Fabric Security

(Securing the SAN Infrastructure)

Daniel Cohen

Solutioneer

Brocade Communications Systems, Inc

Agenda

- Why Secure a SAN?
- SAN Security Threats – Weaknesses
- Fabric Security Controls
- Security Management
- Cryptographic Mechanisms and Standards
- Brocade Product Architecture
- Brocade Security
  - Secure Fabric OS Controls and Policies
- Brocade Security Management
- Cryptographic mechanisms
- Field Upgrades – Compatibility
- Future Security Capabilities
- Additional information
- Q and A

Why Secure a Storage Area Network?

- Security is a fundamental requirement for an enterprise Storage Area Network, just like any other network
- Physical monitoring and management is no longer operationally feasible or cost-effective as Storage Area Networks increase in size and complexity
- Multi-tenant environments have new security requirements
  - Security enables sharing of SAN resources among multiple customers securely
  - Reduces xSP infrastructure costs and enables economies of scale

General SAN Security Weaknesses

- Inadequate (or granular) administrator access control
- Lack of strong or binding authentication among SAN devices (switches and servers)
- Inadequate control and granularity in SAN Management access and policy distribution
- Lack of privacy for sensitive management data such as passwords

Inadequate Administrator Access Control

- SAN fabrics require more controls to prevent inadvertent or unauthorized access to:
  - A switched fabric to prevent access to sensitive information (i.e., zoning data, security policies, etc.)
  - SAN fabric switches through unprotected connections (i.e., switch serial ports, etc.)
  - The front panel of fabric switches and other SAN infrastructure devices
- SAN fabrics require more granularity in management access controls
  - Multiple user or administrator profiles

Lack Of Strong Authentication

- Without authentication, SANs are susceptible to:
  - Spoofing – a host signing on with a phony WWN in order to get unauthorized access to devices or data
    - Zoning is not strong enough protection as it does not control access to the fabric
    - Zoning limits access ***after*** the hosts have logged on
  - Denial of service attack - unauthorized host application gaining access to the fabric and sending out a high volume of dummy management messages or I/Os to a LUN it does not own
  - Rogue devices could be added to the fabric either intentionally or inadvertently
    - Either way the integrity of the SAN has been impacted

In Adequate Controls in SAN Fabric Management Access

- The need to control how a SAN fabric is managed
  - Preventing SAN fabric switches (or other elements) from arbitrarily changing security policies and parameters (including zoning)
    - Centralization of security policies and configuration
    - Secure distribution of all such policies form a trusted source – asymmetric management model
  - Ability to turn ON/OFF or otherwise control certain management access to the fabric
    - Open management ports are an easy way to gain unauthorized access and modify system parameters
  - Control of end points accessing management facilities within the fabric (management consoles, clients, etc.)
  - Remote management access over public networks

Lack Of Data Privacy (Management)

- Encryption is required to eliminate eavesdropping threats
  - Cleartext passwords and other data
    - Corporate policy for ensuring that no cleartext passwords are used
  - Unprotected Remote Access
    - The need to encrypt management traffic (i.e., using SSL and SSH)
  - Unauthorized analysis on the Fibre Channel line or other interfaces to analyze management or data traffic (i.e, Sniffers)

SAN Security – An Infrastructure Decision

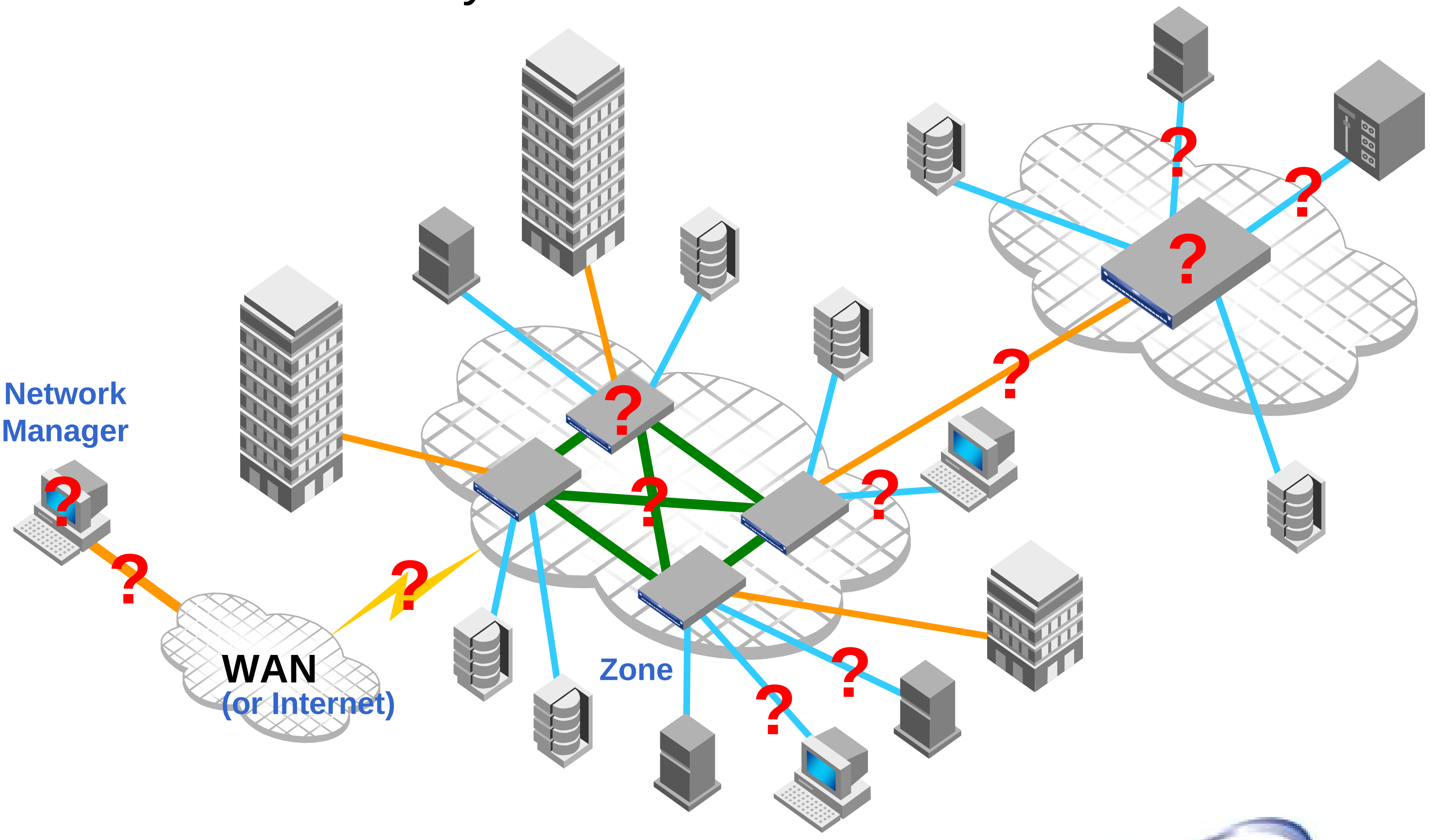
Security is a fundamental consideration when designing a SAN and selecting SAN infrastructure

As with any network, SAN security must be:

- Robust
- Scalable
- Policy-based
- Standards-based using proven mechanisms
- Manageable
- Auditable

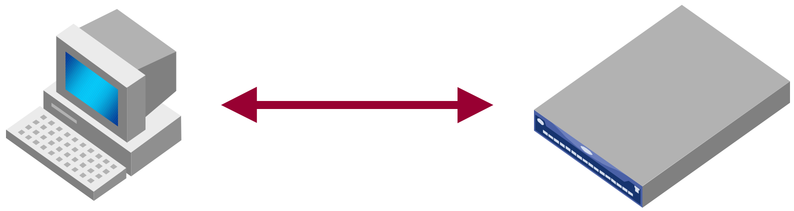
A Secure SAN Infrastructure

? = Potential Security Control Points

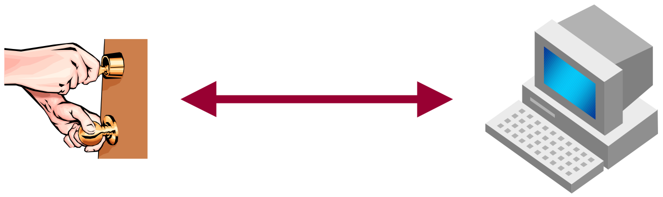


Fabric Security Domains and Vulnerabilities

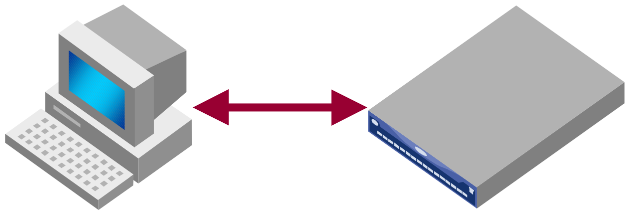
- Host to Fabric



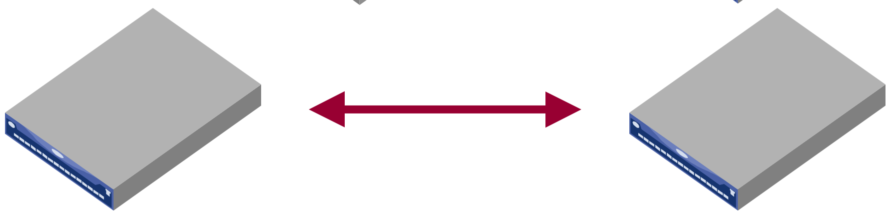
- Fabric/Security Manager Access



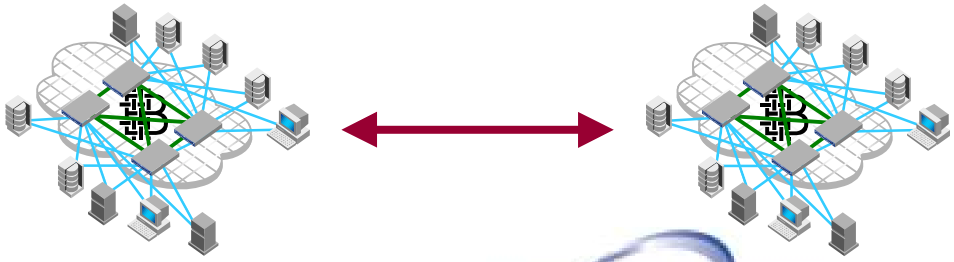
- Management Application to Fabric



- Switch to Switch

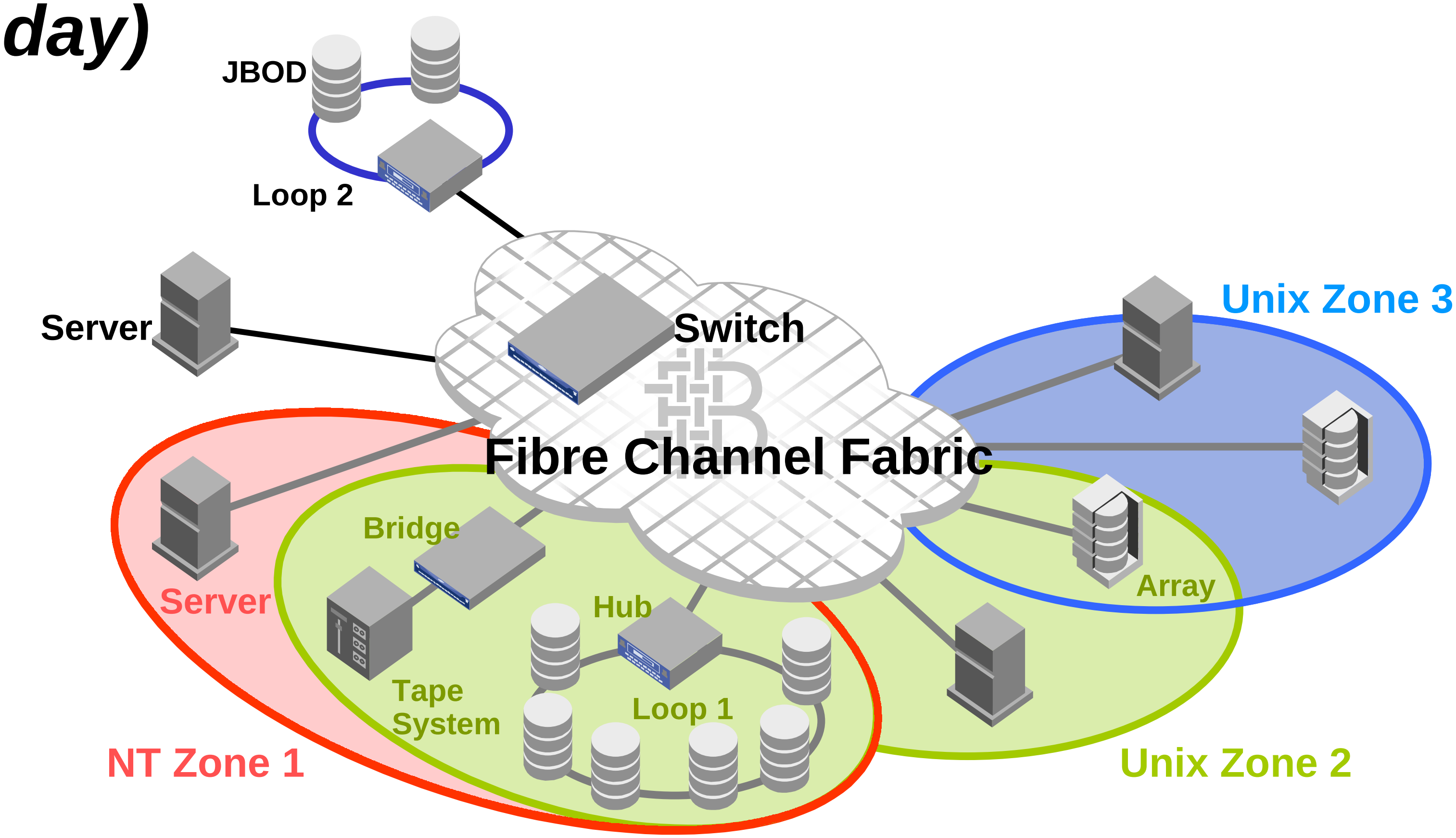


- SAN to SAN



NOTE: ***The storage element/device <u>content</u> security is not within the fabric security domain!***

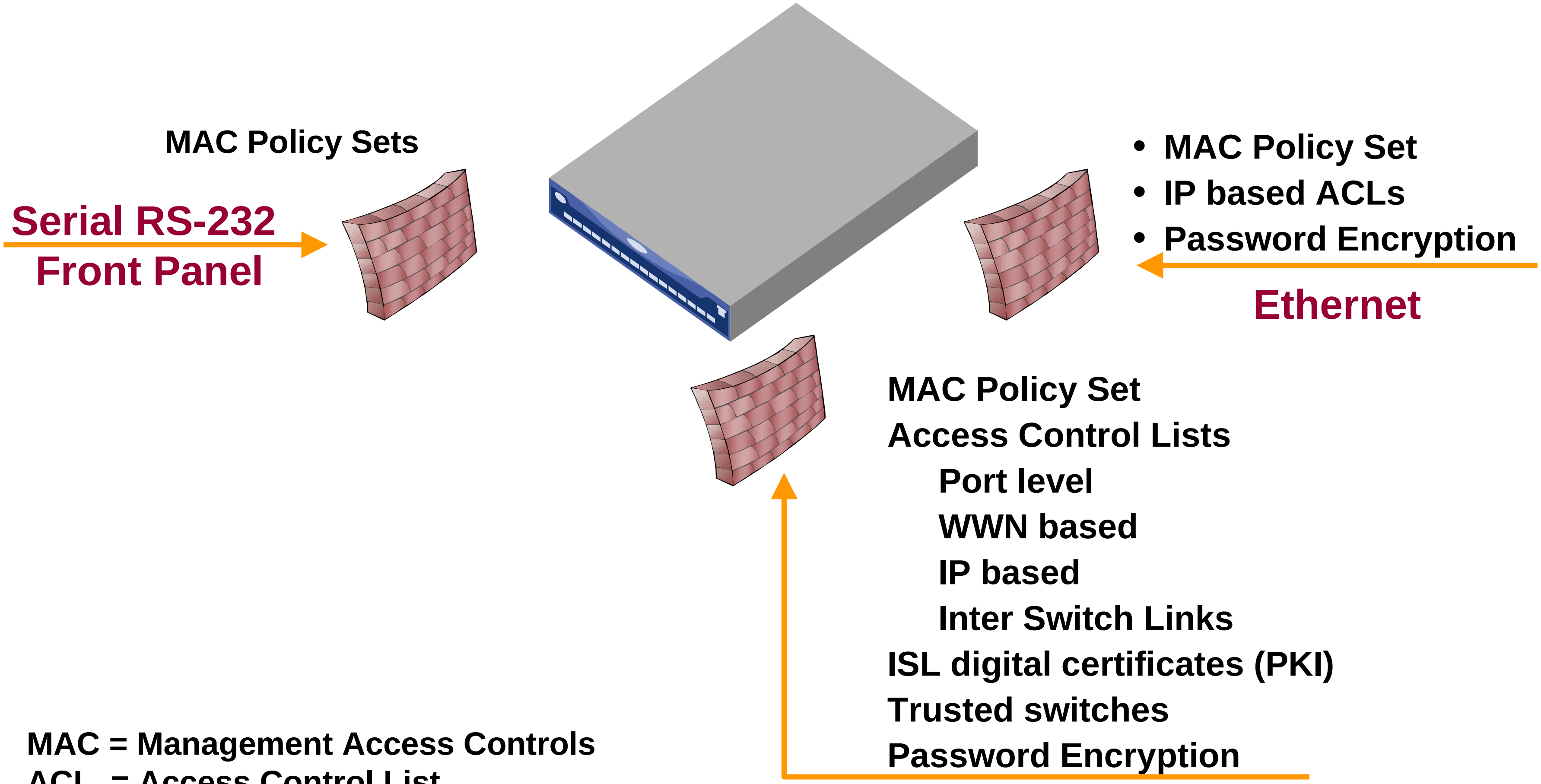
Zoning – *Association of Storage with Servers (Today)*



Zoning is the logical association of storage with servers

- Used for access control (I.e. Enables heterogeneous Fabrics)
- Must be hardware enforced

Fabric Security Controls



MAC Policy Sets

Serial RS-232
Front Panel

- MAC Policy Set
- IP based ACLs
- Password Encryption

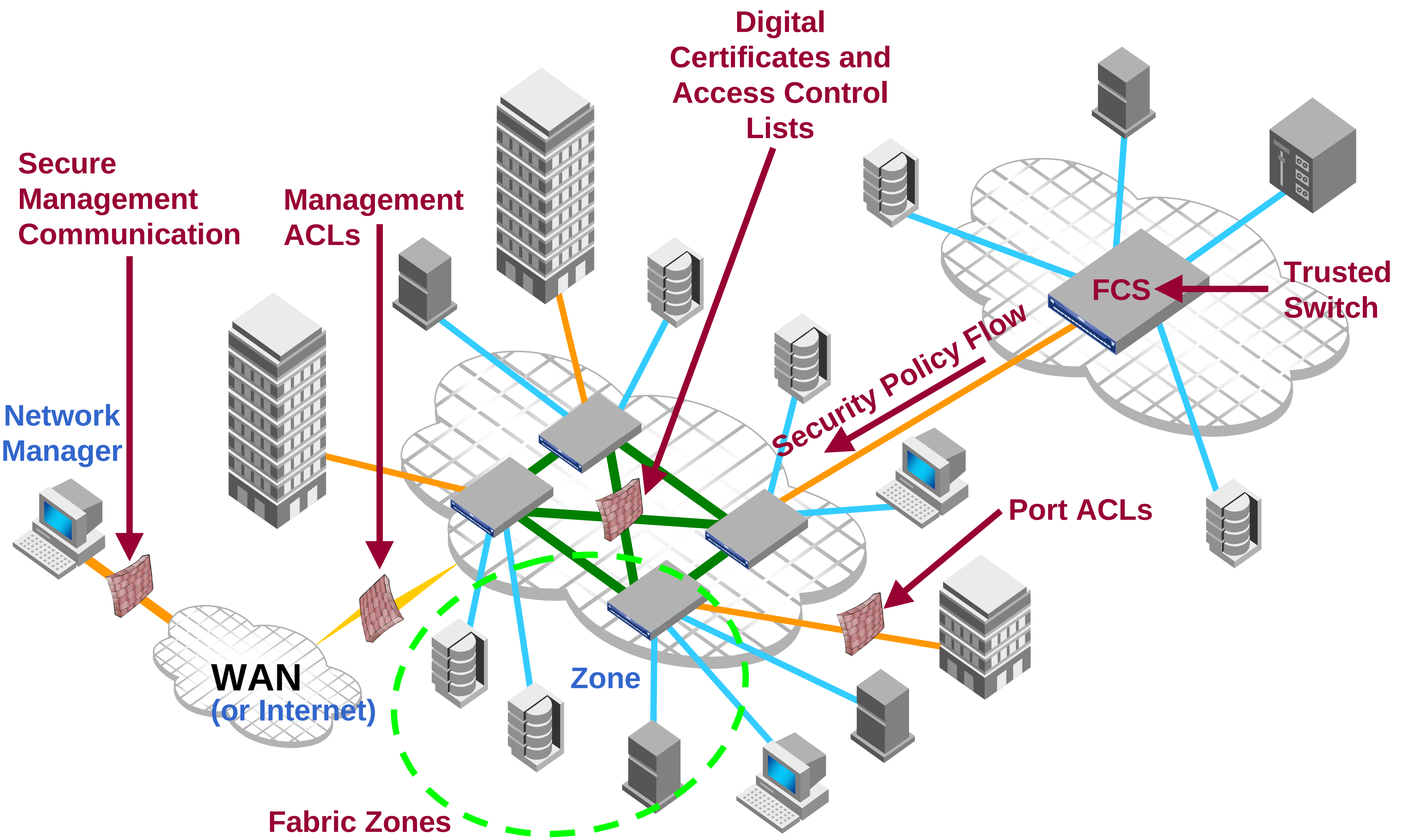
Ethernet

MAC Policy Set
Access Control Lists
  Port level
  WWN based
  IP based
  Inter Switch Links
ISL digital certificates (PKI)
Trusted switches
Password Encryption

In-Band (FC)

MAC = Management Access Controls
ACL = Access Control List
ISL = Inter Switch Link

A Secure SAN Infrastructure



Security Threats and Best-in-Class Solutions

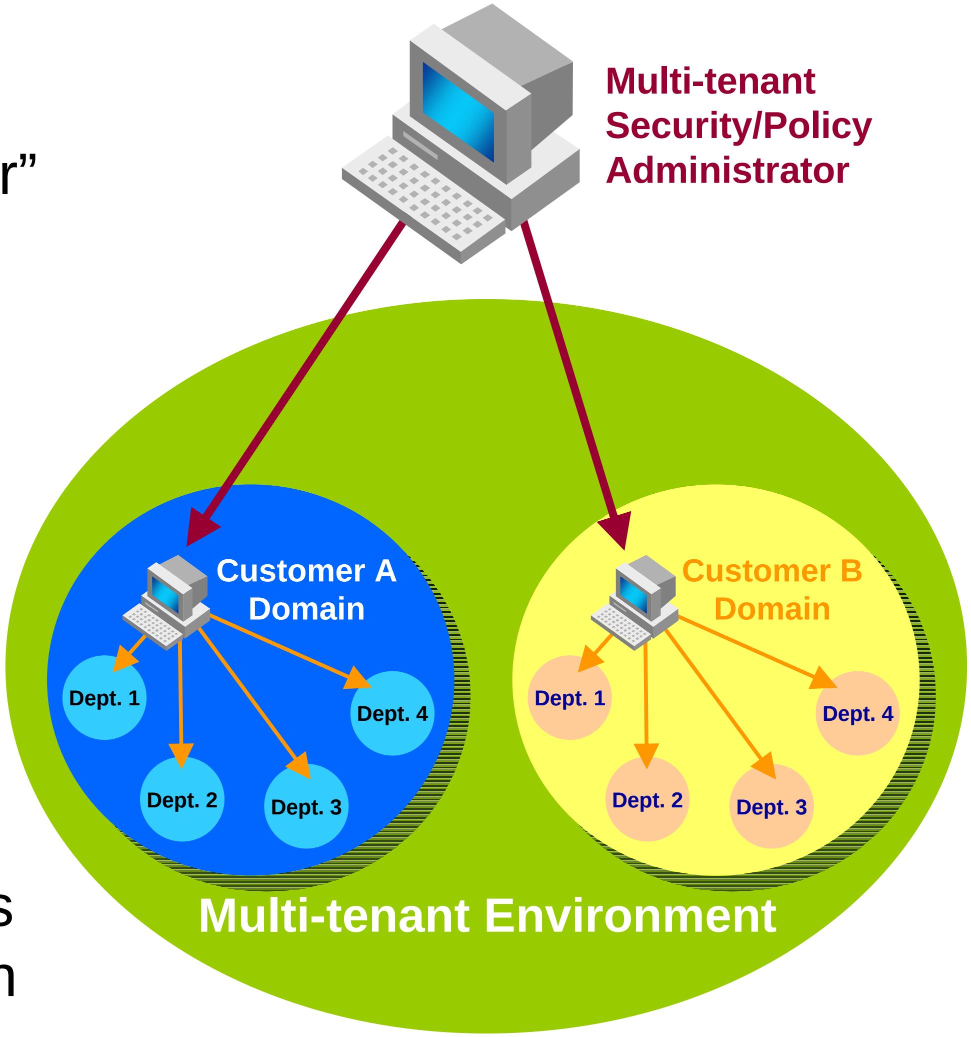
Threat / Risk	*Best-In-Class Solutions*
Unauthorized / Unauthenticated User Access	- Multilevel password control and encryption - Strong authentication – Integrate with customer's existing infrastructure (I.e. RADIUS / TACACS+)
Insecure Management Access	- Management access control policies - Encrypt management information (user name and password) where applicable Other Solutions : SSL, SSH, IPSEC
Spoofing of Device Names (WWNs)	- More granular access control for hosts/servers (at the switch port level) - Strong in-band authentication of SAN fabric logon attempts
Management Controls From Uncontrolled Access Points	- Asymmetric management approach such as Trusted switches to set security controls - Use of strong authentication (PKI)

Security In a Multi-Tenant Environment

- The Security/Policy administrator creates “customer” domains

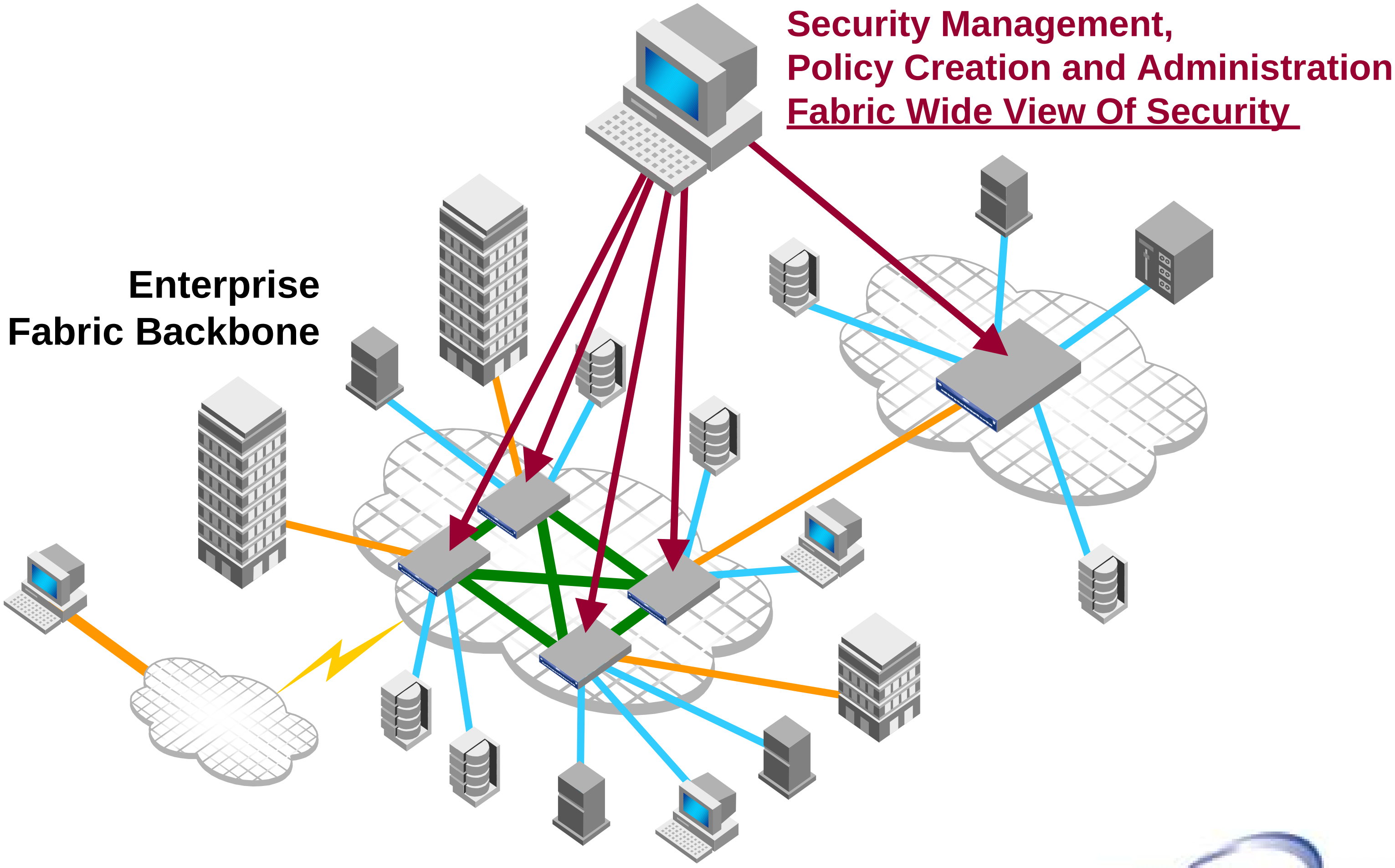
- The Security/Policy administrator assigns specific access privileges to each “customer” for controls within their own domains

- Each customer will establish security boundaries and access policies within their own domain



Fabric Security Management and Administration

- Must provide a fabric wide view of security



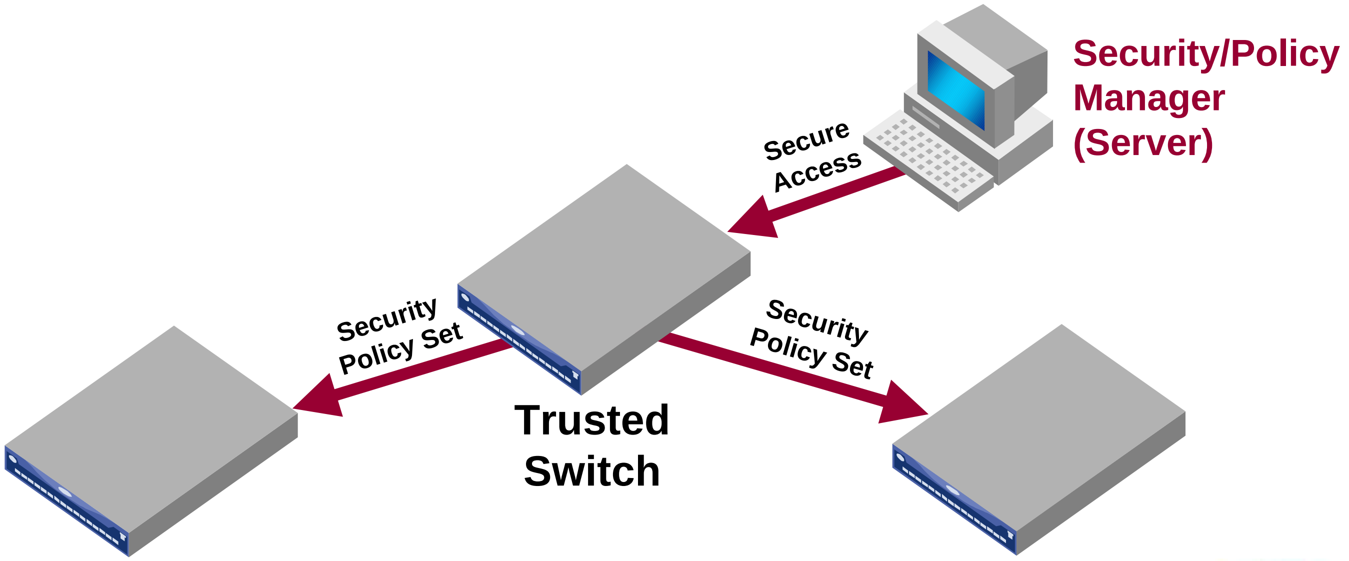
Security Management,
Policy Creation and Administration
Fabric Wide View Of Security

Enterprise
Fabric Backbone

Manager to Fabric Communication

Management application security functions:

- Authentication of switches
- Secure access (encrypted password and other data)
- Secure software download
- Control or distribution of security policies



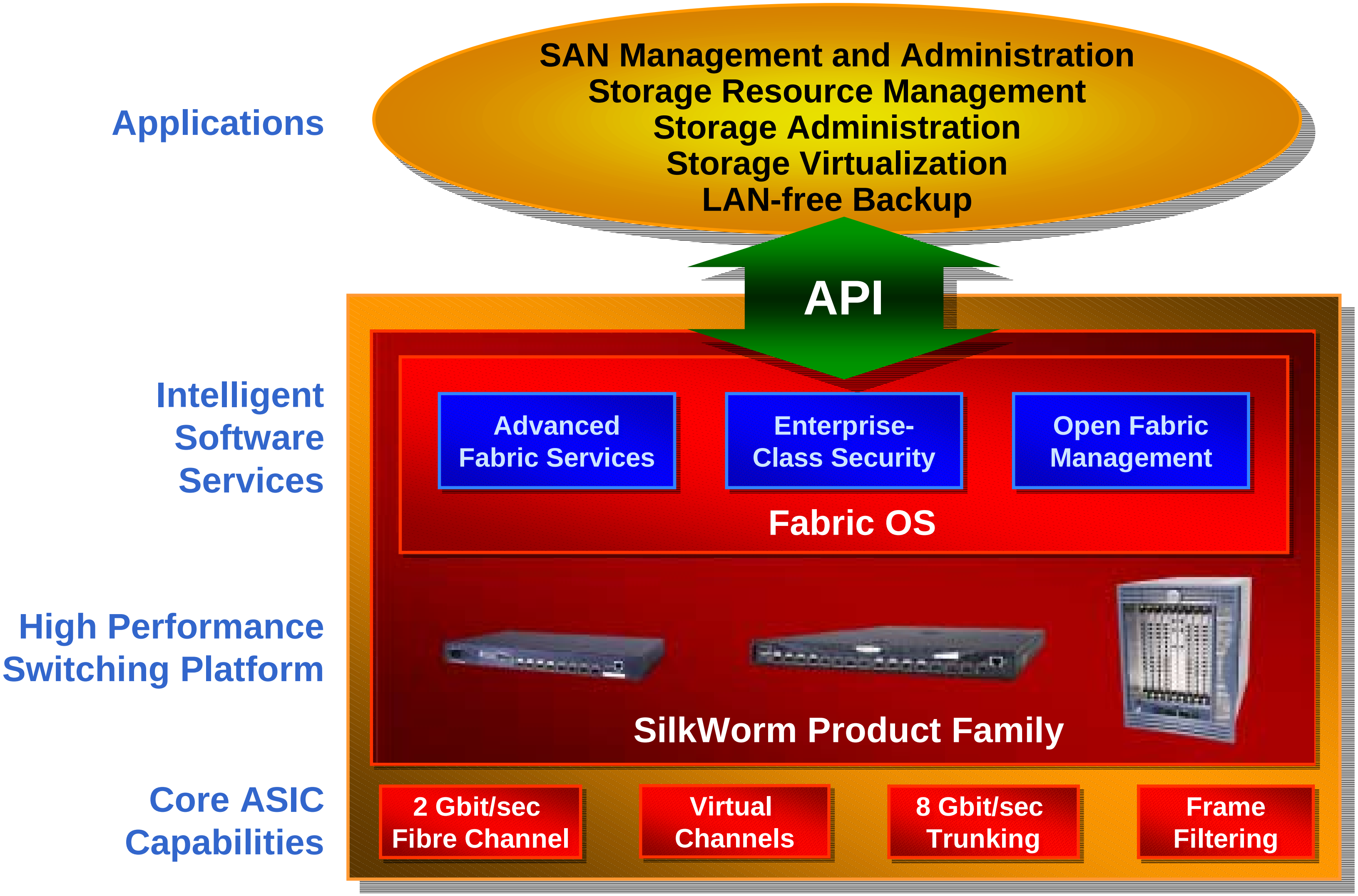
New and Proposed Standards Activities

- Switch Link Authentication Protocol (SLAP) based on ISO/IEC 9798-3 protocol, optimized for SANs – (has been implemented) – Brocade
- SLAP has been Extended to FCAP (Fibre Channel Authentication Protocol) to include end-device authentication and Diffie-Hellman based key agreement
- iSCSI - IPSEC (ESP) and SRP (No implementation in SANs)
- FC - ESP based Security - Requires comprehensive changes in the infrastructure (No implementation – Early proposal stage
- Karthika has proposed an analysis of the Key-Server. They are on the hook to bring in some enhancements
- Brocade has proposed the Brocade Security Architecture based on policies
- Security study group is now a T11 security project (FC-SP) that will produce a standard. Brocade chairs the group

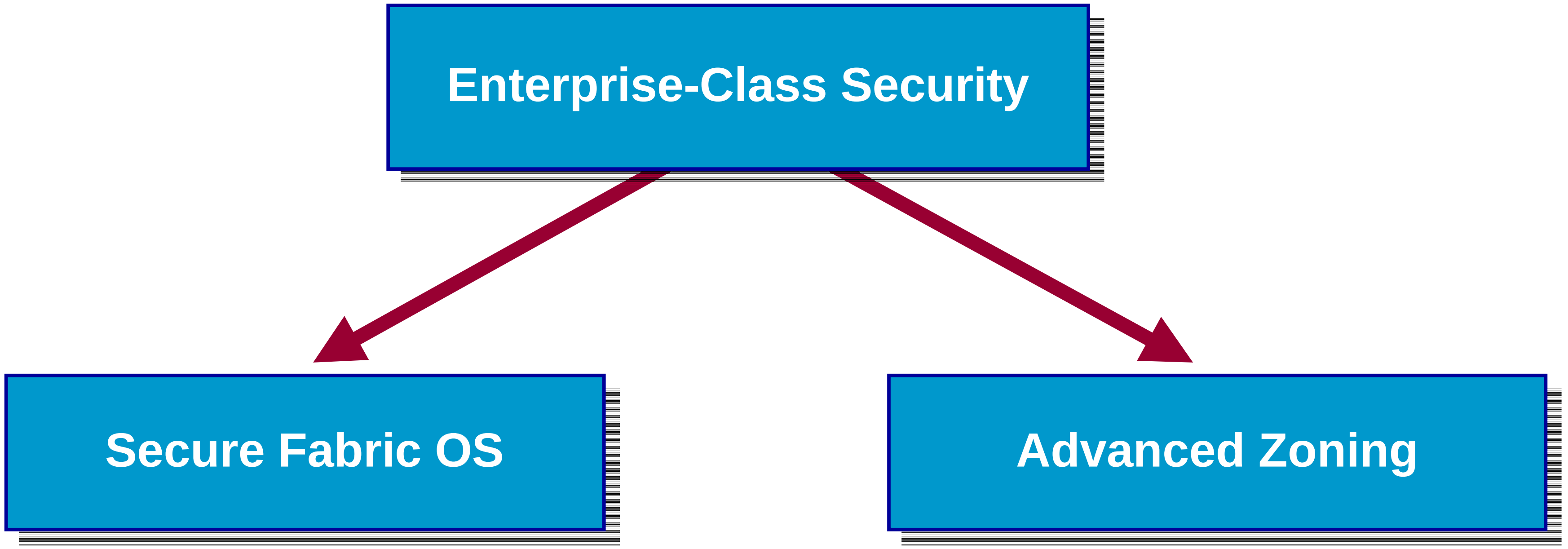
Brocade Security

Secure Fabric OS

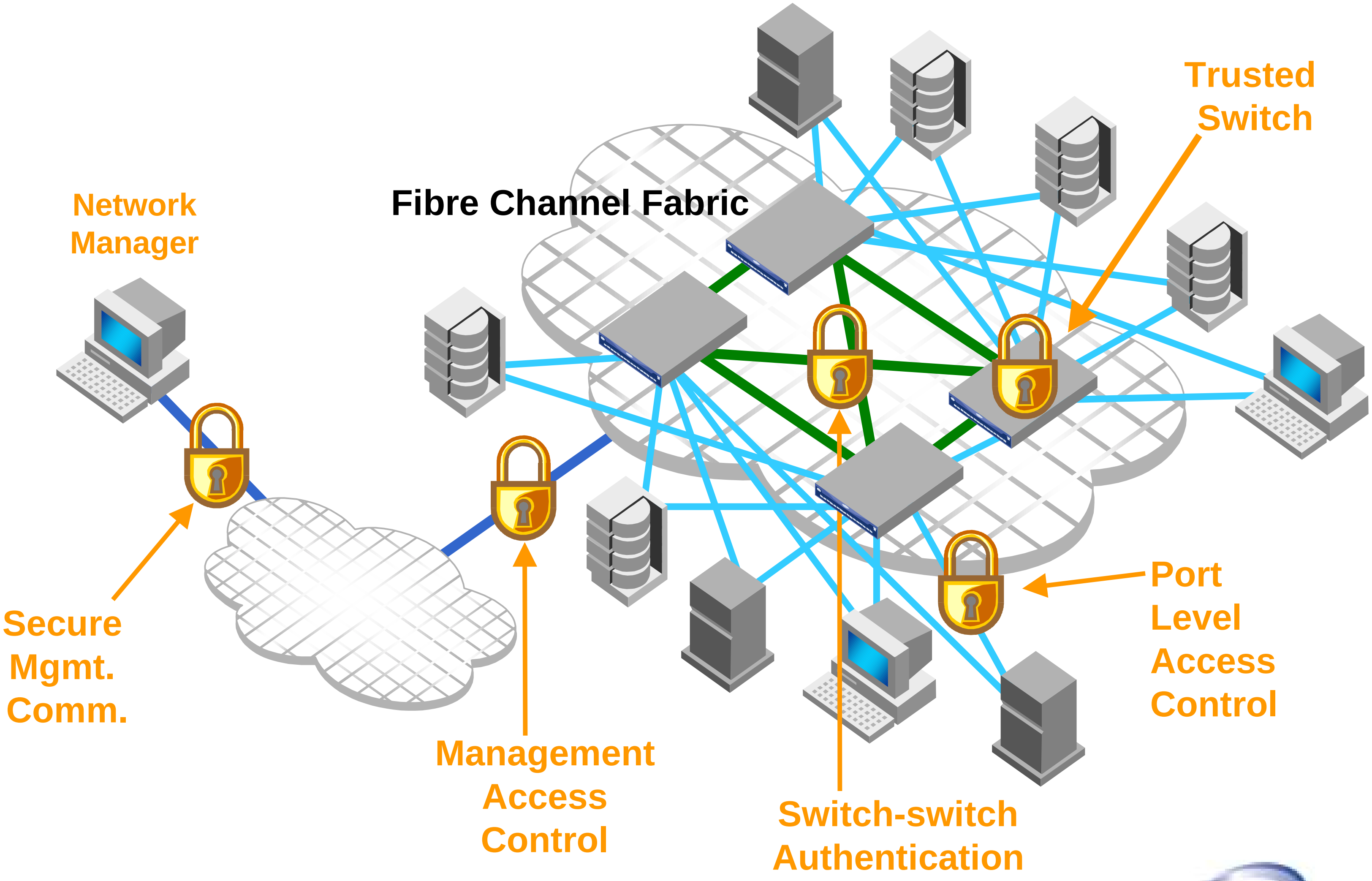
Brocade Intelligent Fabric Services Architecture



Brocade Enterprise-Class Security



Secure Fabric OS –
Securing The SAN Infrastructure



Fabric Management Policy Sets (FMPS)

- Fabric security is managed through policies
- The FMPS consists of the following policies:
- Fabric Configuration Server (FCS) Policy (Trusted Switch) – ***Required***
- Management Access Control (MAC) Policies - Controls Telnet, HTTP, SNMP, SES, MGMT SRVR and API Access
- Device Connection Control (DCC) Policies - Port level Access Control Lists
- Switch Connection Control (SCC) Policy – Switch level Access Control Lists
- Options Policy – Controls whether the use of Node WWN can be used for WWN-based zoning

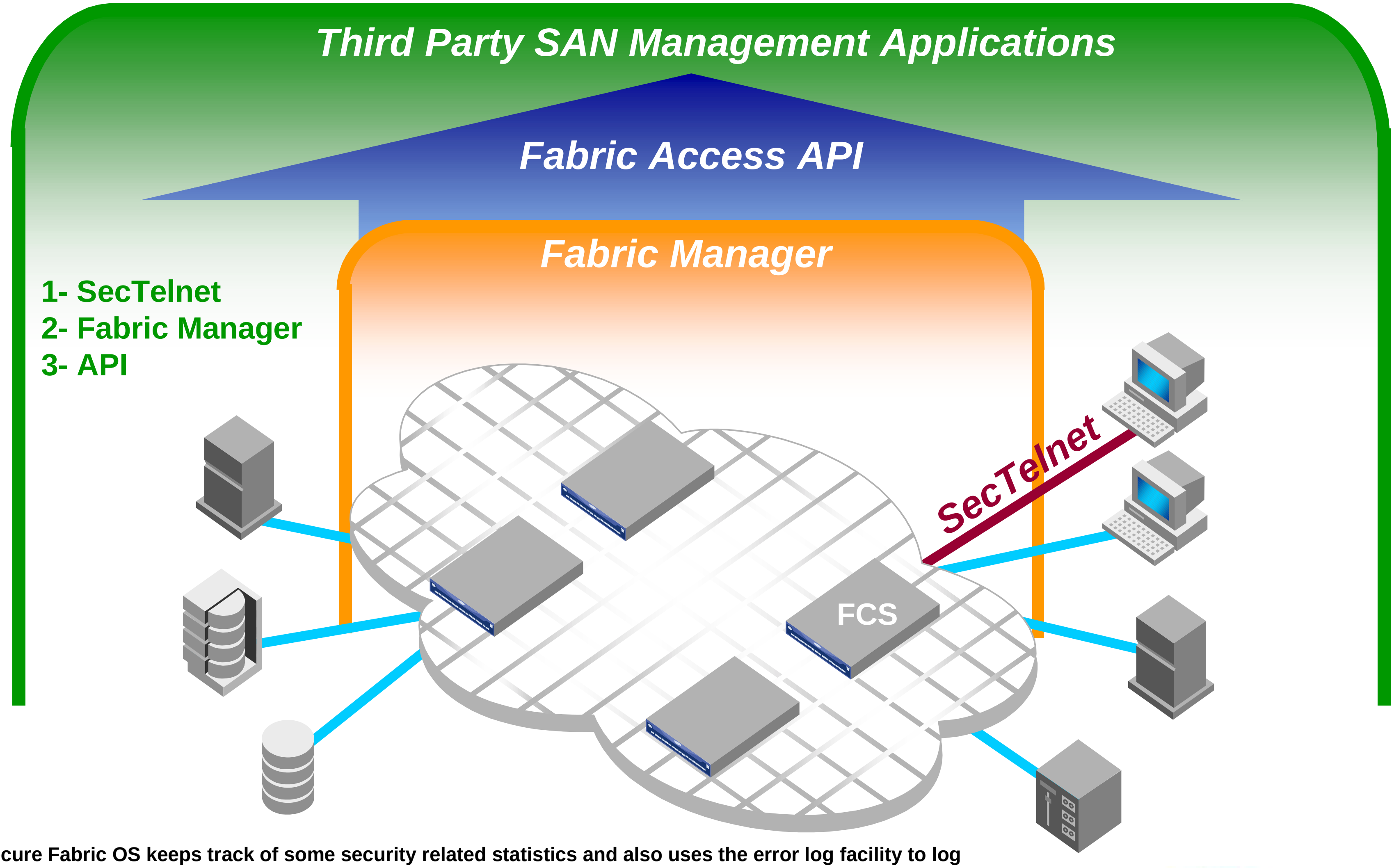
Automatic Security Functions

- The following features are not based on any particular security policy and are initiated automatically in Secure Mode
- Inter-Switch Authentication
  - Switch Link Authentication Protocol (SLAP)
- Digital signatures and time-stamping of security and zoning configuration data distributed from the trusted switch
- Encryption of passwords
  - SecTelnet, Fabric Manager, Web Tools, API

Secure Fabric OS Benefits

- The product provides the ability to:
- Secure the SAN infrastructure from unauthorized / unauthenticated management and device level access
- Share resources within the same fabric by tightly controlling where devices (servers/hosts) can attach
- Ensure a secure means for distributing fabric wide security and zoning information (trusted switch)
- Protect sensitive management data against eavesdropping
- Create a “trusted SAN infrastructure”

Security Policy Management



The Secure Fabric OS keeps track of some security related statistics and also uses the error log facility to log security related events. (e.g., all policy violations are tracked by the security statistics and entered in the error log)

Brocade Management – Family Overview

Integrated Administration Applications
(EMC, Veritas, BMC, SUN, Compaq, …)

Fabric Manager

- Host-based app
- Centralized management platform
- Aggregate mgmt info
- /Multi-fabric admin console
- Hierarchical drill down and fine grain detail
- Distributed architecture supports current and future products

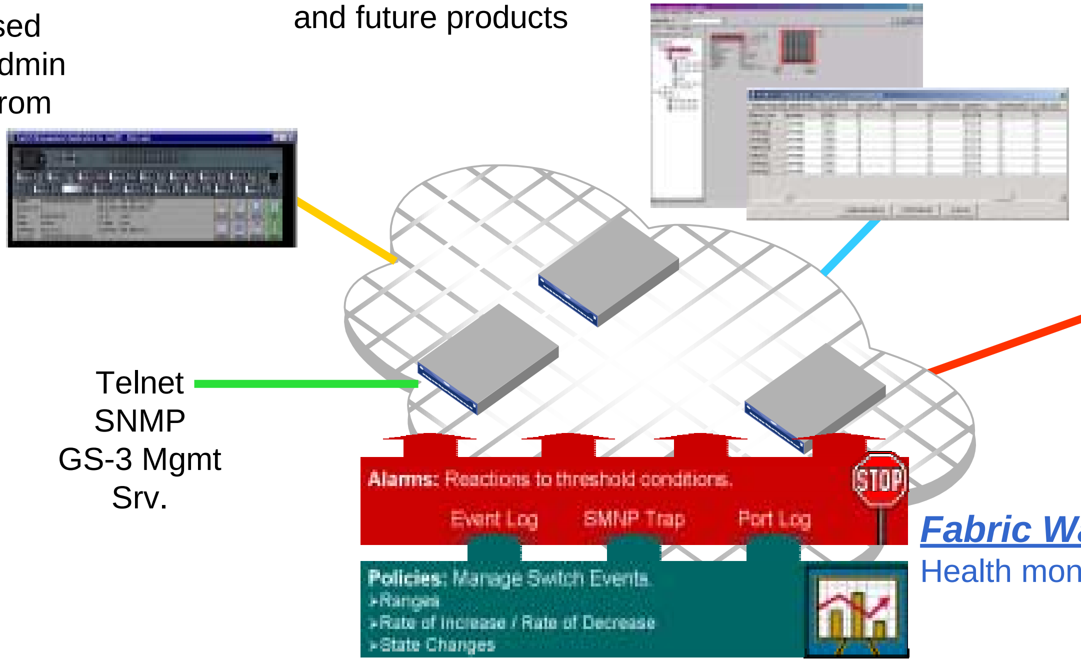
Fabric Access

***Fabric Access Layer* API**

- Integrate SAN management with higher-level management applications
- C/XML Host library
- Full access to core switch/fabric capabilities
- CIM compatible

Web Tools

- Switch based
- Element focused
- Small fabric admin
- Self-delivery from any Silkworm

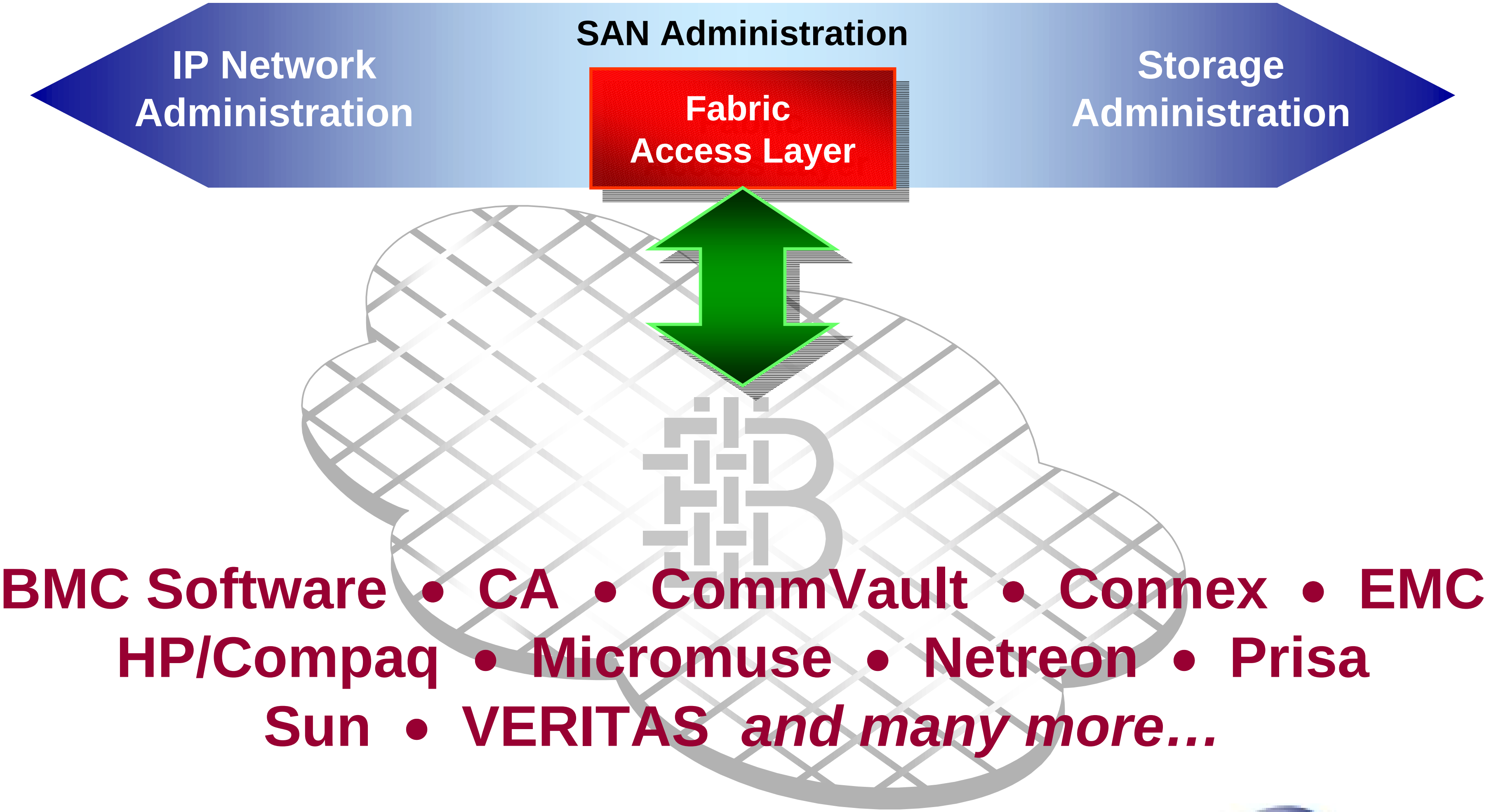

Alarms: Reactions to threshold conditions.
STOP
Event Log
SMNP Trap
Port Log
Policies: Manage Switch Events.
›Ranges
›Rate of Increase / Rate of Decrease
›State Changes

Telnet
SNMP
GS-3 Mgmt
Srv.

Fabric Watch
Health monitoring service

Open Fabric Management – API

End-to-End Integrated Management Applications



IP Network Administration

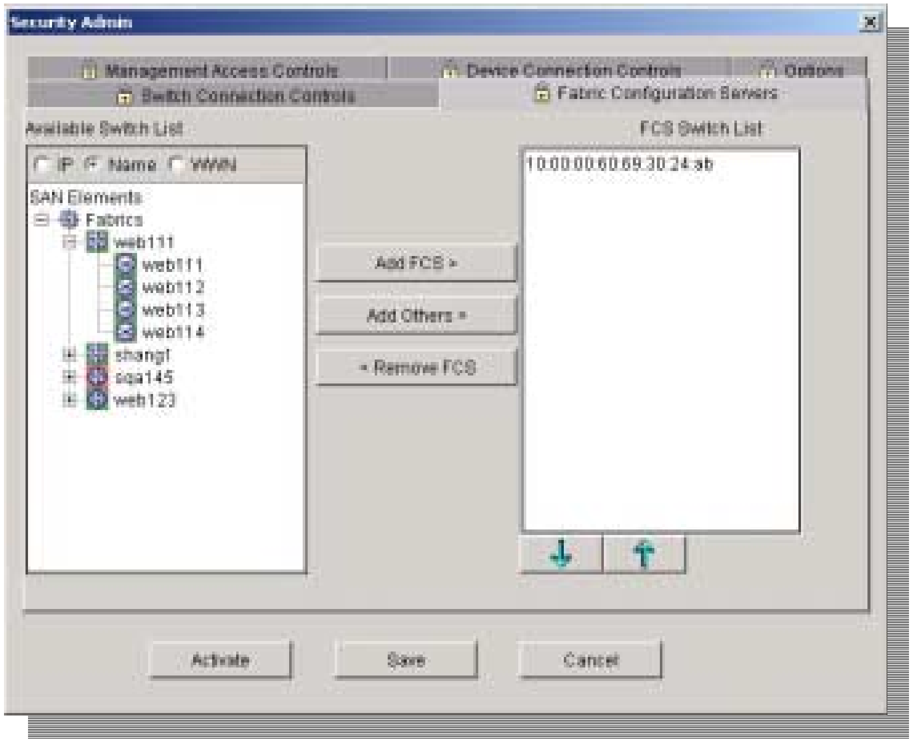
SAN Administration

Fabric Access Layer

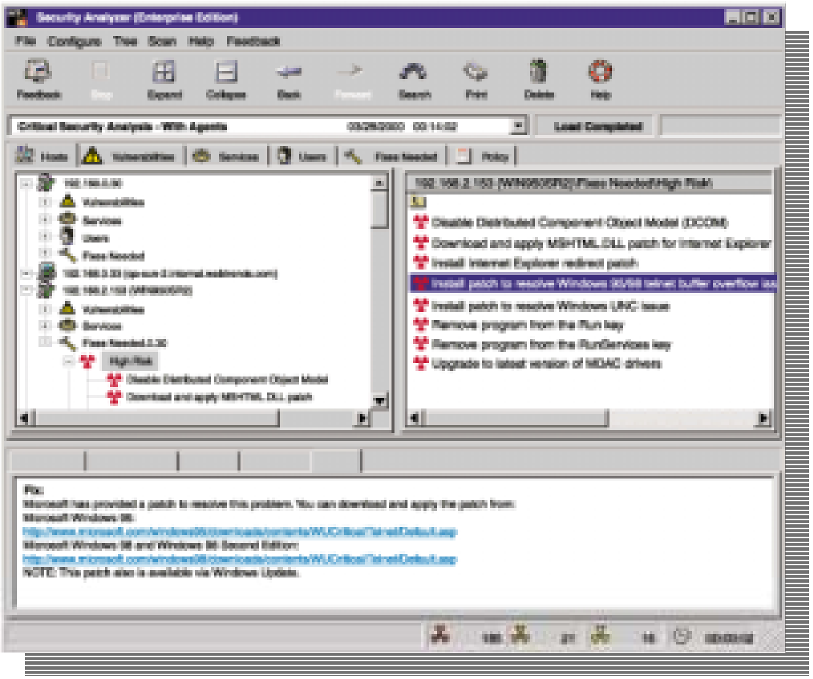
Storage Administration

BMC Software • CA • CommVault • Connex • EMC
HP/Compaq • Micromuse • Netreon • Prisa
Sun • VERITAS *and many more…*

Fabric Manager
Simplifies Security Policy Management



FCS Switch List: 10:00:00:60:69:30:24:ab


Security Analyzer (Enterprise Edition)
File Configure Tree Scan Help Feedback
Feedback
Stop
Expand
Collapse
Back
Forward
Search
Print
Delete
Help
Critical Security Analysis - With Agents
Load Completed
Hosts
Vulnerabilities
Services
Users
Fixes Needed
Policy
192.168.0.30
Vulnerabilities
Services
Users
Fixes Needed
192.168.2.33 (sprout-2.internal.webtrends.com)
192.168.2.153 (WIN9505R2)
Vulnerabilities
Services
Fixes Needed 2.30
High Risk
Disable Distributed Component Object Model
Download and apply MSHTML.DLL patch
192.168.2.153 (WIN9505R2)\Fixes Needed\High Risk\

- Disable Distributed Component Object Model (DCOM)
- Download and apply MSHTML.DLL patch for Internet Explorer
- Install Internet Explorer redirect patch
- Install patch to resolve Windows 95/98 telnet buffer overflow iss
- Install patch to resolve Windows UNC issue
- Remove program from the Run key
- Remove program from the RunServices key
- Upgrade to latest version of MDAC drivers

Fix:
Microsoft has provided a patch to resolve this problem. You can download and apply the patch from:
Microsoft Windows 95:
http://www.microsoft.com/windows95/downloads/contents/WUCritical/Telnet/Default.asp
Microsoft Windows 98 and Windows 98 Second Edition:
http://www.microsoft.com/windows98/downloads/contents/WUCritical/Telnet/Default.asp
NOTE: This patch also is available via Windows Update.

- **Security Policy control**
- **Security audit and reporting**
- **Multi personality**
  (manage secure and non-secure fabrics from a single console)

Compatibility – Field Upgrades

- Release 2.6, 3.1 and 4.1 will be backwards compatible with previous OS releases. However, not with the security enabled
- All switches in the fabric must be upgraded to v2.6 (and later 3.1 and 4.1) before security can be turned on in the fabric
- Segmentation will occur if older or unauthorized switches (not in policy) are kept or introduced in a secure fabric

Security/Cryptographic Mechanisms Secure Fabric OS

- RSA Public Key Encryption – 1024 bit keys
  - For Encryption of passwords between the manager and the switch
- AES (Advance Encryption Standard) – 128 bit keys
  - For Encryption of the Switch's Private Key which is used in digital signatures and password encryption processes
- ITU X.509 v3 Certificates
  - Assigned to each switch in the factory or out in the field for strong binding and authentication of its WWN as well as for other security functions
- RSA Digital Signatures
  - For authentication of switches in conjunction with their digital certificates
  - For signing of security parameters distributed from the FCS (trusted switch)
- Switch Link Authentication Protocol (SLAP)
  - Protocol used to authenticate switches (E-Ports) within a fabric
  - An instance of the Fibre Channel Authentication Protocol (FCAP)

Note: Brocade has received export approval for all (friendly) countries

Some Future Security Features

- Support for SSL and SSL protocols
- More detailed security logs and events (on-going)
- Security audit snapshot
  - Status of the fabric and its security configs/discrepancies
- More administrative and user domains
  - More roles, privileges, and hierarchies
- Support for third party CAs / PKIs
- Support for and co-existence with RADIUS, TACACS+, and Kerberos authentication facilities
- End point (i.e., host) authentication using FCAP
- Counter measures – policy-based
- Factory defaults – Security enabled or disabled

More information ….

- Current educational tools (all available on-line, Now!)
  - Secure Fabric OS White paper http://www.brocade.com/SAN/white_papers.jhtml
  - Secure Fabric OS Datasheet http://www.brocade.com/SAN/data_sheets.jhtml
  - Secure Fabric OS FAQ
  - Secure Fabric OS Users Guide (comprehensive)
  - Secure Fabric OS Best Practices Guide (comprehensive)
- Security Course – SFO100 – Available Now!
  - 2 Days - lecture and hands-on lab
  - Ideal for SAN administrators and other network professionals
- Legal – Certification Practices Statement (CPS) – Available Now
- Secure Fabric OS Software Availability
  - For The 2xxx Series 1G Switches - Available Now! (in R2.6)
  - For 2G Products – 2H’02 (TBD) – (in R3.1, 4.1)
- Contact your Brocade Partner or Sales Executive
- E-mail: info@brocade.com

Thank You

Brocade Communications Systems, Inc.