SAN SECURITY OVERVIEW

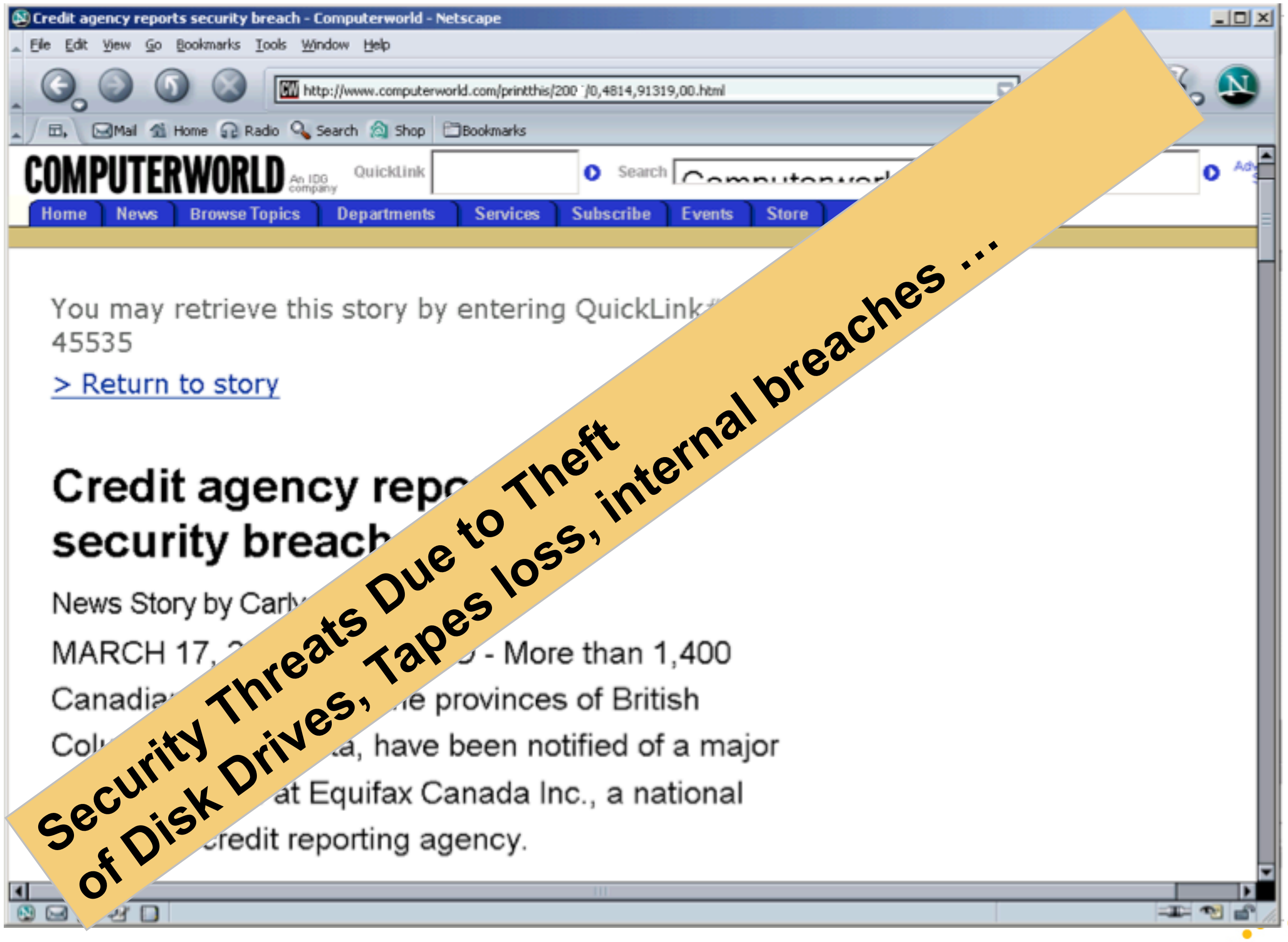
Session # 9316

Tony Almeida
Consulting Systems Engineer
Cisco Mainframe Solutions
talmeida@cisco.com

Session 9316 Abstract

Security is a major concern in all aspects of the Enterprise. As the technology continues to evolve, it is important to review all of the technology. SAN Security will be discussed in the following areas: encryption of data in flight, encryption of data at rest, access control security and other areas of potential interest.

Security breaches – real threat


Credit agency reports security breach - Computerworld - Netscape
File Edit View Go Bookmarks Tools Window Help
http://www.computerworld.com/printthis/200 /0,4814,91319,00.html
Mail Home Radio Search Shop Bookmarks
COMPUTERWORLD An IDG company
QuickLink
Search
Home News Browse Topics Departments Services Subscribe Events Store

You may retrieve this story by entering QuickLink# 45535

> Return to story

Credit agency repo security breach

News Story by Carly

MARCH 17, 2 - More than 1,400 Canadia e provinces of British Col a, have been notified of a major at Equifax Canada Inc., a national credit reporting agency.

Security Threats Due to Theft of Disk Drives, Tapes loss, internal breaches …

Agenda

- SAN Security Scope
- Cisco SAN Security
  - SAN Management Security
  - Fabric and Target Access Security
  - Fabric Protocols Security
  - IP Storage Security
  - Unified Fabric Access Security
  - Security for Data in Flight
- Storage Media Security
  - Security for Data at Rest
  - PCI DSS Compliance
- Summary

SCOPE OF STORAGE SECURITY

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-Blilely 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’

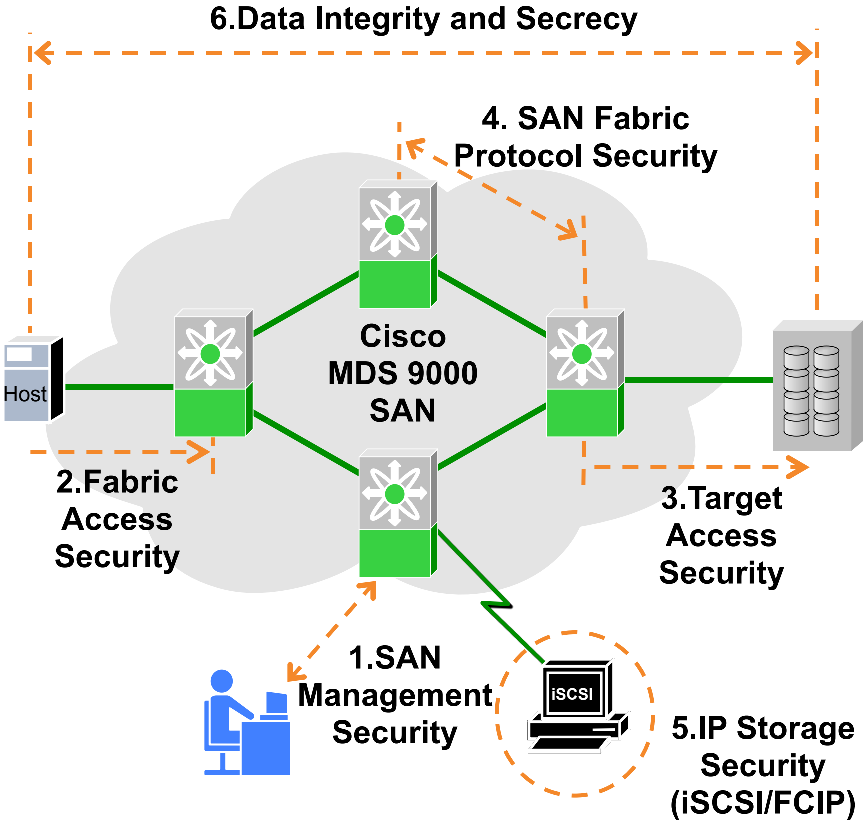
Several Threats: Incomplete Solutions

- SAN security is often overlooked as an area of concern but can have the most detrimental impact
- Application-level integrity and security is well addressed, but the back-end network carrying data is generally not
- SAN extension solutions now push SANs outside the data center boundaries
- Not all compromises are intentional (many are accidental breaches), but they still have the same impact
- SAN security is only one part of complete DC solution:
  - Host access security—one-time passwords, audit logs, VPNs
  - Storage security—data-at-rest encryption, LUN security
  - Datacenter physical security

SAN Security Scope

- Fabric security augments overall application security
  - Host and disk security also required
- Six key areas of focus

1. SAN management access—secure access to management services
2. Fabric access—secure device access to fabric service
3. Target access—secure access to targets and LUNs
4. SAN protocols—secure switch-to-switch communication protocols
5. IP storage access—secure FCIP and iSCSI services
6. Data integrity and secrecy—encryption of data in transit and at rest


6.Data Integrity and Secrecy
4. SAN Fabric Protocol Security
Host
Cisco MDS 9000 SAN
2.Fabric Access Security
3.Target Access Security
1.SAN Management Security
iSCSI
5.IP Storage Security (iSCSI/FCIP)

SAN Management Security

SAN Management Potential Threats

Three Main Areas of Vulnerability:

1. Intentional disruption of switch processing
   - CPU hogging from unnecessary queries
   - Denial-of-service attacks

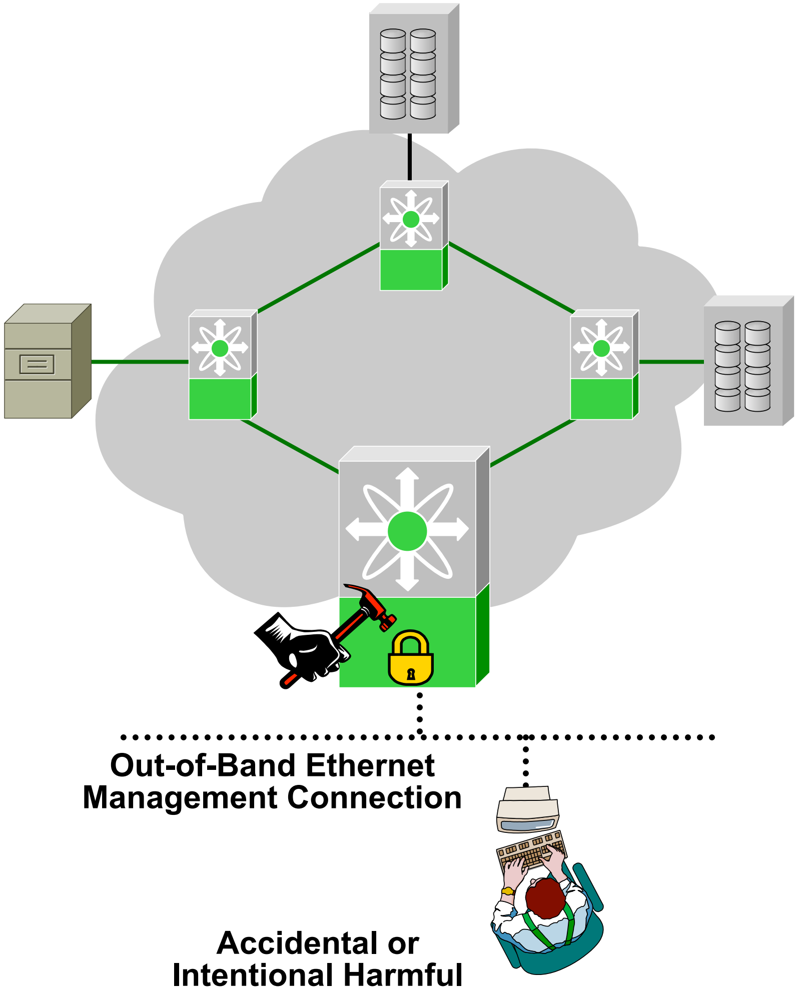
   Result: switch can't react to fabric events

2. Compromised fabric stability
   - Altered/lost switch configurations
   - Removal of other security services
   - Disabled switches/ISLs/device ports

   Result: loss of service, unplanned down time

3. Compromised data integrity and secrecy
   - Altered target (and LUN) visibility
   - Altered zoning configuration

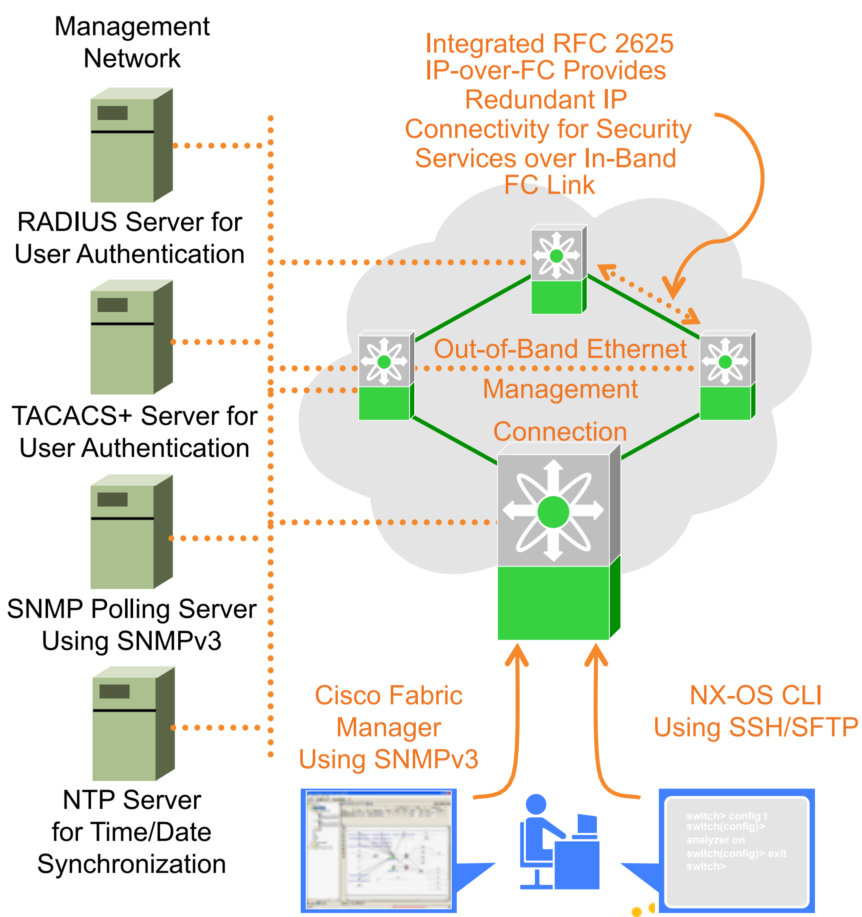
   Result: LUN corruption, data corruption, data theft, or loss


Out-of-Band Ethernet Management Connection
Accidental or Intentional Harmful Management Activity

SAN Management Security

- Securing access to all management facilities on MDS SAN
  - Must secure console sessions
  - Must secure GUI application access
  - Must secure API access (SMI-S)
  - Must also secure file transfer to/from switch
- Equally important to enable audit mechanisms
  - Integrated RADIUS for user accounting and switch scope assignment
  - Integrated syslog for switch-event accounting
  - Integrated SNMP traps for access-denial accounting
  - Network time protocol (NTP) support to synchronize clocks, log entry time stamps

SAN Management Security Infrastructure

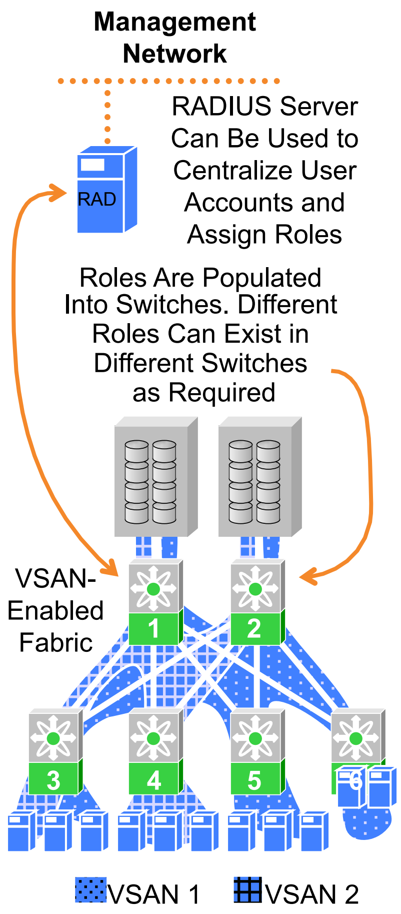

Management Network
RADIUS Server for User Authentication
TACACS+ Server for User Authentication
SNMP Polling Server Using SNMPv3
NTP Server for Time/Date Synchronization
Integrated RFC 2625 IP-over-FC Provides Redundant IP Connectivity for Security Services over In-Band FC Link
Out-of-Band Ethernet Management Connection
Cisco Fabric Manager Using SNMPv3
NX-OS CLI Using SSH/SFTP

```
switch> config t
switch(config)>
analyzer on
switch(config)> exit
switch>
```

Roles-Based Access Control (RBAC)

- Partitioning management capabilities in the MDS SAN
  - Different roles for different user profiles (sys admin, network admin, super admin)
  - Common roles across CLI access and Cisco Fabric Manager access
- Integrated roles-based-access-control
  - Assign subsets of full command set to roles
  - Users are then assigned to roles
  - May have a maximum of 64 unique roles
  - Roles include IP storage features (iSCSI/FCIP)
  - Commands not visible if not part of assigned role
- VSAN-based RBAC
  - Roles can be assigned to specific VSAN(s) only
  - Enables administrator-per-VSAN model
  - Reduce infrastructure costs through consolidation using VSANs and still delegate fabric island administration

Roles-Based Access Control Details


Management Network
RAD
RADIUS Server Can Be Used to Centralize User Accounts and Assign Roles
Roles Are Populated Into Switches. Different Roles Can Exist in Different Switches as Required
VSAN-Enabled Fabric
1
2
3
4
5
6
▨VSAN 1
⊞VSAN 2

Sample Roles

Role #1—Super Admin	
Zoning	Full
FSPF	Full
VSANs	Full
FCID Policy	Full
iSCSI	Full
FCIP	Full

Role #2—Dept. Admin	
Zoning	**VSAN-2**
FSPF	**VSAN-2**
VSANs	No
FCID Policy	**VSAN-2**
iSCSI	View-only
FCIP	View-only

Role #3—Network Admin	
Zoning	View-only
FSPF	View-only
VSANs	View-only
FCID Policy	View-only
iSCSI	Full
FCIP	Full

Bill—SAN admin
Role #1
All Switches
(Full Fabric Admin)

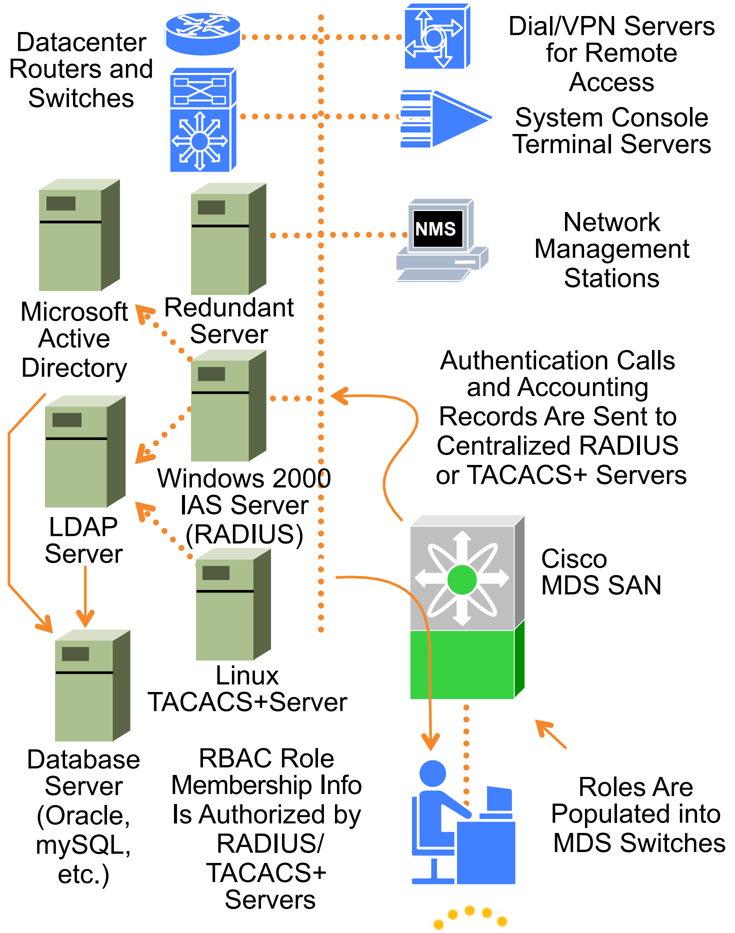
Sally—Network Admin
Role # 3
Configure FCIP
(FCIP and iSCSI only)

Fred—Email Admin
Role #2
Switch 3, 4 only
(VSAN-2—Email App)

Flexible RADIUS and TACACS+ Services

- Used for AAA (Authentication, Authorization, and Accounting) services
  - Limit management access to a subset of switches
  - MDS supports up to five HA server definitions
- RADIUS—**R**emote **A**uthentication **D**ial **I**n **U**ser **S**ervice (IETF RFC-2865 standard)
  - Initially used for dial-in networks—now greatly expanded to a variety of uses
    - System user account centralized authentication
    - Network-device user account AAA services
    - Dial-in/VPN service AAA services
    - iSCSI host authentication
- TACACS+—**T**erminal **A**ccess **C**ontroller **A**ccess **C**ontrol **S**ystem (based on RFC-1492)
  - Widely used and supported by Cisco
  - Freely available from Cisco—similar to RADIUS
- Native LDAP/Active Directory integration
  - Single sign on

RADIUS and TACACS+ Deployments


Datacenter Routers and Switches
Dial/VPN Servers for Remote Access
System Console Terminal Servers
NMS
Network Management Stations
Microsoft Active Directory
Redundant Server
Authentication Calls and Accounting Records Are Sent to Centralized RADIUS or TACACS+ Servers
LDAP Server
Windows 2000 IAS Server (RADIUS)
Cisco MDS SAN
Linux TACACS+Server
Database Server (Oracle, mySQL, etc.)
RBAC Role Membership Info Is Authorized by RADIUS/ TACACS+ Servers
Roles Are Populated into MDS Switches

Reference

Sample Radius Accounting Record

- Example snapshot of a Microsoft IAS RADIUS record generated during an MDS 9509 CLI session
- Start/stop records are recorded by default, accounting records of actual commands are enabled on as an option
- Similar record generated by TACACS+

Decoded Microsoft IAS Radius Accounting Record Using Microsoft's 'iasparse.exe' Support Tool (Part of Windows 2000/2003 Distribution)

```
NAS-IP-Address          : 172.19.48.87
User-Name               : net-adm-1
Record-Date             : 10/3/2007
Record-Time             : 11:51:08
Service-Name            : IAS
Computer-Name           : IBM305S1
NAS-Identifier          : login
NAS-Port-Type           : Virtual
NAS-Port                : 3001
Service-Type            : Authenticate-Only
Calling-Station-Id      : sjc-1.cisco.com
Client-IP-Address       : 172.19.48.87
Client-Vendor           : CISCO
Client-Friendly-Name    : core3
SAM-Account-Name        : IBM305S1\net-adm-1
Fully-Qualified-Name    : IBM305S1\net-adm-1
Authentication-Type     : PAP
Class                   : 311 1 172.19.48.54 10/3/2007 18:44:03 1
Packet-Type             : Access-Request
Reason-Code             : The operation completed successfully.
```

Full RADIUS Accounting Record

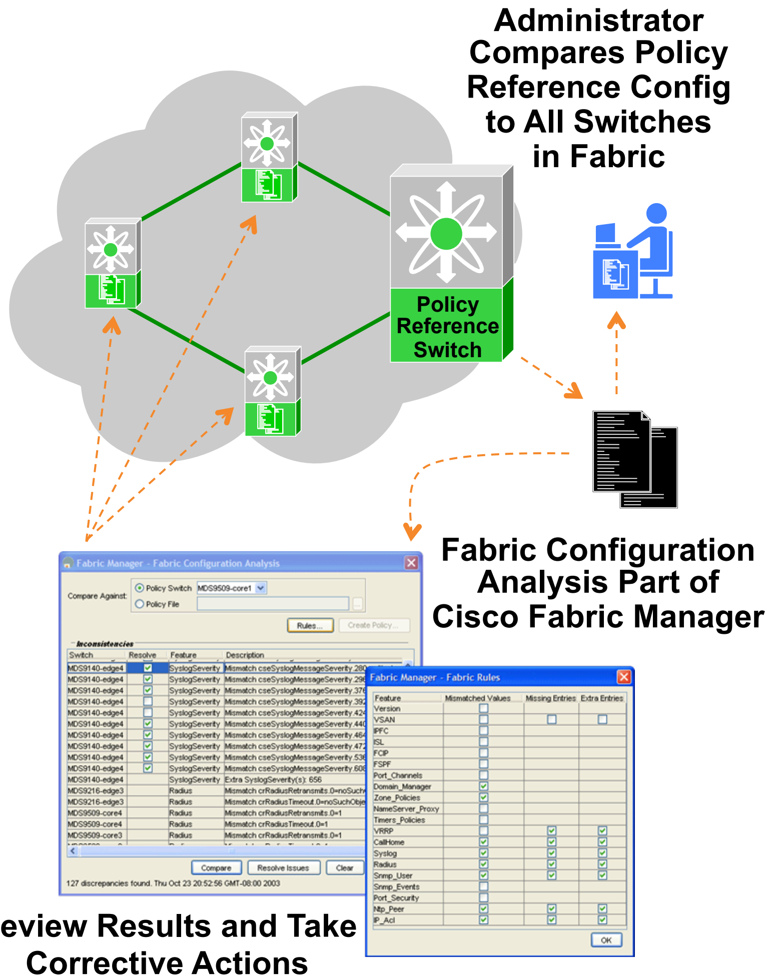
```
172.19.48.87,net-adm-1,10/3/2007,11:51:08,IAS,IBM305S1,32,login,61,5,5,3001,6,8,31,sjc-1.cisco.com,4108,172.19.48.87,4116,
9,4128,core3,4129,IBM305S1\net-adm-1,4130,IBM305S1\net-adm-1,4127,1,25,311 1 172.19.48.54 10/3/2007 18:44:03 1,4136,1,4142,0
```

```
172.19.48.87,net-adm-1,10/3/2007,11:51:08,…,shell:roles=network-admin,MDS Policy,172.19.48.87,core3,IBM305S1\net-adm-1,…
172.19.48.87,net-adm-1,10/3/2007,11:51:34,…,accounting:accountinginfo=vsan:4001 values updated interoperability mode:1,…
172.19.48.87,net-adm-1,10/3/2007,11:51:56,…,accounting:accountinginfo=vsan:4001 values updated loadbalancing:src-id/dst-id/oxid,…
172.19.48.87,net-adm-1,10/3/2007,11:52:02,…,accounting:accountinginfo=Interface fc3/1 state updated to down,…
172.19.48.87,net-adm-1,10/3/2007,11:52:05,…,accounting:accountinginfo=Interface fc3/1 state updated to up,…
172.19.48.87,net-adm-1,10/3/2007,11:52:16,…,accounting:accountinginfo=vsan:4001 deleted,…
172.19.48.87,net-adm-1,10/3/2007,11:52:20,…,accounting:accountinginfo=vsan:4000 deleted,…
172.19.48.87,net-adm-1,10/3/2007,11:52:23,…,accounting:accountinginfo=shell terminated,…
```

Some of These Records Have Been Shortened to Fit Them on this Slide

Configuration Consistency Analysis

- Important to keep consistent configurations across all switches
  - Especially important for security configurations: RADIUS/TACACS+, remote syslog, NTP, SNMP communities, authentication, and roles
- Configurations can be extracted from switches as a flat text file
  - Allows for easy and regular archiving
- Cisco Fabric Manager provides fabric configuration analysis tool
  - Checks all switch configurations against policy switch or file
  - Can take corrective action to fix configurations
  - Also has zone-merge analysis tool to validate zone-merge validity



Administrator Compares Policy Reference Config to All Switches in Fabric

Fabric Configuration Analysis Part of Cisco Fabric Manager

Fabric Manager - Fabric Configuration Analysis

Compare Against: ● Policy Switch MDS9509-core1
○ Policy File

Inconsistencies

Switch	Resolve	Feature	Description
MDS9140-edge4	☑	SyslogSeverity	Mismatch cseSyslogMessageSeverity.280
MDS9140-edge4	☑	SyslogSeverity	Mismatch cseSyslogMessageSeverity.296
MDS9140-edge4	☑	SyslogSeverity	Mismatch cseSyslogMessageSeverity.376
MDS9140-edge4	□	SyslogSeverity	Mismatch cseSyslogMessageSeverity.392
MDS9140-edge4	□	SyslogSeverity	Mismatch cseSyslogMessageSeverity.424
MDS9140-edge4	☑	SyslogSeverity	Mismatch cseSyslogMessageSeverity.440
MDS9140-edge4	☑	SyslogSeverity	Mismatch cseSyslogMessageSeverity.464
MDS9140-edge4	☑	SyslogSeverity	Mismatch cseSyslogMessageSeverity.472
MDS9140-edge4	☑	SyslogSeverity	Mismatch cseSyslogMessageSeverity.536
MDS9140-edge4	☑	SyslogSeverity	Mismatch cseSyslogMessageSeverity.608
MDS9140-edge4		SyslogSeverity	Extra SyslogSeverity(s): 656
MDS9216-edge3		Radius	Mismatch crRadiusRetransmits.0=noSuch
MDS9216-edge3		Radius	Mismatch crRadiusTimeout.0=noSuchObje
MDS9509-core4		Radius	Mismatch crRadiusRetransmits.0=1
MDS9509-core4		Radius	Mismatch crRadiusTimeout.0=1
MDS9509-core3		Radius	Mismatch crRadiusRetransmits.0=1

127 discrepancies found. Thu Oct 23 20:52:56 GMT-08:00 2003

Fabric Manager - Fabric Rules

Feature	Mismatched Values	Missing Entries	Extra Entries
Version	□		
VSAN	□	□	□
IPFC	□		
ISL	□		
FCIP	□		
FSPF	□		
Port_Channels	□		
Domain_Manager	☑		
Zone_Policies	☑		
NameServer_Proxy	□		
Timers_Policies	□		
VRRP	□	☑	☑
CallHome	☑	☑	☑
Syslog	☑	☑	☑
Radius	☑	☑	☑
Snmp_User	☑	☑	☑
Snmp_Events	□		
Port_Security	□		
Ntp_Peer	☑	☑	☑
IP_Acl	☑	☑	☑

Review Results and Take Corrective Actions

Define Analysis Rules

SAN Management Recommendations

- Use RBAC to grant adequate privilege to SAN administrators
  - Example: not every administrator needs capability to disable modules
  - Reserve select functions to fewer super-admin RBAC role:
  - VSAN definition, firmware upgrades, roles definition, RADIUS, and SSH configuration
- Use RADIUS or TACACS+ for centralized user account administration
  - Ensures consistent and timely removal of users if required
  - Use RADIUS accounting feature for audit log of configuration events
- Use all secure forms of management protocols—disable others
  - SSH, SFTP, SCP, SNMPv3, SSL for SMI-S support
  - Disable Telnet, FTP, TFTP, SNMPv1,v2
- Enable NTP across all switches for consistent time stamping of events
- Log and archive everything
  - Enable centralized syslog
  - Take regular copies of switches configurations (can use CiscoWorks RME)
  - Turn on MDS call-home feature to alert of anomalies

Fabric and Target Access Security

Fabric and Target Access Potential Threats

Three Main Areas of Vulnerability:

- Compromised application data
  - Unauthorized access to targets and LUNs
  - High potential for data corruption, loss, or theft

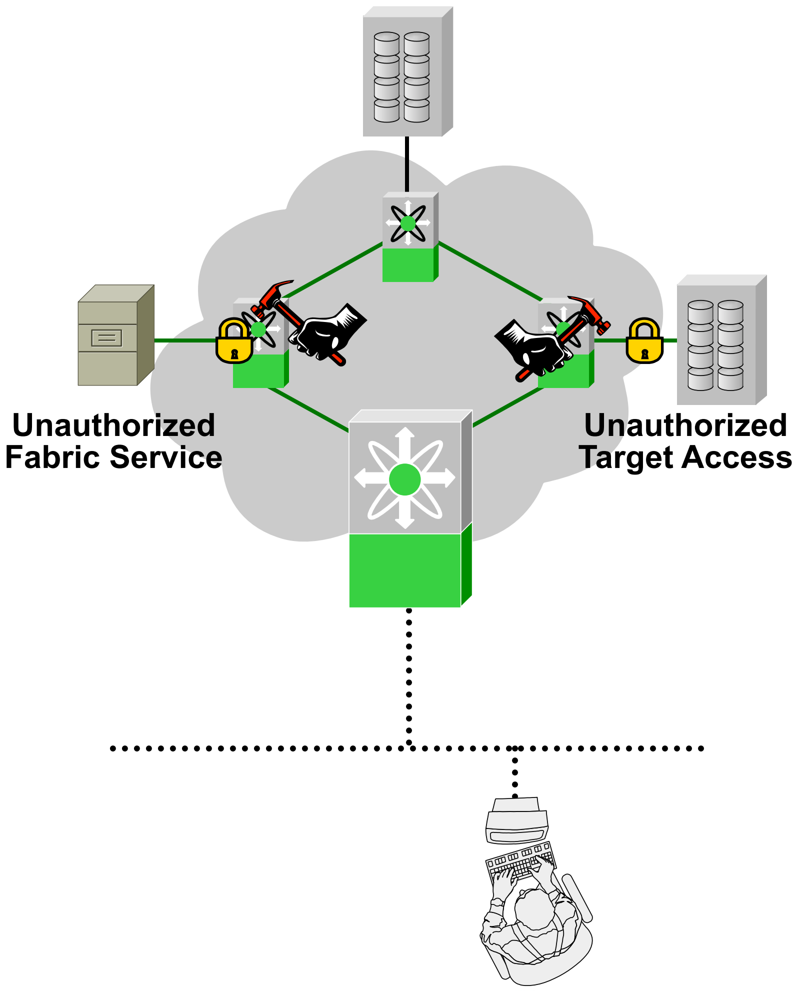
  Result: unplanned down time, costly data loss

- Compromised LUN integrity
  - LUN corruption due to unintentional OS mount
  - Accidental formatting of LUN—loss of data

  Result: unplanned down time, costly data loss

- Compromised application performance
  - Unauthorized I/O potentially causing congestion
  - Injected fabric events causing disruption; i.e., rogue HBA hammering fabric controller

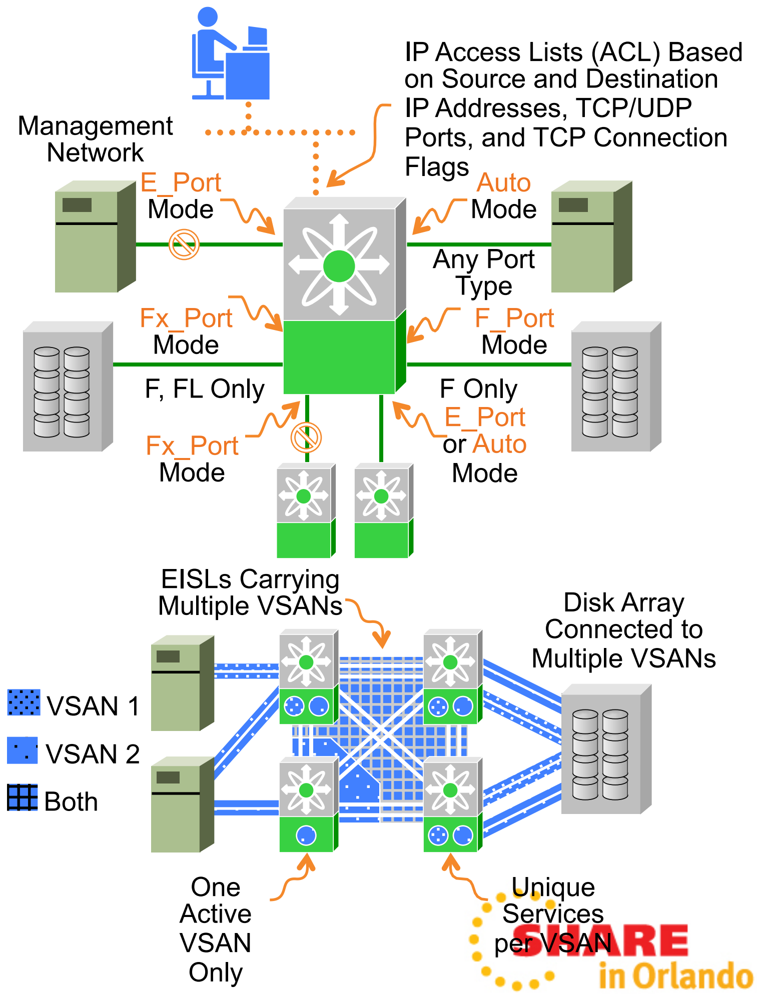
  Result: unplanned down time, poor I/O performance



Fabric Access Security: Port Modes

- Port-mode security—allow edge ports to form F_Ports or FL_Ports only, i.e., no ISL/EISL
    - MDS supports an Fx_Port mode which allows F_Port or FL_Port only
    - Limit users who can change port mode via roles-based access control assignments
- VSAN-based security—only allow access to devices within attached VSAN
    - Strict isolation based on fabric service partitioning and explicit frame tagging
    - Independent name server table per VSAN
    - Independent active zoneset per VSAN
    - Part of ANSI T11 fabric expansion study group
- Management port access security
    - Provides IP access control lists (ACLs) for management traffic (SNMP, SSH, Telnet, etc.)

Port Mode and VSAN-Based Security

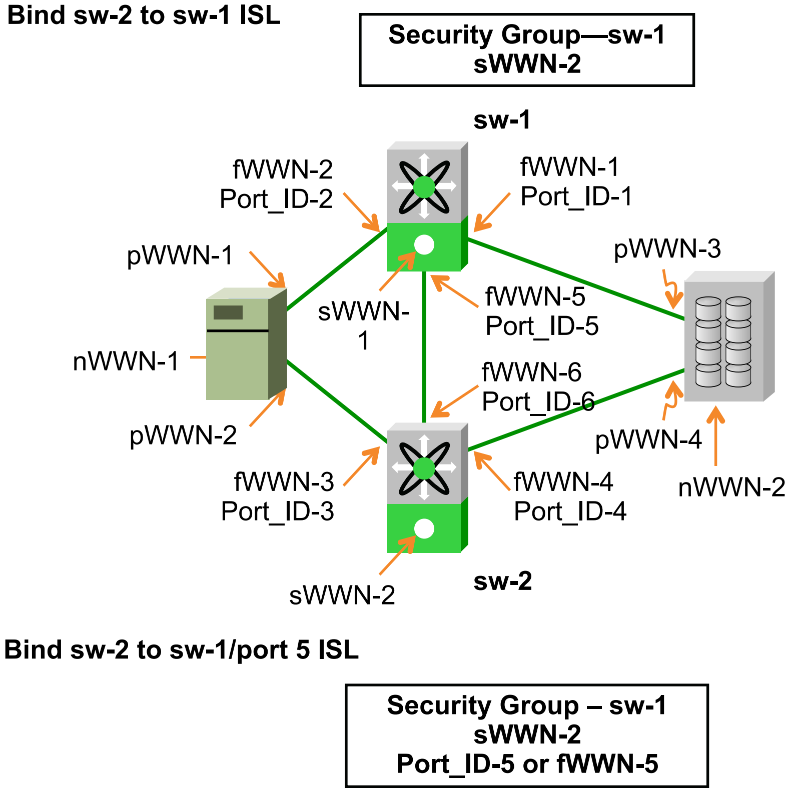


Fabric Access Security

- MDS access security technology
  - Grant selective access to fabric based on device identity
  - Failure results in link-level login failure
  - Prevents FC frame S_ID spoofing through hardware frame filtering
- Supports switch-to-switch (fabric binding) and device-to-switch (port security)
  - Auto-learning mode to ease initial configuration
- Uses grouping of attributes to define binding configuration
  - WWN or Port_ID – port identifier on switch (i.e. fc1/2)
  - Multiple groups are created and activated as a group set to enforce desired policy
- Default configuration
  - Set port administrative default value to SHUT
  - Do not put ports in VSAN 1
  - Ports by default in VSAN 4094 (isolated)

Fabric Access Security: Fabric Binding

- Used to allow ISL establishment
- Attributes to define binding configuration:
    - fWWN—fabric WWN of switch port
    - sWWN—switch WWN
    - Port_ID—port identifier on switch (i.e., fc1/2)



Bind sw-2 to sw-1 ISL

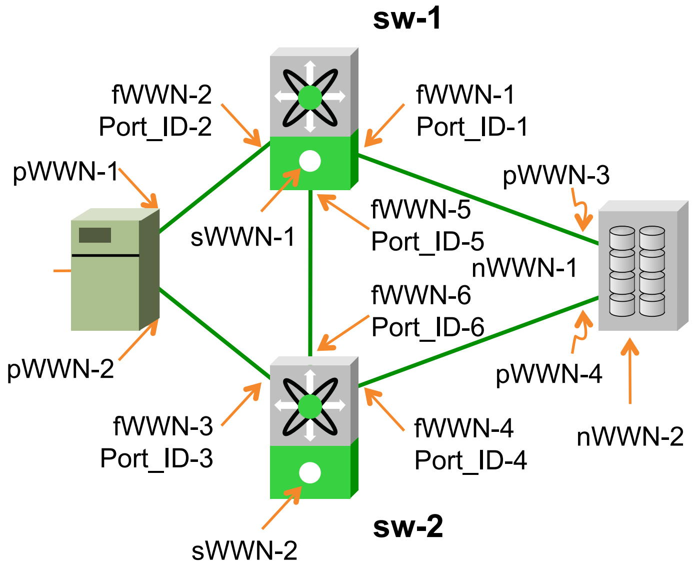
Security Group—sw-1
sWWN-2

Bind sw-2 to sw-1/port 5 ISL

Security Group – sw-1
sWWN-2
Port_ID-5 or fWWN-5

Fabric Access Security: Port Security

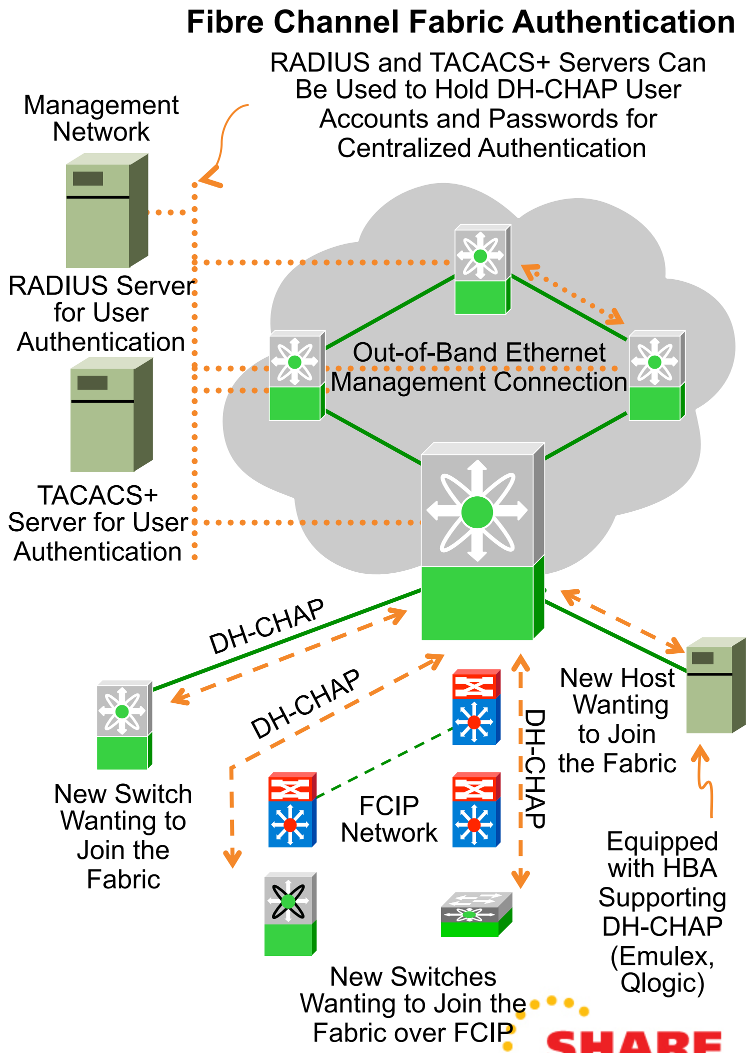
- Used to allow device-to-switch login
- Attributes to define binding configuration
  - pWWN—port WWN of attaching device
  - nWWN—node WWN of attaching device
  - fWWN—fabric WWN of switch port
  - Port_ID—port identifier on switch (i.e. fc1/2)



Bind Host to sw-1 (Any Port)	**Security Group – sw-1_pWWN-1 or nWWN-1**
Bind Host, disk to sw-1 (Any Port)	**Security Group – sw-1** **pWWN-1 or nWWN-1 pWWN-3 or nWWN-2**
Bind Host to sw-1/port 2	**Security Group – sw-1** **pWWN-1 or nWWN-1 Port_ID-2 or fWWN-2**
Bind Host HBA-1 to sw-1/port 2	**Security Group – sw-1** **pWWN-1 Port_ID-2 or fWWN-2**

Fabric Access Security: Authentication

- Device authentication provides stronger means of ensuring device identity
  - WWNs can be spoofed by simple means
- ANSI T11 FC-SP security protocols working group
  - Cisco was the prime contributor
- DH-CHAP provides authentication mechanism
  - Switch-to-switch authentication
  - Device-to-switch authentication (when adopting HBA supporting DH-CHAP)


Fibre Channel Fabric Authentication
RADIUS and TACACS+ Servers Can Be Used to Hold DH-CHAP User Accounts and Passwords for Centralized Authentication
Management Network
RADIUS Server for User Authentication
TACACS+ Server for User Authentication
Out-of-Band Ethernet Management Connection
DH-CHAP
DH-CHAP
DH-CHAP
New Switch Wanting to Join the Fabric
FCIP Network
New Host Wanting to Join the Fabric
Equipped with HBA Supporting DH-CHAP (Emulex, Qlogic)
New Switches Wanting to Join the Fabric over FCIP

Fabric Access Recommendations

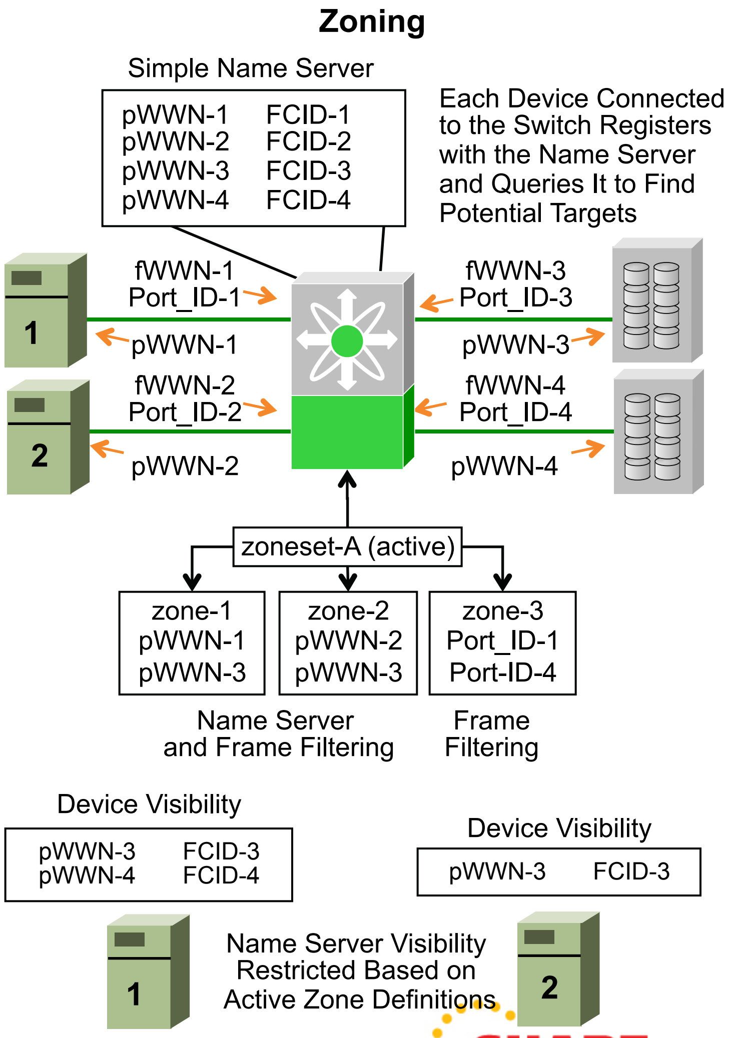
- Use IP ACLs on management interfaces to block unused services
  - Enable logging of denied attempts—block denial-of-service attacks
- Hard-fix switch-port administrative modes to assigned port function
  - Lock (E)ISL ports to only be (T)E_Ports—set to E_Port mode
  - Lock access ports to only be F(L)_Ports—set to Fx_Port mode
- Use VSANs to isolate departments
  - Provides security **and** availability benefits
  - RBAC management control per VSAN allows individual admin assignment
- Use port security features everywhere
  - Bind devices to switch as a minimum level of security
  - Bind devices to a port as an optimal configuration
    - Consider binding to line card in case of port failure
  - Bind switches together at ISL ports—bind to specific port, not just switch
- Use FC-SP authentication for switch-to-switch fabric access
  - Use device-to-switch when available

More information and step by step configuration in the NX-OS Security Configuration Guide at:

http://www.cisco.com/en/US/docs/switches/datacenter/mds9000/sw/nx-os/configuration/guides/sec/sec_cli_4_2_published/sec.html

Target Access Security: Zoning

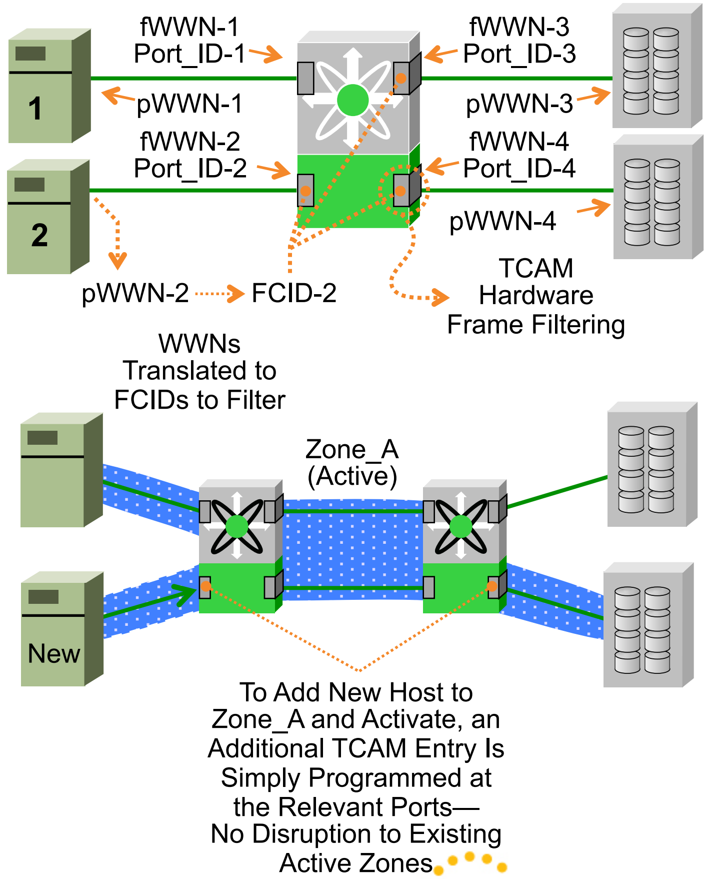
- Zoning is prime mechanism for securing access to SAN targets (disk and tape)
- Two prime types of zoning:
  - Soft zoning (sw-based name server filtering)
    - Communication still possible if FC_ID known
  - Hard zoning (hw-enforced frame filtering)
    - Absolute requirement for true security
    - Also involves name server filtering
  - Can filter on various attributes
    - Switch port_IDs—vendor-specific
    - Device nWWN/pWWNs—standards-based
    - Advanced zoning features offered by Cisco
- Zoning is very complementary to VSANs
  - One active zoneset per VSAN
  - Multiple configured zonesets per VSAN
  - Non-disruptive zoneset activation to other VSANs



MDS Zoning Services

- All zoning services offered by Cisco are implemented in hardware
  - No dependence on whether using mix of WWNs and Port_IDs in a zone—all hardware based
  - WWN-based zoning implemented in software with hardware reinforcement (i.e., no name server only zoning)
  - WWNs are translated to FCIDs to be frame-filtered
- Dedicated high-speed port filters called ternary CAMs (TCAMs) filter each frame in hardware and reside in front of each port
  - Support up to 20,000 programmable entries consisting of zones and zone members
  - Very deep frame filtering for new innovative features
  - Wire-rate filtering performance—no impact regardless of number of zones or zone entries
  - Optimized programming during zoneset activation—incremental zoneset updates
- RSCNs contained within zones in given VSAN
- Selective default zone behavior—default is deny
  - Per VSAN setting

Hardware-Based Zoning Details



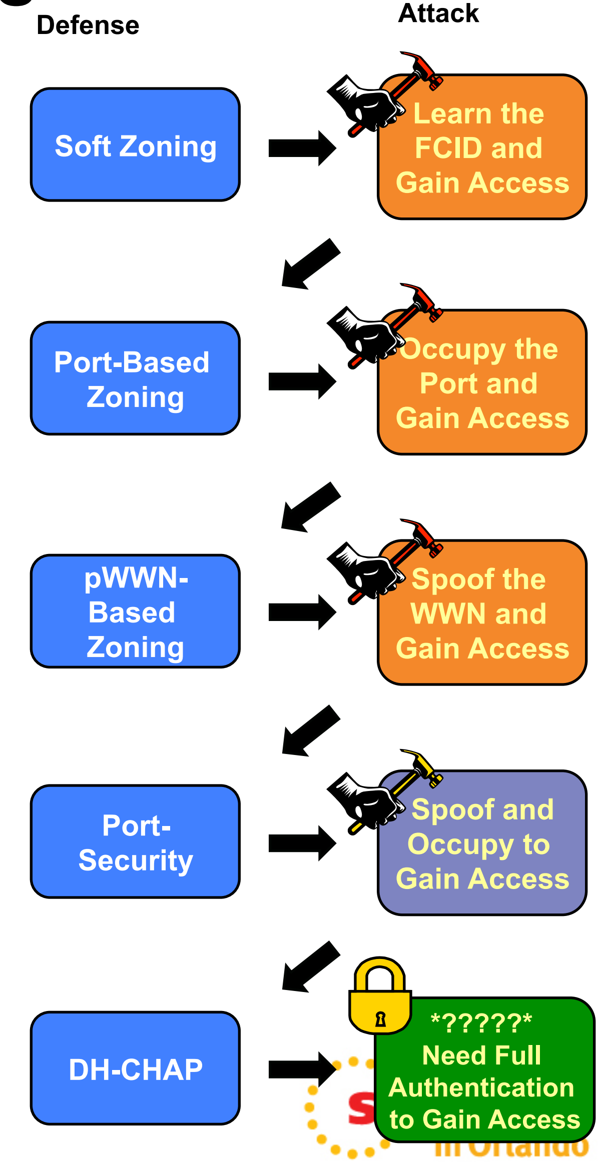
TCAM Hardware Frame Filtering

WWNs Translated to FCIDs to Filter

To Add New Host to Zone_A and Activate, an Additional TCAM Entry Is Simply Programmed at the Relevant Ports—No Disruption to Existing Active Zones

Target Access Recommendations

- Use zoning services to isolate where required
  - Port or WWN-based, all hardware enforced
  - Set default-zone policies to deny
- Suggested to only allow zoning configuration from one or two switches to minimize access
  - Use RBAC to create two roles, only one allowing zoning configuration
  - Install permit role on two switches, deny role on remainder
  - Or, use RADIUS or TACACS+ to assign roles based on particular switch, more flexible
- Use WWN-based zoning for convenience and use port-security features to harden switch access
  - Works well for interop with non-Cisco switches
  - Port-based zoning in native mode interoperability in SANOS v1.2



Defense

Attack

Soft Zoning → Learn the FCID and Gain Access

Port-Based Zoning → Occupy the Port and Gain Access

pWWN-Based Zoning → Spoof the WWN and Gain Access

Port-Security → Spoof and Occupy to Gain Access

DH-CHAP → *?????* Need Full Authentication to Gain Access

Fabric Protocols Security

Fabric Protocols Potential Threats

Three Main Areas of Vulnerability:

- Compromised fabric stability
  - Injection of disruptive fabric events
  - Creation of traffic black-hole

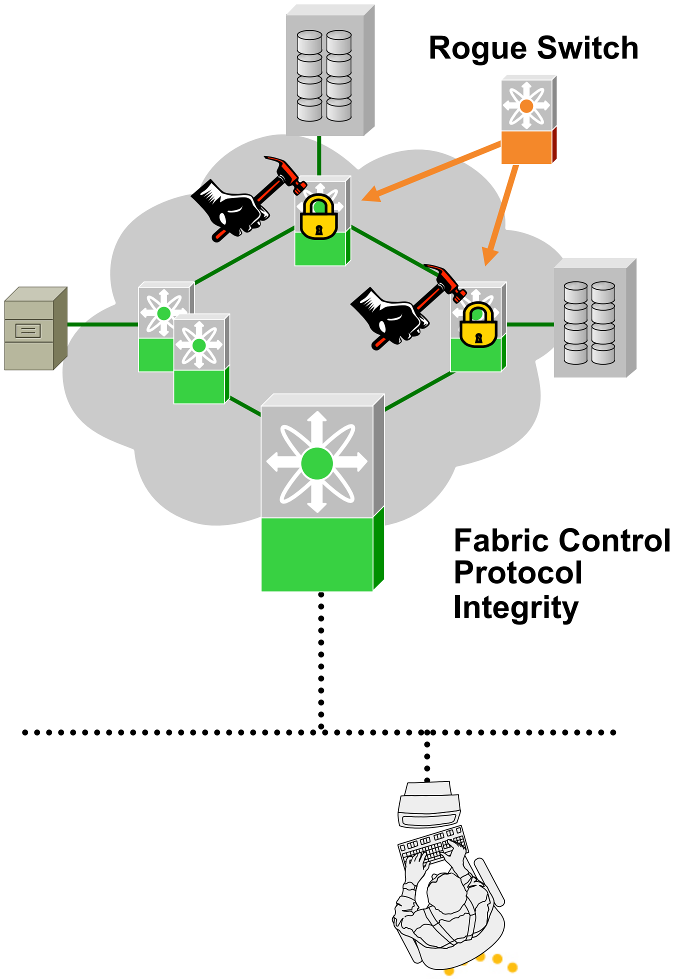
  Result: unplanned down time,
  fabric instability

- Compromised data security
  - Injection of harmful zone reconfiguration data
  - Open access to fabric targets

  Result: unplanned down time, costly data loss

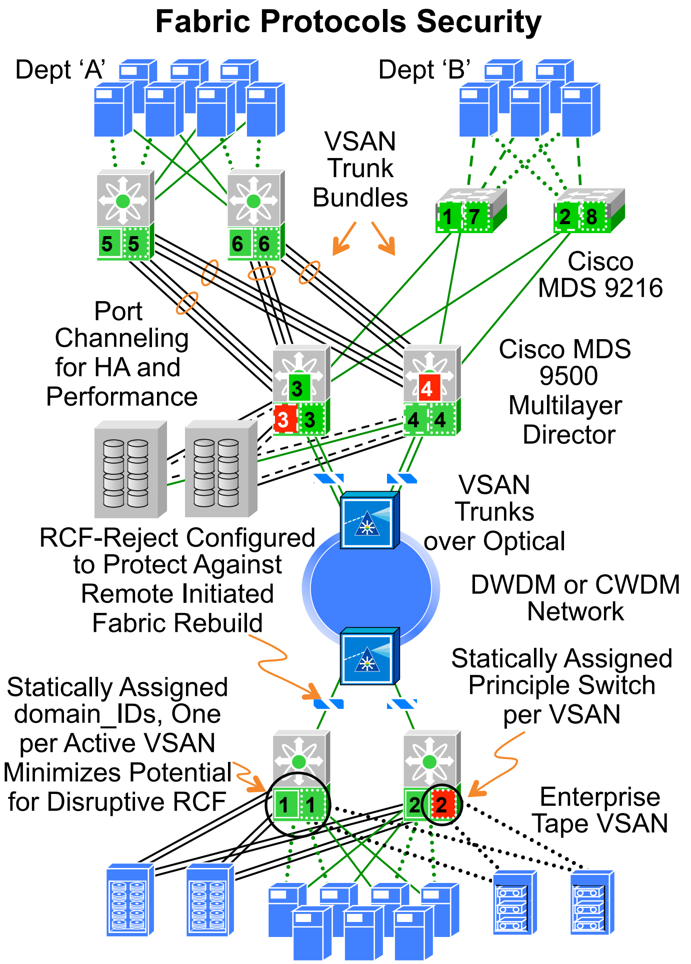
- Compromised application performance
  - Unauthorized I/O potentially causing congestion
  - Numerous disruptive topology changes

  Result: unplanned down time,
  poor I/O performance



SAN Fabric Protocols Security

- Very important to secure the fabric control protocols to ensure fabric stability
  - Securing access to control protocol configuration via Cisco RBAC is first step
  - Enable port-security for switch binding
  - Using FC-SP for switch-to-switch authentication is next critical step to block rogue ISLs
- Plug-n-play fabric protocol configuration is convenient—however, static configuration is more secure
  - Configure static principle switch
  - Enable static domain IDs
  - Enable static FCIDs optional but recommended
    - Great benefit for HP/UX and AIX environments
  - Enable RCF-reject, especially on long-haul links
  - Enable RSCN-suppression where necessary
- Use VSANs to divide and manage individual fabric configuration and resiliency


Fabric Protocols Security
Dept ‘A’
Dept ‘B’
VSAN Trunk Bundles
5 5
6 6
1 7
2 8
Cisco MDS 9216
Port Channeling for HA and Performance
3
3 3
4
4 4
Cisco MDS 9500 Multilayer Director
VSAN Trunks over Optical
RCF-Reject Configured to Protect Against Remote Initiated Fabric Rebuild
DWDM or CWDM Network
Statically Assigned Principle Switch per VSAN
Statically Assigned domain_IDs, One per Active VSAN Minimizes Potential for Disruptive RCF
1 1
2 2
Enterprise Tape VSAN

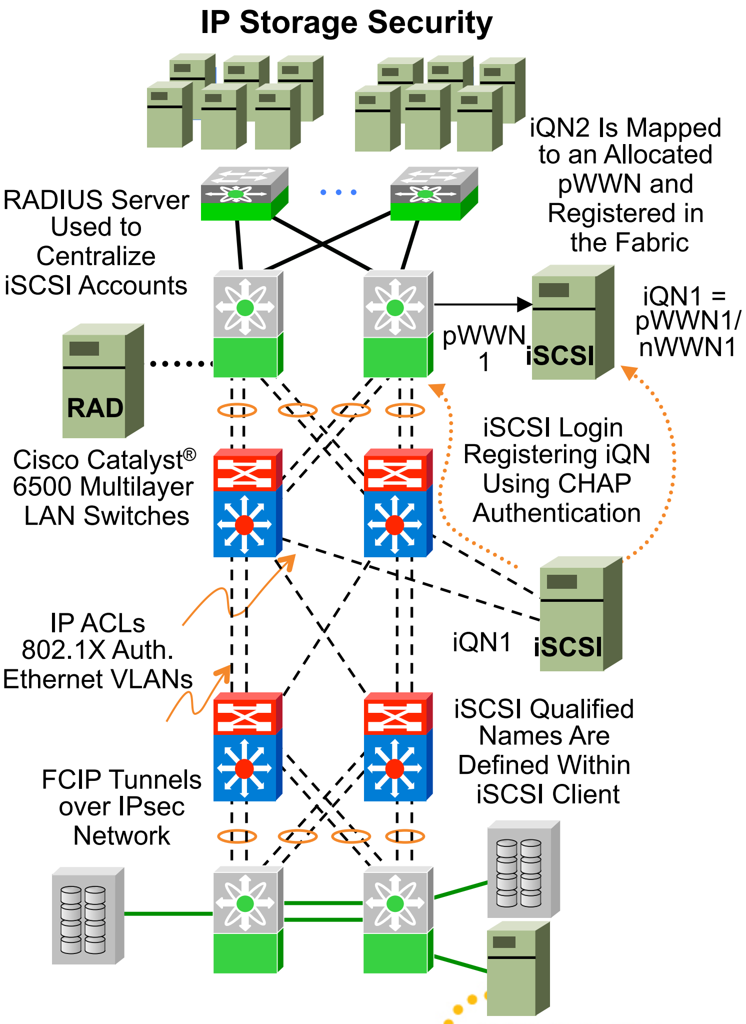
Agenda

- SAN Security Scope
- Cisco SAN Security
  - SAN Management Security
  - Fabric and Target Access Security
  - Fabric Protocols Security
  - IP Storage Security
  - Unified Fabric Access Security
  - Security for Data in Flight
- Storage Media Security
  - Security for Data at Rest
  - PCI DSS Compliance
- Summary

IP Storage Security

IP Storage Security

- iSCSI leverages many of the security features inherent in Ethernet and IP
  - Ethernet Access Control Lists (ACLs) ↔ FC zones
  - Ethernet VLANs ↔ FC VSANs
  - Ethernet 802.1x port security ↔ FC port security
  - iSCSI authentication ↔ FC DH-CHAP authentication
- iSCSI offers LUN masking/mapping capability as part of gateway function
- FCIP security through IPsec
  - IPsec used to connect through public carriers
  - High-speed encryption services in specialized HW
  - Can also be run through a firewall
- FCIP tunnel is a virtual ISL—can leverage FC-based FC-SP switch-to-switch authentication


IP Storage Security
RADIUS Server Used to Centralize iSCSI Accounts
iQN2 Is Mapped to an Allocated pWWN and Registered in the Fabric
iQN1 = pWWN1/ nWWN1
pWWN 1
iSCSI
RAD
Cisco Catalyst® 6500 Multilayer LAN Switches
iSCSI Login Registering iQN Using CHAP Authentication
IP ACLs 802.1X Auth. Ethernet VLANs
iQN1
iSCSI
iSCSI Qualified Names Are Defined Within iSCSI Client
FCIP Tunnels over IPsec Network

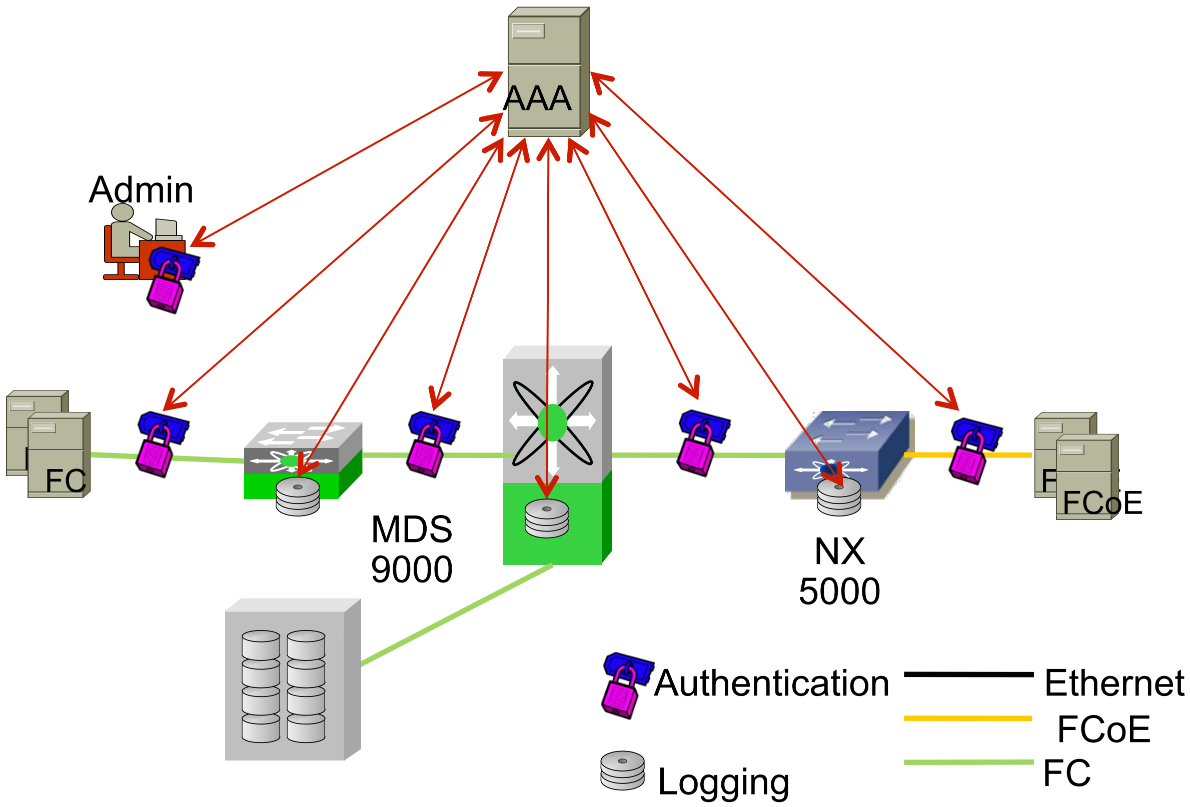
SHARE in Orlando 2011

Agenda

- SAN Security Scope
- Cisco SAN Security
  - SAN Management Security
  - Fabric and Target Access Security
  - Fabric Protocols Security
  - IP Storage Security
  - Unified Fabric Access Security
  - Security for Data in Flight
- Storage Media Security
  - Security for Data at Rest
  - PCI DSS Compliance
- Summary

Unified Fabric Access Security

MDS 9000 and Nexus 5000 Common AAA



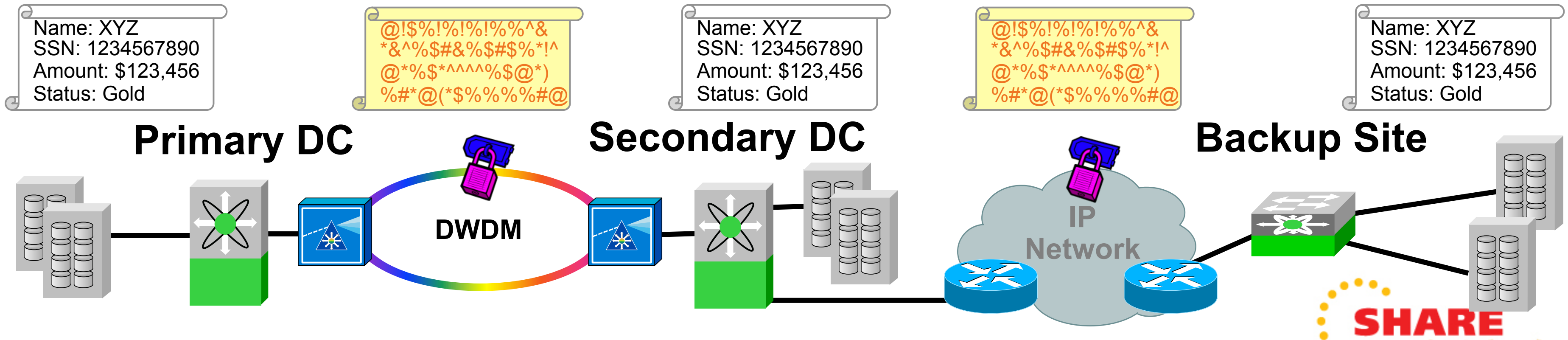
- Homogeneous AAA
  - User accounts/groups, device identities: Local or RADIUS/TACACS
  - RBAC best practices: Unified-admin, LAN-admin, SAN-admin
- Common FC features
  - VSANs, Zoning, IVR, Port Channeling, Trunking, fabric services etc.

Agenda

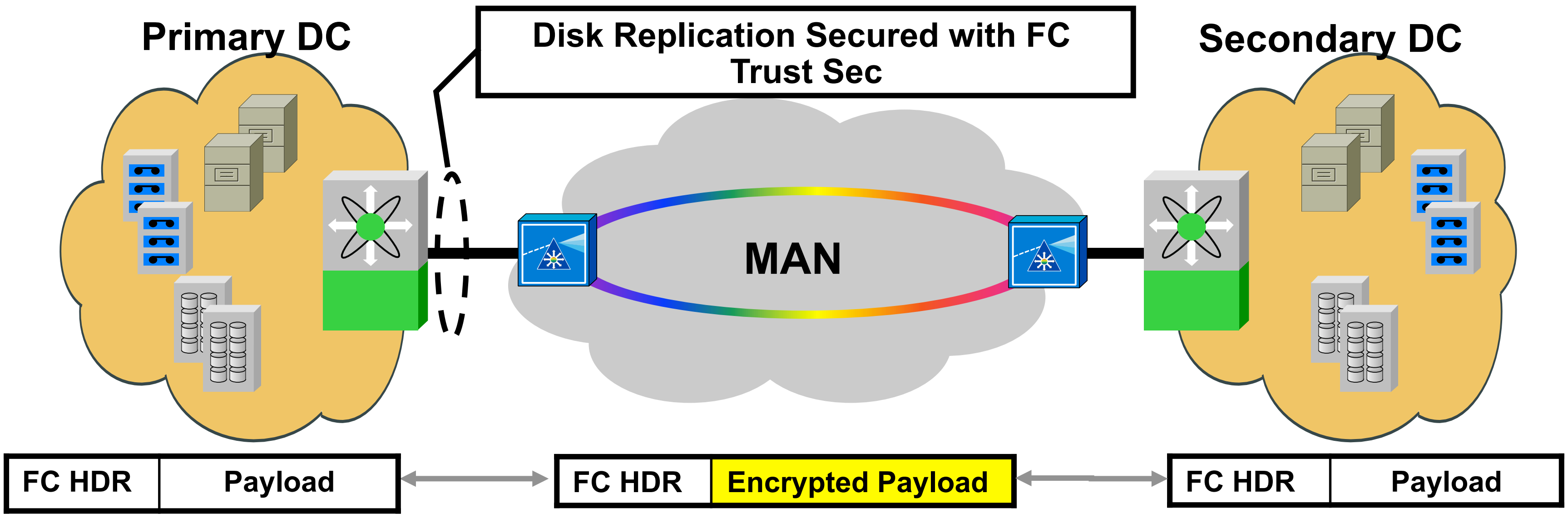
- SAN Security Scope
- Cisco SAN Security
  - SAN Management Security
  - Fabric and Target Access Security
  - Fabric Protocols Security
  - IP Storage Security
  - Unified Fabric Access Security
  - Security for Data in Flight
- Storage Media Security
  - Security for Data at Rest
  - PCI DSS Compliance
- Summary

Link Layer Security - Overview

- Data Confidentiality requirements are part of business today
- Businesses need to ensure that data is not compromised while be transmitted between Data Centers
- Cisco TrustSec (FC) and IPsec (FCIP) used to secure data over ISLs between switches

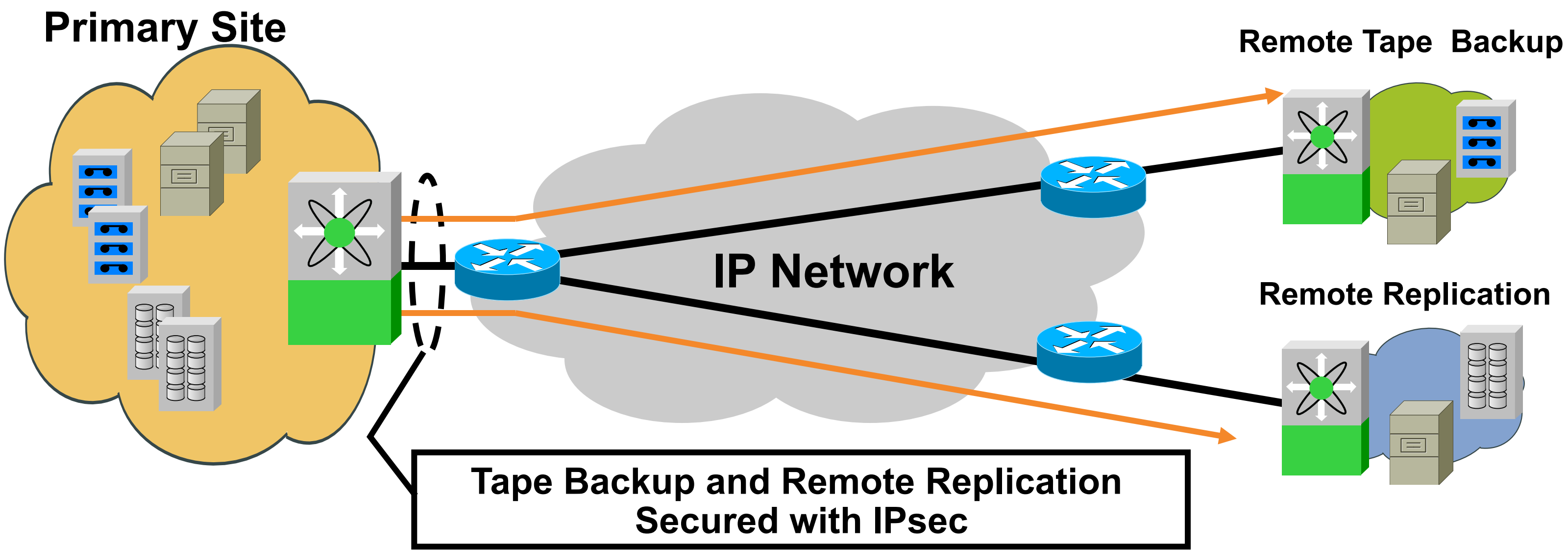


FC Link Encryption - Cisco TrustSec



- Extension to FC-SP protocol to provide encryption of data
  - DH-CHAP used for peer authentication
  - Encryption: AES 128 bit key
- Integrity, confidentiality, authentication, no replay across Dark Fiber/ MAN
- HW-based 8G FC wire rate on Gen-3 8G FC blades
- No change to existing SAN, functionality provided by edge switches

FCIP data security - IPsec Encryption



- Standards-based IPsec Encryption—implements RFC 2402 to 2410, & 2412
  - IKE for protocol/algorithm negotiation and key generation
  - Encryption: AES (128 or 256 bit key), DES (56 bit), 3DES (168 bit)
- Hardware-based GigE wire rate performance with latency ~ 10µs per packet
- Provides integrity, confidentiality, origin authentication, anti-replay across the IP network

Agenda

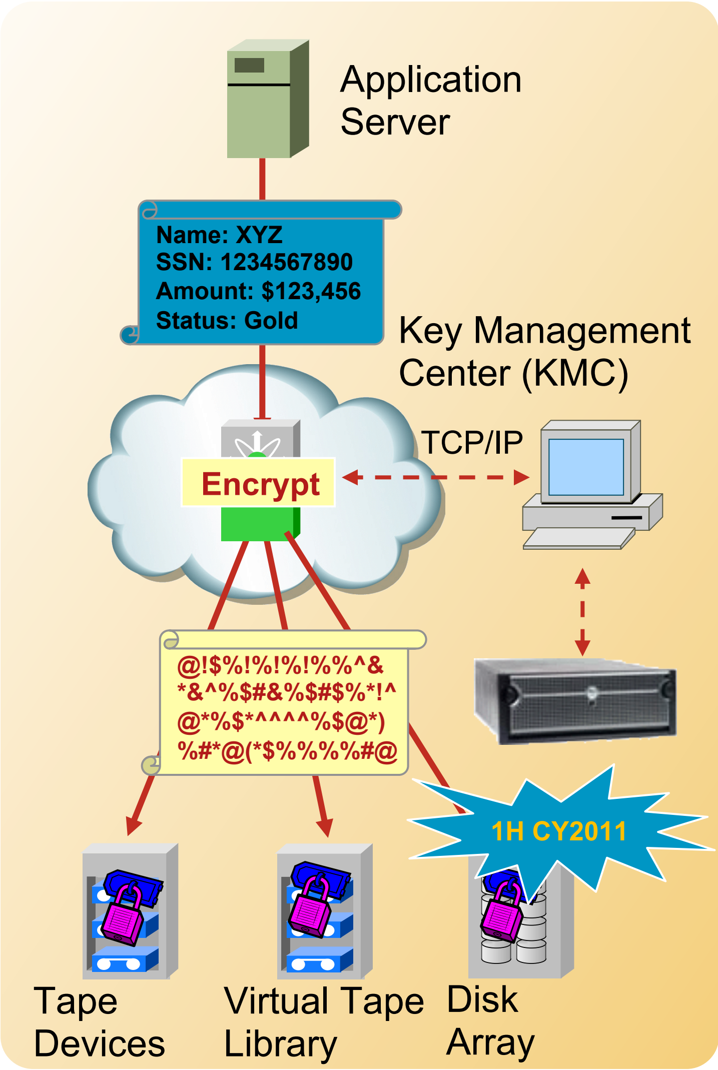
- SAN Security Scope
- Cisco SAN Security
  - SAN Management Security
  - Fabric and Target Access Security
  - Fabric Protocols Security
  - IP Storage Security
  - Unified Fabric Access Security
  - Security for Data in Flight
- Storage Media Security
  - Security for Data at Rest
  - PCI DSS Compliance
- Summary

Security for Data at Rest

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 and Arrays
  - High Performance
  - New Drives and possibly new media needed
  - Could be costly
- Fabric Based
  - Ease of installation
  - Scalable
  - Integrated with Key Management Solutions

Cisco SME - Secure, Integrated Solution



- Encrypts media for SAN attached tapes, virtual tape libraries and disk arrays

  Uses IEEE AES-256 encryption

  Disk – XTS, Tape – GCM

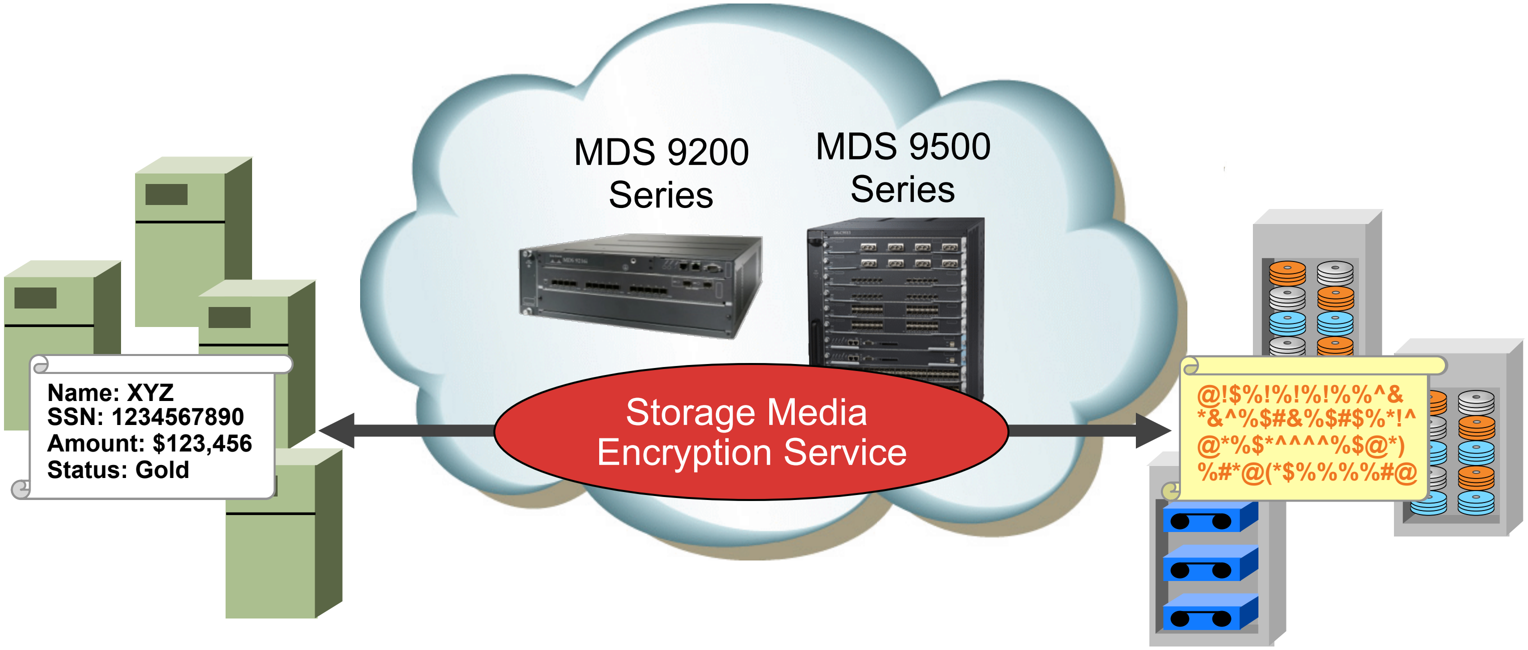
  CC EAL-3 and FIPS 140-2 certified switch

- Solution includes Cisco KMC for provisioning and key management

  Integration with RSA Key Manager

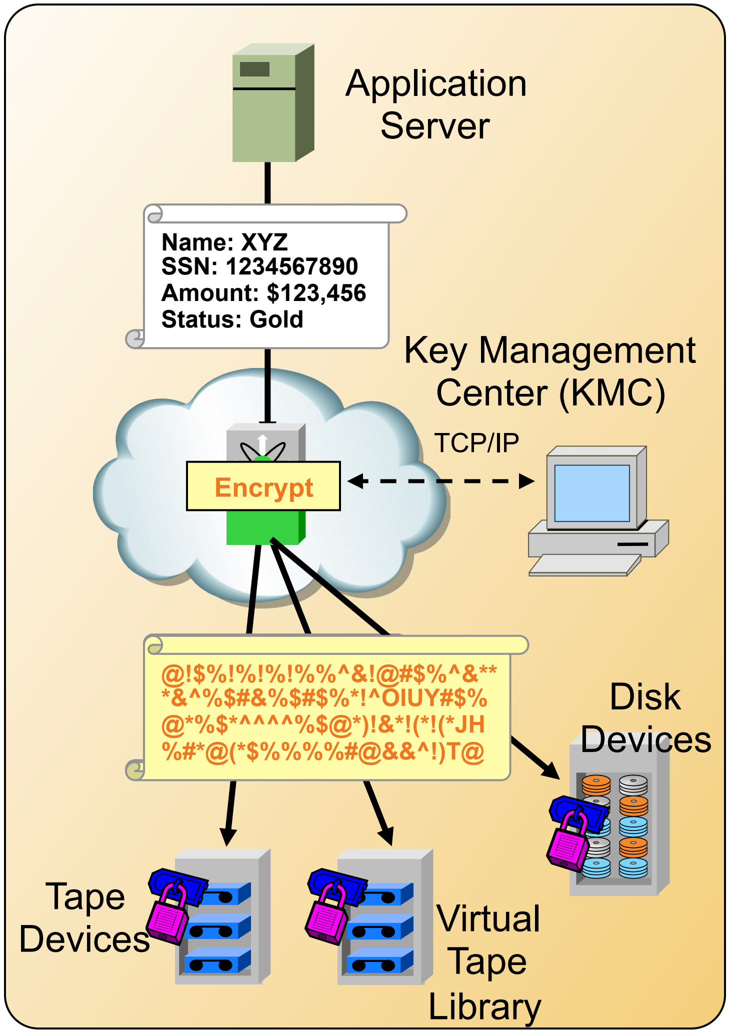
- Handles traffic from any VSAN in fabric
- Compresses tape data equal or better than tape drives
- Offline data recovery tool decrypts tape without MDS 9000 using Linux server

Delivering Encryption as a SAN Service



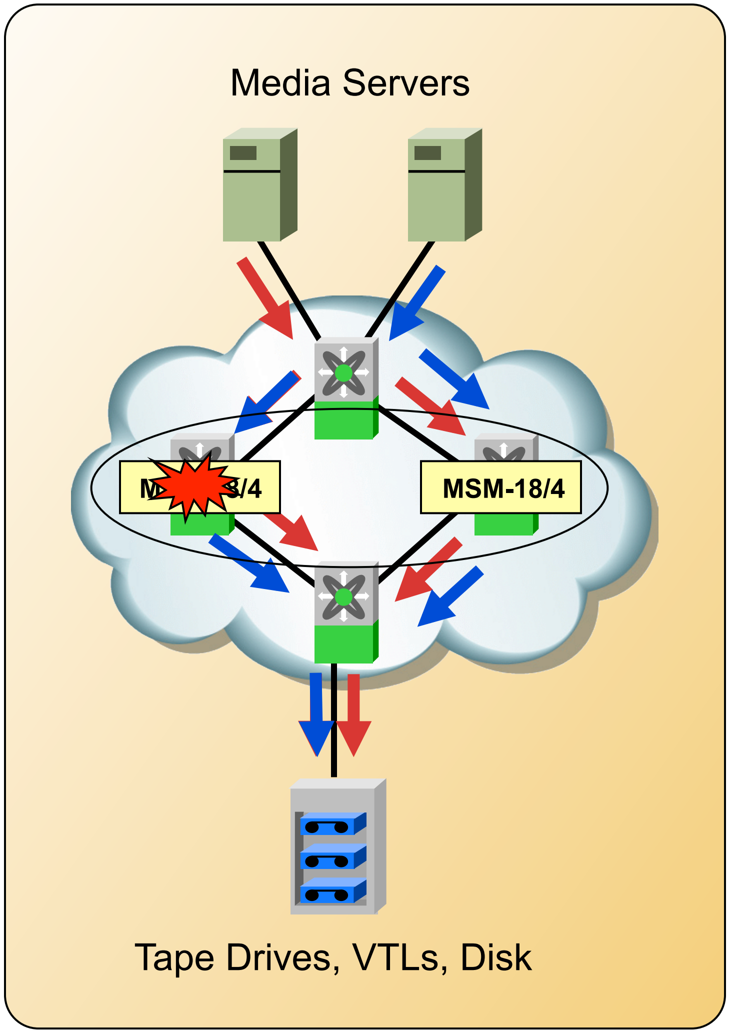
1. Insert Virtualization modules or use MDS 9222i switches
2. Enable Cisco SME and setup encryption service
3. Provision encryption for specific storage devices

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
- Compresses tape data
- Allows offline, software only media recovery

Cisco SME - Scaleable, Highly Available



- Integrates transparently in MDS fabrics
- Dramatically reduces deployment time
  - No SAN re-configuration or re-wiring to insert appliances
  - Provisioning becomes a simple, logical process of selecting what to encrypt
- Modular, clustered solution offers highly scaleable and reliable performance
- Load balances automatically
- Redirects traffic if a failure occurs
- Provisions quickly with Cisco Fabric Manager wizards

Agenda

- SAN Security Scope
- Cisco SAN Security
  - SAN Management Security
  - Fabric and Target Access Security
  - Fabric Protocols Security
  - IP Storage Security
  - Unified Fabric Access Security
  - Security for Data in Flight
- Storage Media Security
  - Security for Data at Rest
  - PCI DSS Compliance
- Summary

PCI Compliance

Payment Card Industry:
Data Security Standard (PCI DSS)

- Relevant if a primary account number (PAN) is stored, processed or transmitted
- Applies to all system components part of or connected to the cardholder data environment:
  - Servers
  - Networks
  - Applications
- Adequate network segmentation can reduce the scope of the cardholder data environment
- PCI DSS specifies 12 requirements
- How MDS helps customers being compliant

Build and Maintain a Secure Network

1

Use a firewall to protect cardholder data

- MDS network devices are likely used in internal network zone only
- Use SNMPv3 and ssh for management
- Create a protected internal IP network for iSCSI
- Segment the SAN using virtual SANs

2

Do not use vendor-supplied default password

- MDS NX-OS can enforce the use of passwords compliant to PCI

Protect Cardholder Data

3

Protect stored cardholder data

- Deploy SME to protect data at rest
- Store the keys in the Cisco key management server or in a secure third-party key manager as RSA KM
- VSANs provide additional segmentation and abstraction to implement the appendix-B compensating control if needed

4

Encrypt data across public networks

- Use MDS TrustSec for FC encryption across dark fiber/MANs
- Use FCIP over IPsec tunnels for SAN extension

Maintain a Vulnerability Mgmt Program

5

Antivirus

- Not applicable to NX-OS

6

Develop and maintain secure systems and applications

- Use a test VSAN to validate any new configuration before production
- NX-OS has been developed with secure coding guidelines and tested against common vulnerability

Implement Strong Access Control Measures

7

Restrict access by business need-to-know

- MDS security features make it the ideal platform to enforce this. VSANs, advanced zoning, fabric binding, port security, FC-SP authentication and RBAC with SNMPv3 and ssh
- RBAC in particular, if used in conjunction with VSANs, is especially designed to support a tight partitioning of the physical infrastructure

8

Assign a unique ID to each user

- Create an individual account for each administrator with strong password
- Authentication can be performed using the external AAA server of choice (e.g., TACAS+), to implement the desired policy of user authentication and password management

Implement Strong Access Control Measures

9

Restrict physical access to cardholder data

- Media can be encrypted using SME, that provides tools to transfer the key information to share data with a partner, secure the data transferred via courier
- SME can instantaneously cryptographically shred the data without destroying the physical media, that may be recycled

Regularly Monitor and Test Networks

10

Track and monitor all access to network resources and cardholder data

- Fabric Manager server provides continuous monitor of the SAN, it allows to establish criteria and thresholds to generate real time alarm and call home
- Syslog offers detailed entries, it may be redirected to a log server to consolidate monitoring the IT infrastructure
- Note that the log never contains application data

11

Regularly test security systems and processes

- Fabric Manager server provides the configuration and topology information needed to design, schedule, and execute such a test

Maintain an Information Security Policy

12

Policy that addresses information security for employees and contractors

- NX-OS can automatically disconnect unused management sessions
- RBAC allows a clear responsibility assignment for administrators
- Detailed logging supports a detailed audit

Agenda

- SAN Security Scope
- Cisco SAN Security
  - SAN Management Security
  - Fabric and Target Access Security
  - Fabric Protocols Security
  - IP Storage Security
  - Unified Fabric Access Security
  - Security for Data in Flight
- Storage Media Security
  - Security for Data at Rest
  - PCI DSS Compliance
- Summary

Summary

SAN Security Review

- SAN security scope
- Cisco MDS9000 security
  - SAN management security (secure protocols, RBAC, log)
  - Fabric and target access security (fabric binding, port security, authentication, zoning)
  - Fabric protocols security (FCSP, static config, certificates)
  - IP storage security (authentication, secure transport)
  - Data in flight (Cisco TrustSec, FCIP over IPsec)
  - Unified Fabric (AAA, RBAC, VSANs, zoning)
- Security for data at rest: storage media encryption
  - Architecture, key management, HA
  - Configuration options
- PCI DSS compliance: requirement analysis

Conclusions

- As SANs continue to grow and expand outside the data center, security becomes increasingly a concern
- Cisco offers a comprehensive set of security features in the MDS 9000 family
  - No impact on switch performance
  - Data path features are all hardware-based
  - Access, control, multiprotocol, data in flight and data at rest
- Security features are securely managed through Cisco's Fabric Manager
- The adoption of the Cisco MDS 9000 family security feature is a step forward in achieving compliance to applicable regulations

Q and A

References

- Cisco Storage Networking
    - http://www.cisco.com/go/storagenetworks
- Standards:
    - http://www.t10.org (SCSI specs)
    - http://www.ietf.org/html.charters/ips-charter.html (IETF ips wg)
    - http://www.t11.org (FC-SP specs)
    - ftp://ftp.t11.org/t11/pub/fc/sp/06-157V3.PDF(FC-SP v1.8)
- Forums:
    - http://www.snia.org
    - http://www.snia.org/ssif

CISCO