host / Software Based**
  - Keys stored on database or application servers where data resides
  - CPU Intensive
- **SAN Appliances**
  - Scalable by adding more appliances
  - Rewire and reconfigure SAN ports and zoning
- **Tape Drives**
  - High Performance
  - New Drives and possibly new media needed
  - Could be costly
- **Fabric Based**
  - Ease of installation
  - Scalable
  - Integrated with Key Management Solutions

# Delivering Encryption as a SAN Service



1. Insert Cisco MPS-18/4 modules or MDS 9222i switches
2. Enable Cisco SME and setup encryption service
3. Provision encryption for specific storage devices

# Cisco SME – Secure, Integrated Solution

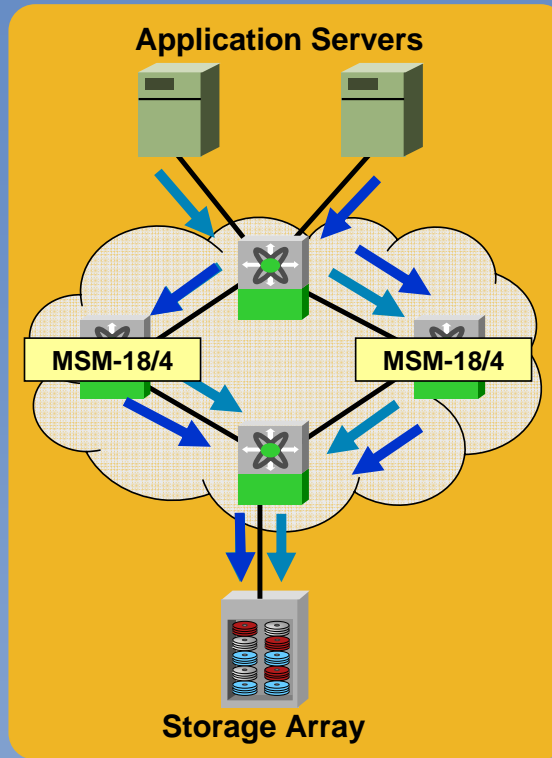


- Encrypts storage media (data at rest)
  - Strong, Std. IEEE AES-256 encryption
  - Integrates as transparent fabric service
  - Handles traffic from any virtual SAN (VSAN) in fabric
- Supports heterogeneous, SAN attached tape devices and virtual tape libraries
- Includes secure key management
  - Open API integrates with enterprisewide, lifecycle key managers, including RSA
- Compresses tape data
- Allows offline, software only media recovery

# Summary



Security



Services-Oriented SANs



Investment Protection

Learn More:  
[www.cisco.com/go/datacenter](http://www.cisco.com/go/datacenter)





**CISCO**