



## Podatkovni centri danas i sutra



***Siniša Mitrović, [smitrovi@cisco.com](mailto:smitrovi@cisco.com), systems engineer***  
***Goran Peteh, [gopeteh@cisco.com](mailto:gopeteh@cisco.com), systems engineer***

# CIOs Are Strengthening Support for Information and Transaction Systems

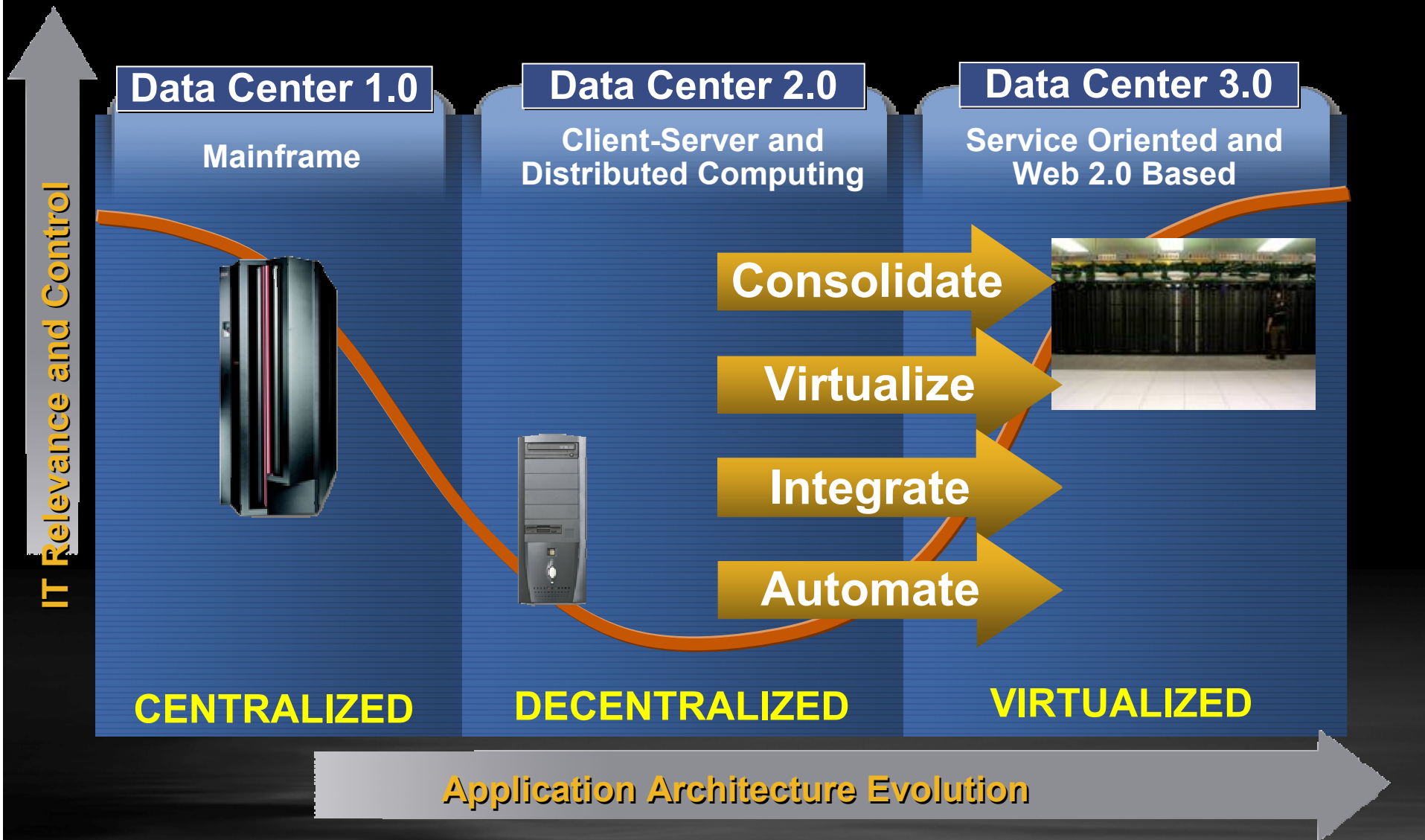
## Top 10 CIO Technologies

To what extent is each of the following a priority for you in 2007?

	2007		2006	2005	2007 Increase
Business intelligence (BI) applications	1	↔	1	2	12.4%
Enterprise applications (ERP, SCM, CRM, etc.)	2		*	*	10.5%
Legacy application modernization	3	↑	10	5	8.8%
Networking; voice and data communications (VoIP)	4	↑	8	7	8.2%
Servers and storage technologies (virtualization)	5	↑	9	10	8.4%
Security technologies	6	↓	2	1	9.3%
Service-oriented applications and architecture	7	↔	7	4	10.2%
Technical Infrastructure management and development	8	↑	12	**	6.6%
Document management	9		*	*	11.4%
Collaboration technologies	10	↓	4	*	8.8%

\*New question for 2007 \*\*New question for 2006

# Data Center and Network Evolution = Growth



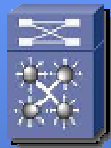
# A Comprehensive Portfolio for Data Center 3.0

## Unified Fabric Networking



Nexus 7000 Modular Switching System  
(Unified Fabric ready)

## Ethernet Networking



Nexus 7000  
Catalyst® 6500 Series  
Catalyst 4900M Top-of-Rack  
Catalyst Blade Server Switches

## Storage Networking



MDS 9500 Storage Directors  
MDS Fabric Switches  
Blade Switches  
(Unified Fabric ready)

## Application Network Services



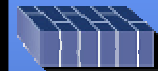
ACE Application Delivery – Module and Appliance  
Wide-Area Application Services  
ACE XML Gateway

## Infiniband Clustering



SFS 7000 Infiniband Switch  
SFS 3000 Infiniband Gateway

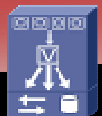
## Data Center Security



Firewall Services Module

## Data Center Provisioning

VFrame Server/Service Provisioning System



## Data Center Management

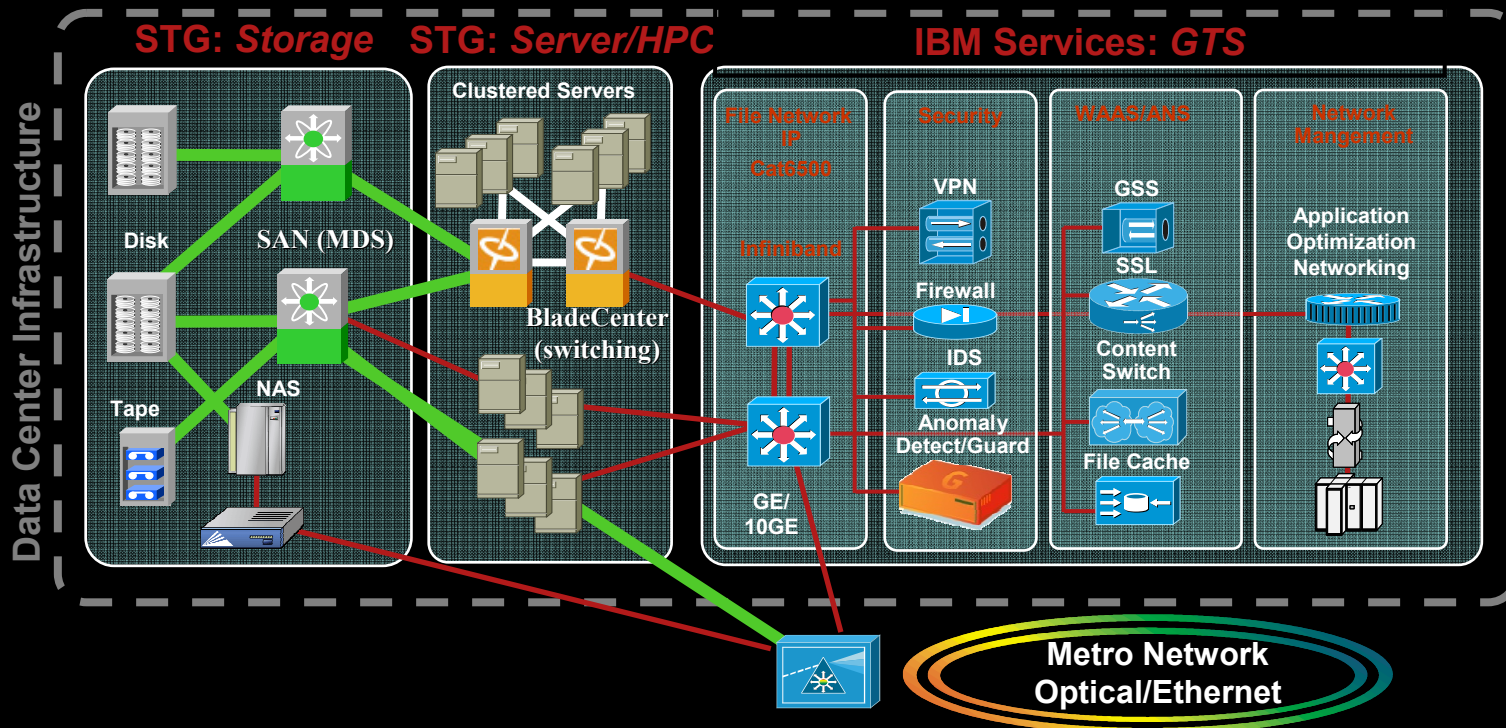
Data Center Network Manager– Topology Visualization and Provisioning

ANM– Advanced L4-7 Services Module Management

# Cisco Data Center Opportunity

A computing, storage and networking portfolio for the Data Center

*Cisco products integrated and/or working with IBM servers, Software, Storage and Services*



## Challenges in today's Data Center:

- Underutilization: server & storage bloat
- Real estate: floor space; cooling; electricity
- Complexity: server/storage operations & management driving up costs
- Regulatory: security; privacy; availability

# Cisco and IBM Relationship Today

## Industry and Horizontal Solutions

- Banking and Insurance
- Retail
- Public Sector
- Energy & Utilities
- Automotive
- SMB
- Unified Communications Solution
- Data Center Solution
- Integrated Security Solutions
- Wireless Offerings
- Storage Offerings

## Demo Capabilities

- 300+ Joint Competency Centers
- UC innovation facilities WW
- Retail and FSS Exec Briefing Centers

## IBM Global Services

- Robust portfolio of service offerings for Cisco (assess, design, install, manage)



## Technology Collaboration

- Software and Hardware
- Tivoli, WebSphere, Lotus, Information Management, and Rational
- System x, System p Servers, SAN Directors,
- Blade Center, Linux, Virtualization Mgmt, Microelectronics —ASICs

## Senior Leadership Support

- CEO Meetings
- Senior Executive Sponsorships WW
- Sharing of visions and strategies

## Channels and Marketing

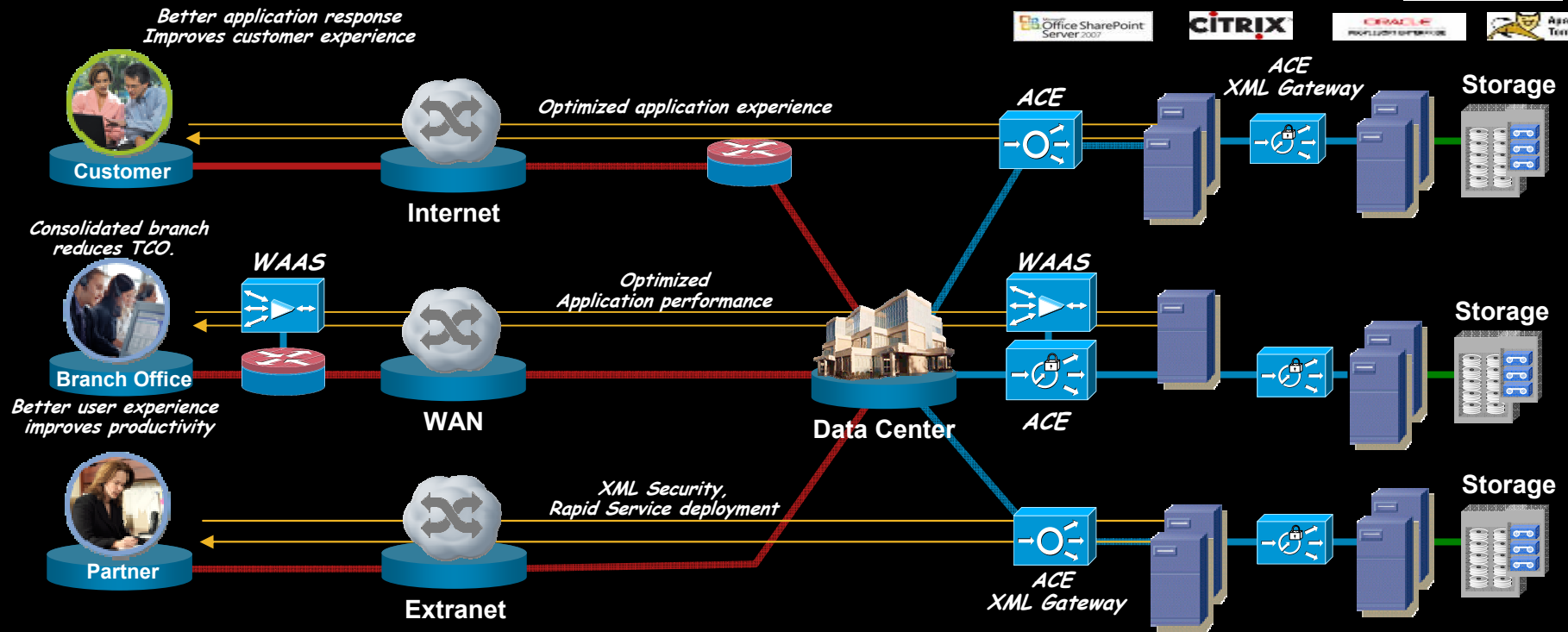
- Cisco Channel Incentive Programs
- Cisco Certification Programs
- Regional Account Planning
- WW Marketing Planning and Campaigns

Together IBM And Cisco Provide an **Unmatched, Holistic** Approach to the Market and Our Mutual Customers

# Consolidation and Application Optimization

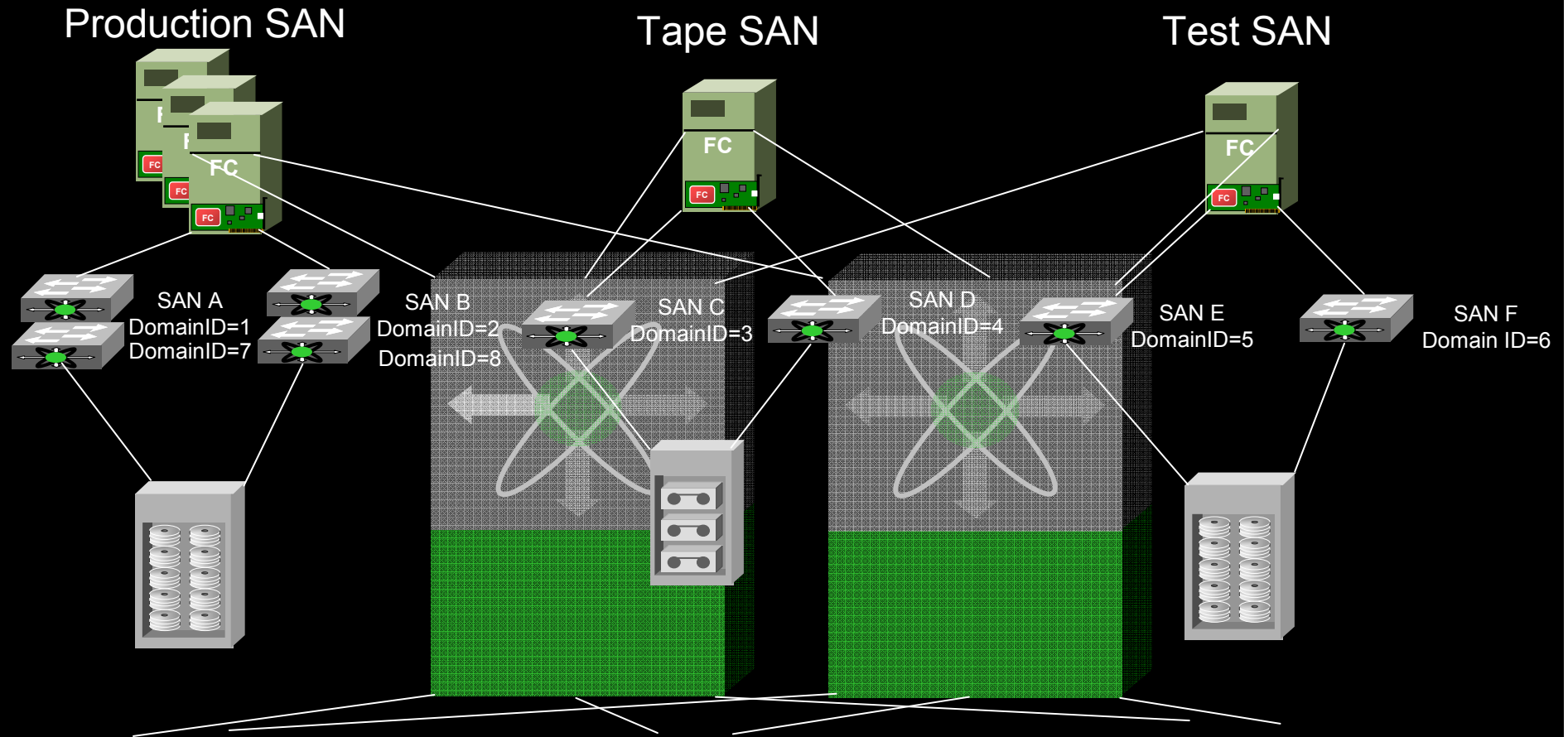
## Addressing application delivery

- Maximize Application Performance, Availability & Security
- Reduce IT Costs
- Ensure Data Privacy & Compliance



# Virtualization and Consolidation

## Understanding Virtual Fabrics (VSANs)

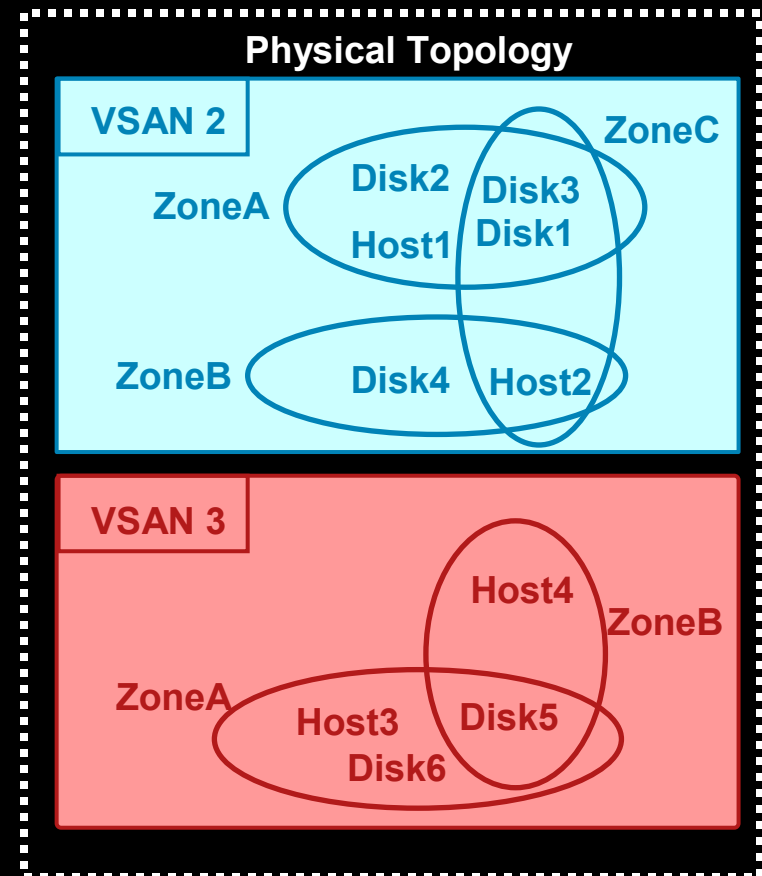




# VSANs, Zones, IVR Zones

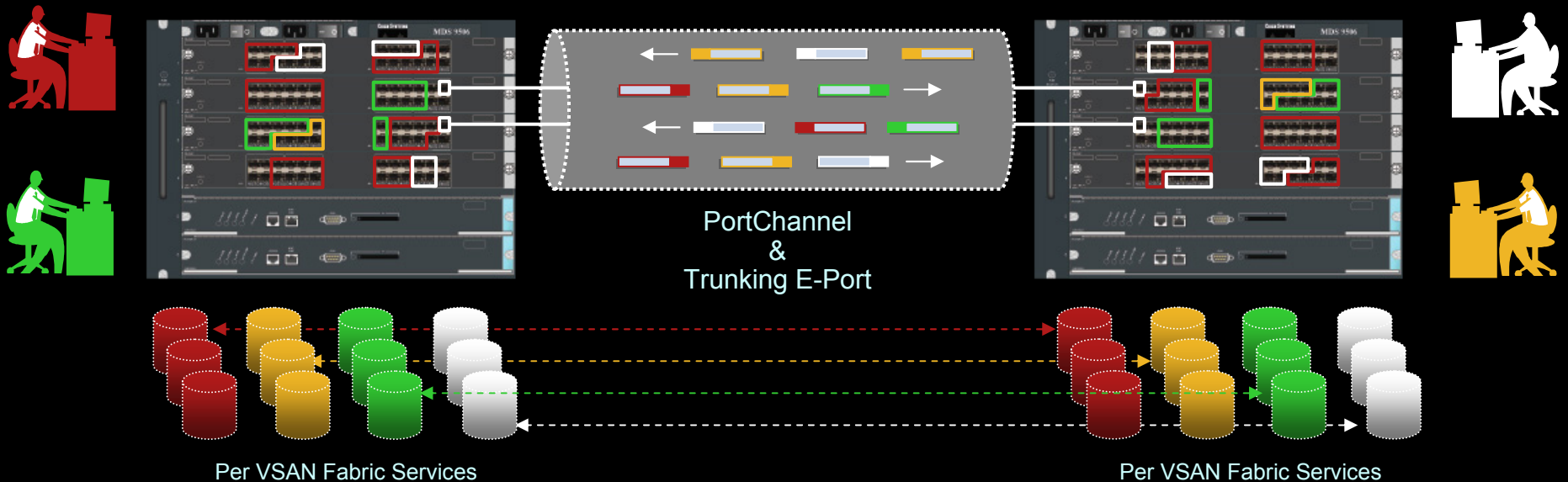
- Hierarchical relationship:
  - First assign physical ports to VSANs
  - Then configure independent zones per VSAN
- VSANs provide traffic statistics
  - Zones provide added security and allow sharing of device ports
- VSANs only change when ports needed per virtual fabric
  - Zones can change frequently (e.g., backup)
- Ports are added/removed non-disruptively to VSANs
- IVR zone: a container or access control, containing two or more devices in different VSANs
  - Standard zones are still used to provide intraVSAN access
- IVR zoneset: a collection of IVR zones that must be activated to be operational

## VSANs and Zoning Are Complimentary



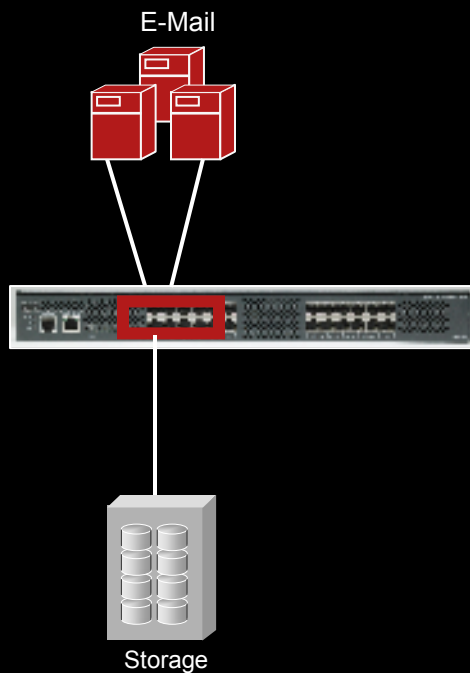
# Cisco VSAN Technology at Work

- VSANs create new instances of fabric services - separate policies and control traffic for each VSAN ensure fault isolation
  - VSANs do not exchange any control plane information (e.g. RSCNs, RCF, BF)
  - Each VSAN topology is independent and separate from the next
- Ports are individually assigned to VSAN (manual or automatically with DVPM)
- All frames (data and control) are tagged with VSAN Identifier when passing between Cisco switches providing hardware enforced separation of virtual fabrics
- Role Based Access Control (RBAC) allows for administrators per VSAN

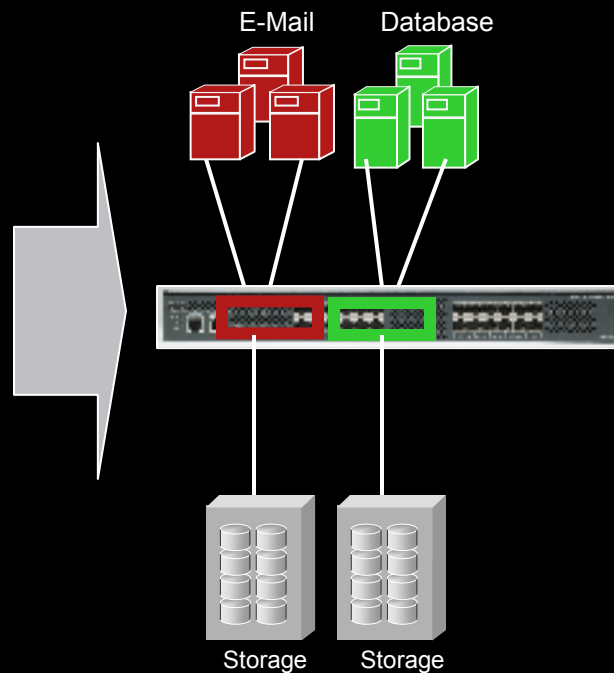


# Exceptional Flexibility – On-Demand Ports and Virtual SAN (VSANs)

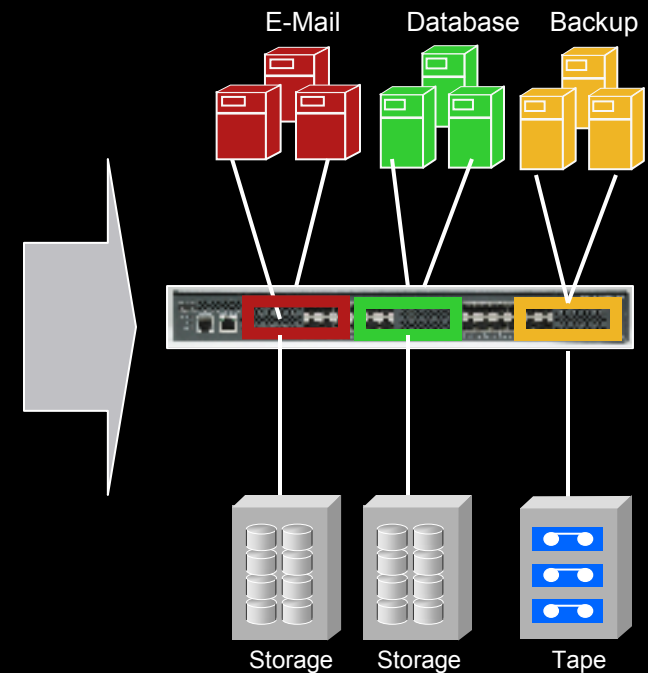
Start with 8-ports and a  
VSAN for E-Mail



Add 8 more ports and a  
VSAN for Database



Add 8 more ports and a  
VSAN for Backup



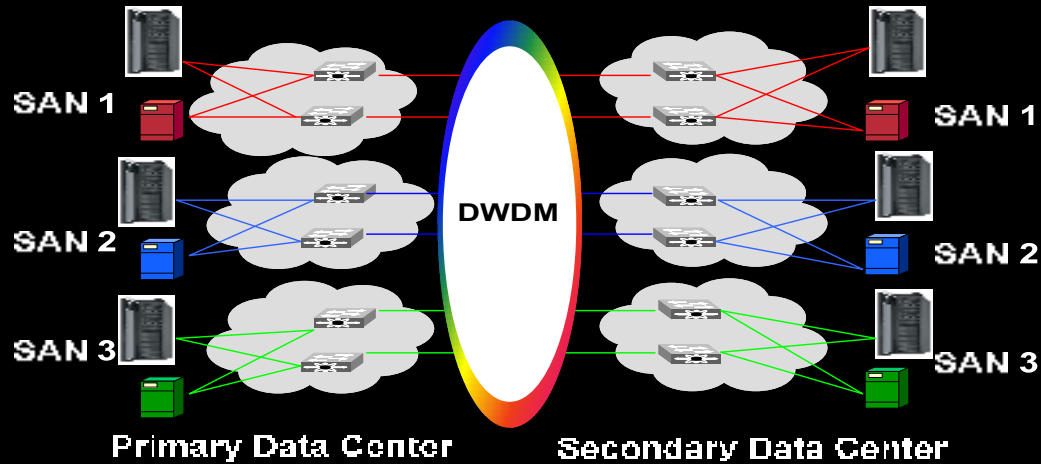
# Virtualizing the Fabric – The Full Solution



- Provide connectivity across virtual SANs without merging the fabrics
- Map and manage virtual fabrics independently
- Set FC parameters per virtual fabrics (e.g. timer values, FID allocation, DID ranges etc.)
- Define separate security policies per virtual fabric
- Troubleshoot per virtual fabric problems
- Separate fabric services per virtual fabric (e.g. routing, zones, RSCNs, QoS, etc.)
- Extend virtual fabric service to FC ISLs, iSCSI, FCIP, FICON, etc.
- Assign virtual fabric membership at the port level

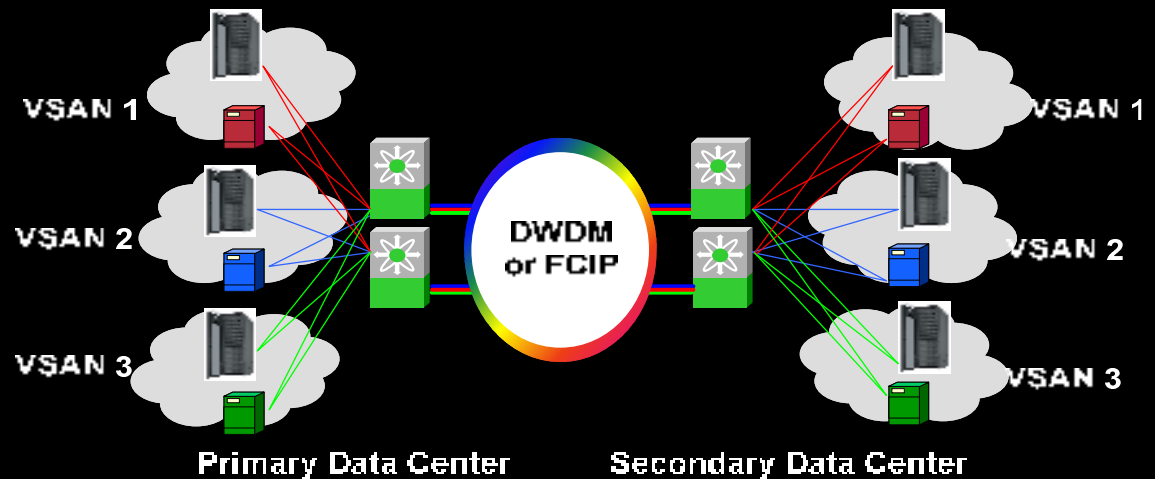
**Full Service End-to-End Virtual Fabric Implementation**

# Virtual Fabrics in Distributed Data Center



Distributed Data Center  
Architecture  
w/o Virtual Fabrics

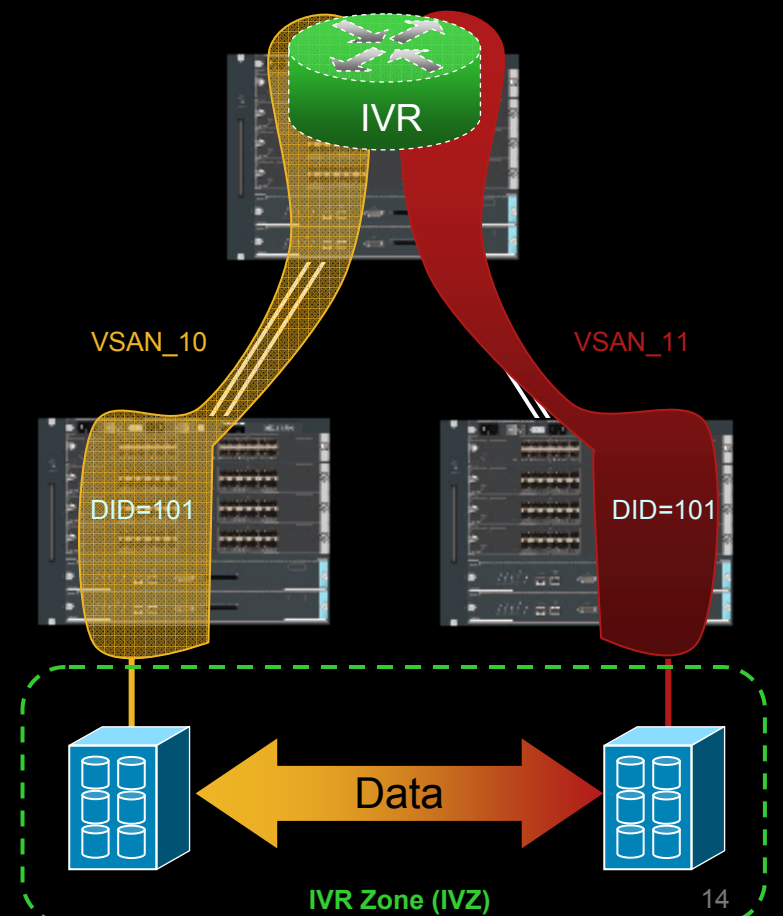
Distributed Data Center  
Architecture  
with Virtual Fabrics



# Cisco Integrated InterVSAN Routing (IVR)

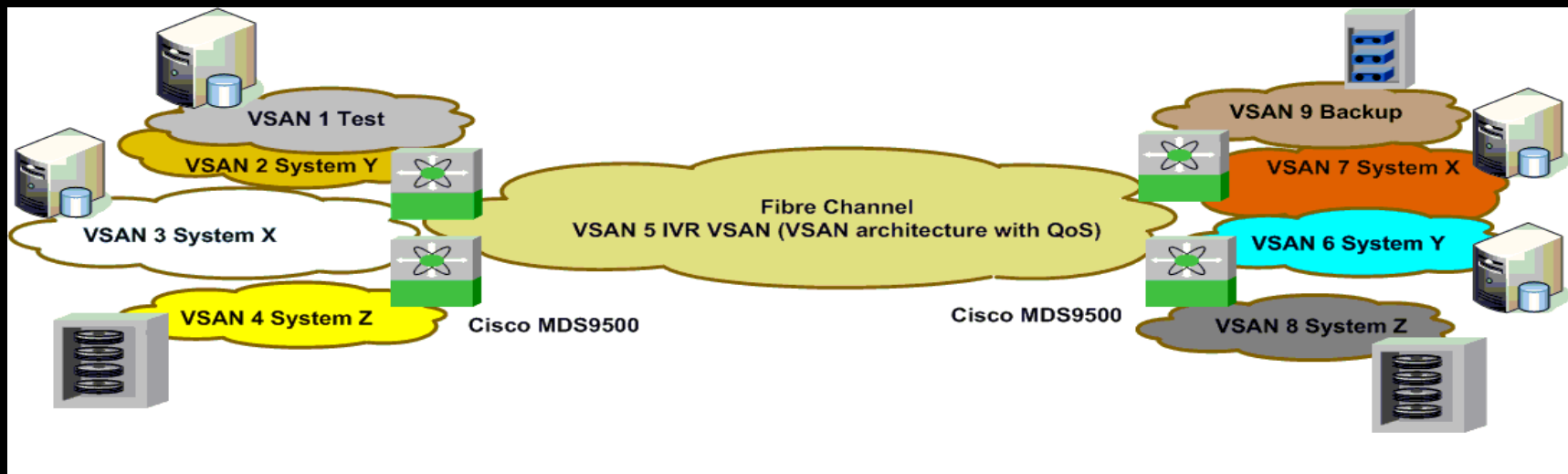
- Allows resources in different VSANs to communicate
  - But without the need to merge fabrics
- Full bidirectional Network Address Translation (NAT)
  - Connect fabrics with overlapping Domain IDs
- Fully Standards based
  - Transparent to third-party switches
- Simple to set-up and manage
  - Uses well understood zoning principles for define allowed exchanges
- Provides high fabric resiliency and VSAN-based manageability
  - Distributed, scaleable, and highly resilient
- Supported at wire rate on any port on the MDS family!
  - No need for special routing modules or appliances

Control Traffic  
not passed  
between VSANs



*Wirespeed FC frame rewriting capability on every MDS 9200 & 9500 port is the foundation for delivering scaleable SAN Routing*

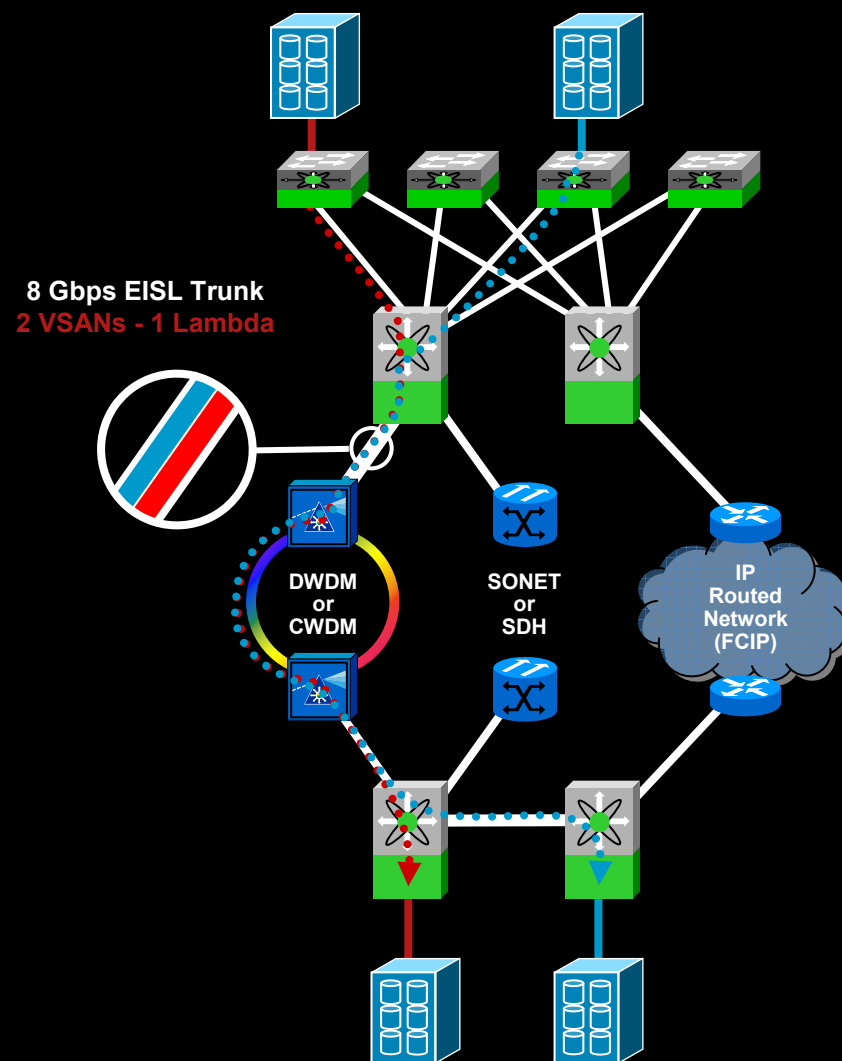
# Storage Area Network – „hierarchical” architecture with Virtual SAN



- Hierarchical design (Virtual Fabric architecture)
- Segmentation and High Availability (InterVSAN routing)
- Scalability
- QoS functionality
- Traffic Engineering
- Support for Fibre Channel over IP and iSCSI
- PortChannel (Load balancing for different length links)

# VSANs Allow Sharing of DR Facilities

- VSANs can be carried between data centers over various links
- Cost savings through consolidation of DR facilities
- SAN Isolation maintained
- Various wide and metro area facilities can be used securely:
  - FCIP (e.g. PoS, ATM, Metro Ethernet)
  - Optical (e.g. SONET, DWDM or CWDM)
- Cisco MDS 9000 can provide traffic statistics per VSAN (departmental chargeback?)
- Full fabric discovery per-VSAN through Cisco Fabric Manager





# Cisco MDS900 - Fabric Consolidation

## Data & Control Plane Scaling

### Cisco PortChannel Link Aggregation

- Adds Performance scalability and resilience
- Group up to 16 links for aggregate of up to 160 Gbps (10G FC interfaces!)

*Any port, any line card, no restrictions*

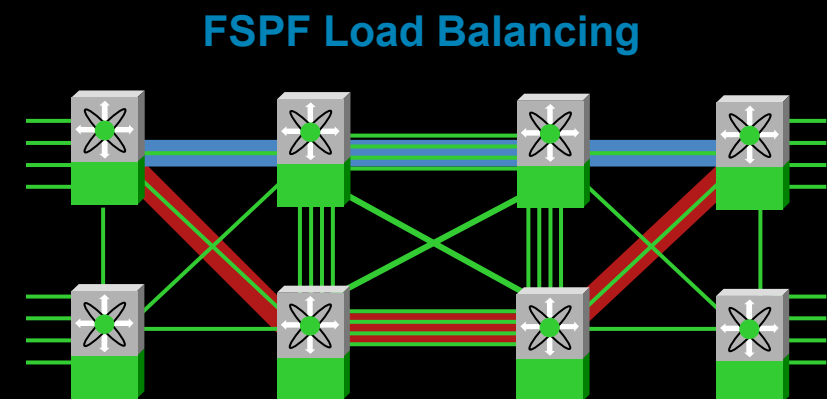
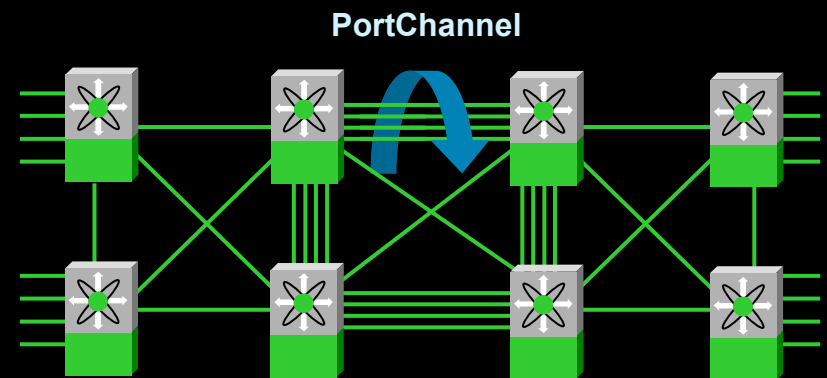
- Hardware-based intelligent load distribution, with rapid failover and re-distribution
- PortChannel Protocol (PCP) for simplified auto set-up and configuration validation

### Robust & Highly Scalable Control Plane\*

- FSPF Routing for up to 16 equal cost paths (1 PortChannel = 1 link)

*With traffic engineering based configurable link costs per Virtual SAN*

- Support for large scale fabrics of up to 12 hops/fabric
- 239 Switches per Virtual SAN
- 8000 Zones per Switch
- 20000 Zone Members per Physical Fabric
- All zoning in hardware!



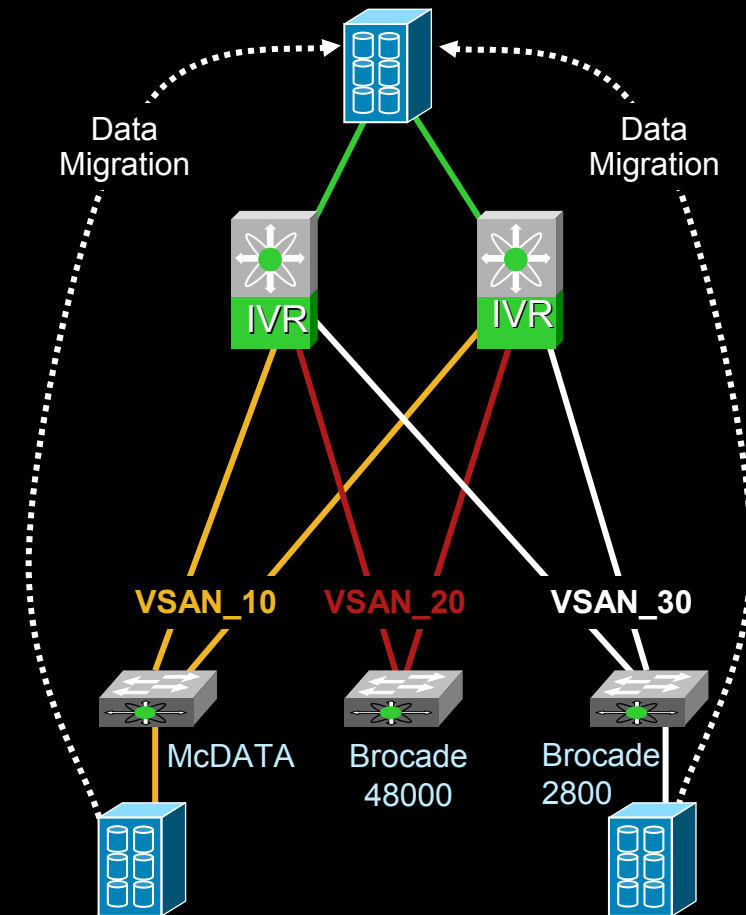
\* Cisco maximums – OSM qualified values maybe smaller

# VSANs, IVR & Legacy Interop Modes

## Enable fabric and data migration

### Cisco Legacy Interop modes

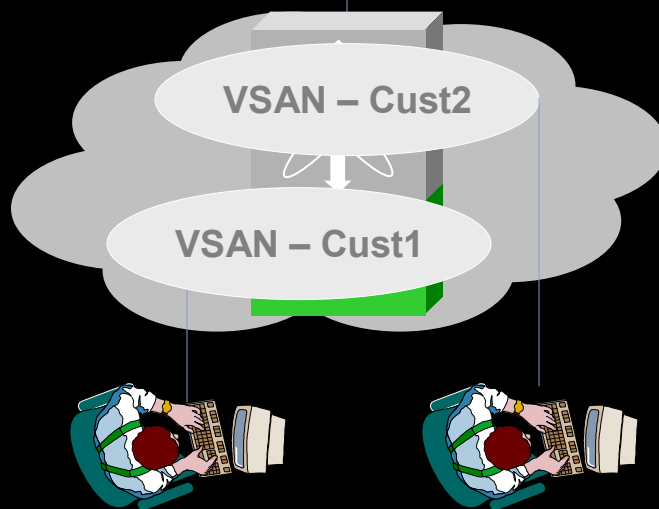
- Enables MDS 9000 family to interoperate with 3<sup>rd</sup> party switches in their 'Native Mode'
  - Re-use existing legacy fabric switches
  - No impairment to Cisco fabric
  - No change required on legacy switch
- Configurable on a VSAN-by-VSAN basis on MDS 9000
- Enhances standard interop mode
  - Mode 1 - Standard interop mode
  - Mode 2 - Supports Silkorm 2x00, 6400, and 3200/3800 (core\_PID=0)
  - Mode 3 - Supports Silkorm 3900, 12000, 48000 (core\_PID=1)
  - Mode 4 - Supports all McData platforms



# MDS Security Features - VSAN Based Roles

## Network Administrator

Configures and manages all platform-specific capabilities



- Enables deployment of VSANs that fit existing operational models

Network-admin configures all platform-specific capabilities

VSAN-admin(s) configure and manage their own VSANs

- The existing “role” definition is enhanced to include VSAN(s)

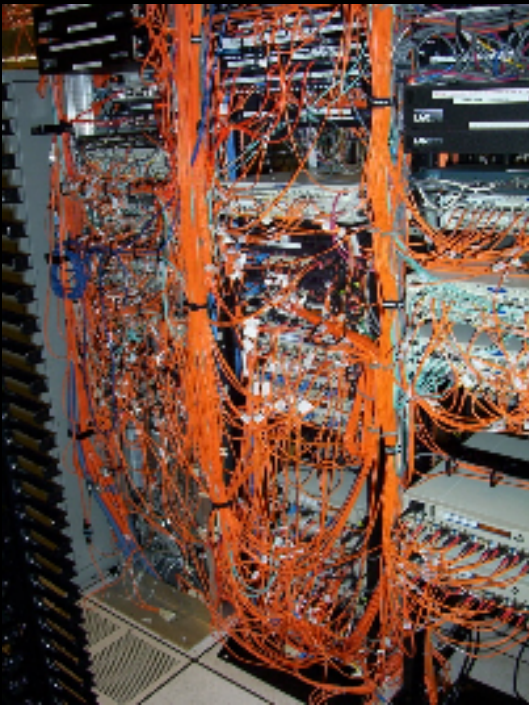
## VSAN Administrators

Configure and manages only their VSANs

# Case Study – Major Insurance Company SAN Consolidation

## Customer Reference

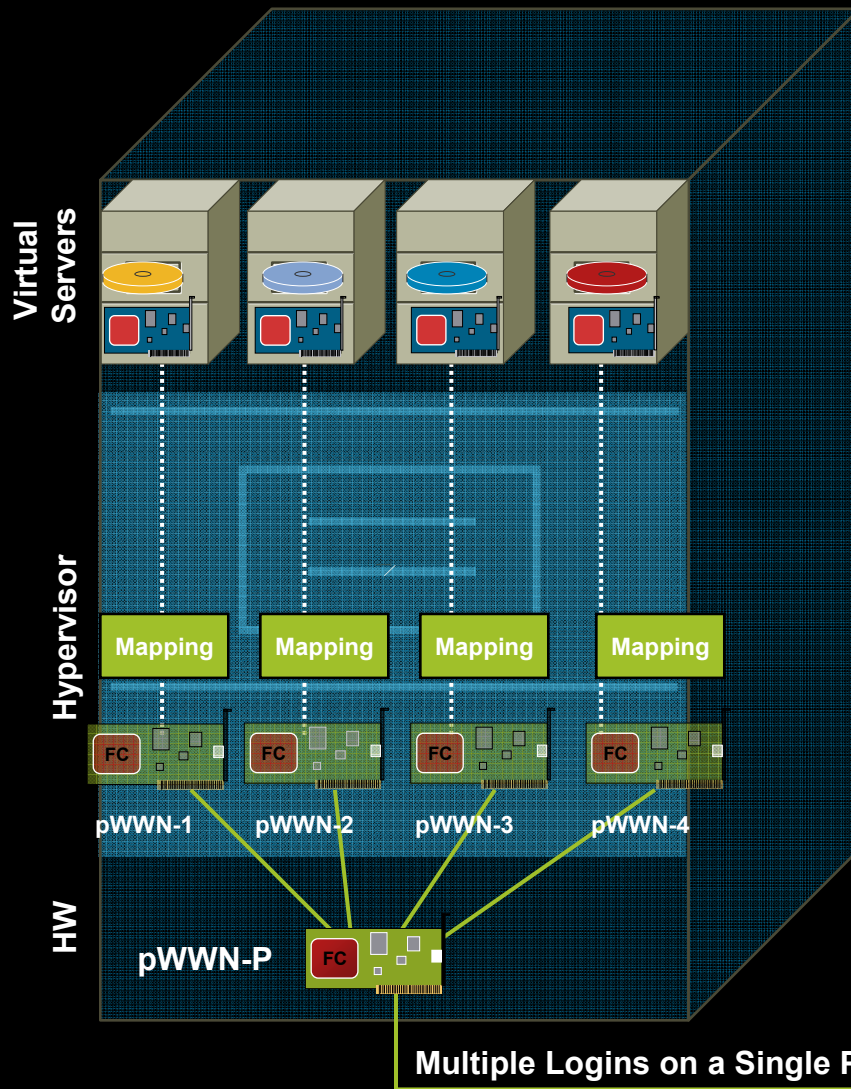
- One of the largest insurance and financial services companies in the world
- Migrated storage infrastructure which includes several hundred Terabytes from several SAN islands to a consolidated MDS 9000-based SAN designed for availability, recoverability, and growth



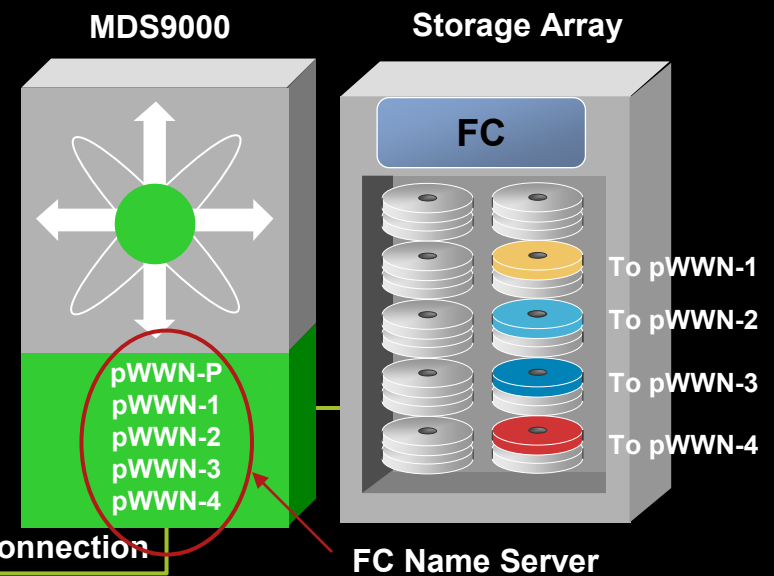
- Converted 24 (competitive) fabrics to 4 fabrics over two production data centers
- Consolidated 102 legacy switches to 20 MDS directors
- Completed project in 90 days



# Virtual Server Using NPIV and Storage Device Mapping

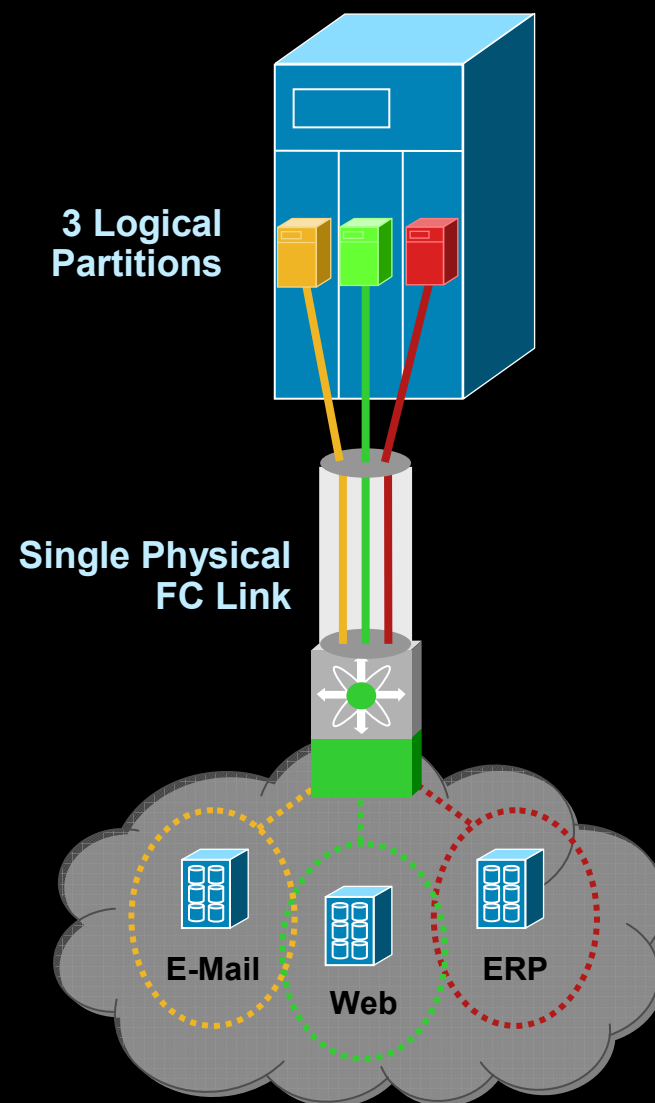


- Virtual HBAs can be zoned individually
- “LUN masking and mapping” is based on the virtual HBA pWWN of each VMs

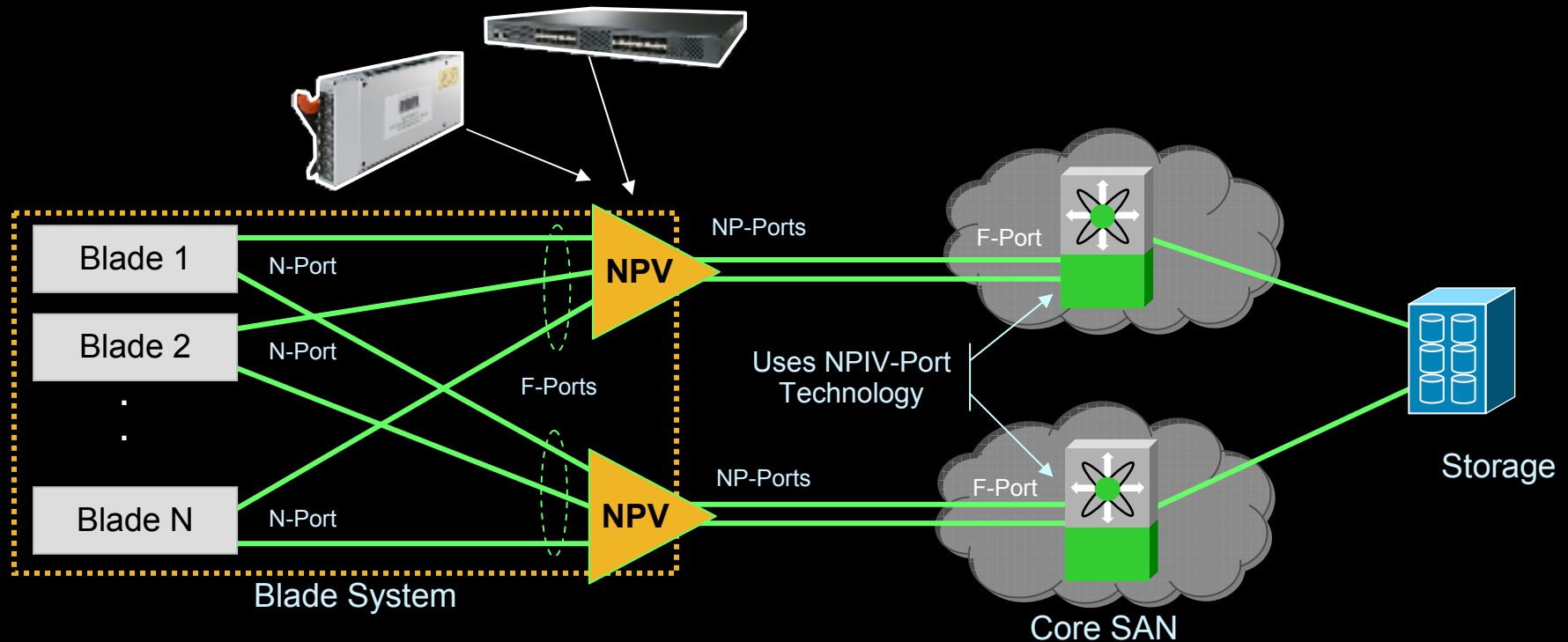


# N-Port ID Virtualization (NPIV)

- NPIV is a standards-based technology specified by INCITS T11
- Allows HBA port sharing between different virtual machines
- Each virtual device logs into the fabric independently
  - 1<sup>st</sup> device uses FLOGI (e.g. HBA)
  - Subsequent devices use FDISC
- Each device registers independently with name service via PLOGI
- Enables Independent fabric policies per Virtual Machine e.g.
  - Zoning
  - Security
  - Traffic mgmt (e.g.. QoS)



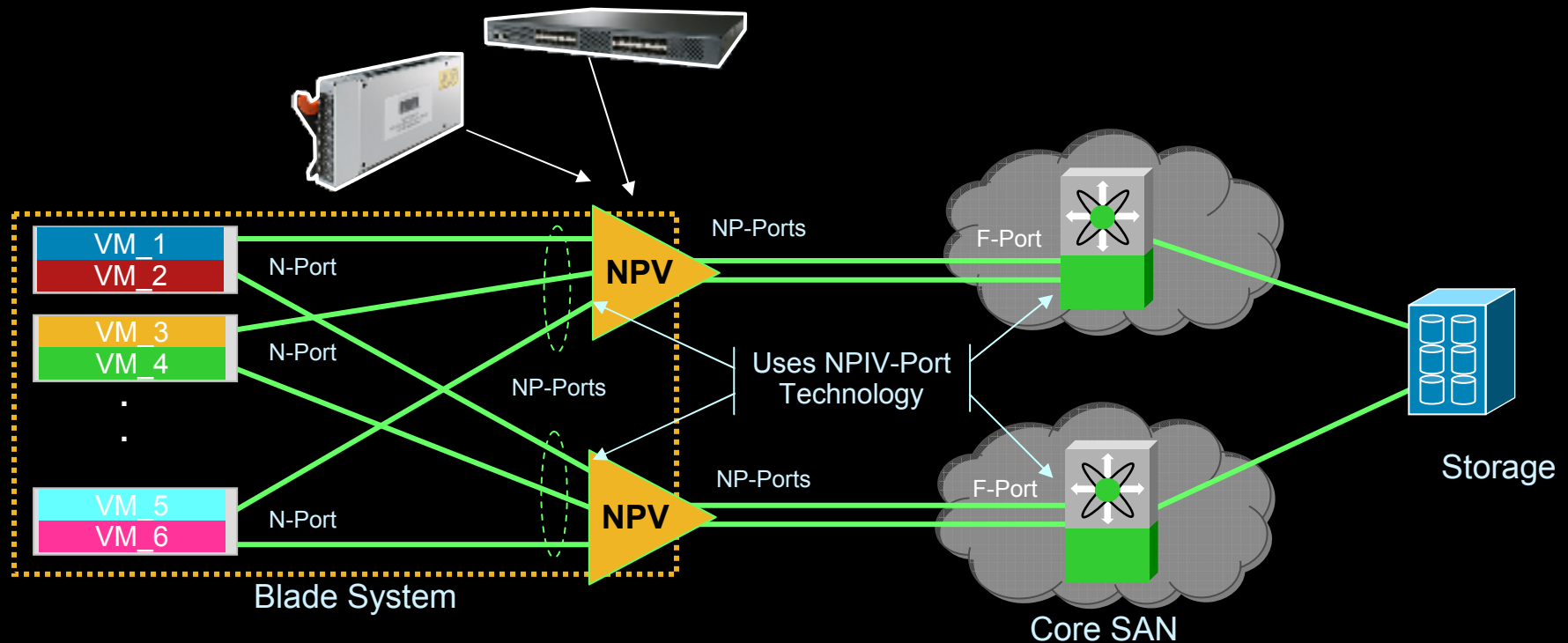
# Introducing N-Port Virtualizer (NPV)



## Key Benefits of NPV

- Solves the Domain ID issue. With NPV, Blade Switch appears as a HBA to the core
- Addresses the interoperability issues since the Blade Switch presents itself as an HBA
- Simplifies management since the server administrator is not exposed to SAN switch management tasks

# Introducing N-Port Virtualizer (NPV)

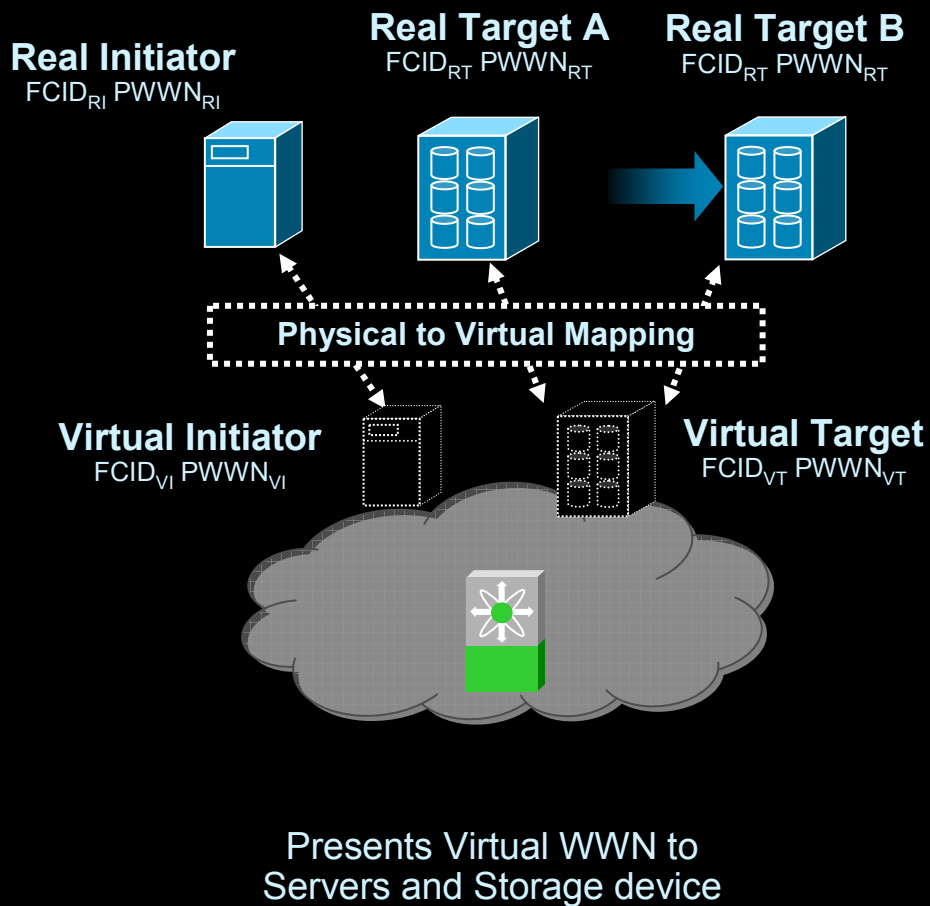


## Key Benefits of Nest NPIV & NPIV

- Total Flexibility – Administration, Mobility, Control
- Massive Scalability – Build SANs with 1000's of Virtual Machines with extremely simple fabric topologies
- Retain management domains and access control
- Further Enhancements on the way – e.g. WWN virtualization



# Cisco SAN Device Virtualization



- Allows provisioning with virtualized servers and storage devices
- Significantly reduces time to replace HBAs and storage devices
  - No reconfiguration of zoning, VSANs, etc. required on MDS
  - No need to reconfigure storage array LUN masking after replacing HBAs
  - Eliminates re-building driver files on AIX and HP-UX after replacing storage

# MDS 9500 Family of Ultra Scaleable Directors

Total Flexibility – any module, any chassis, any combination

## Chassis Options

MDS 9513



**IBM 2054-E11**

MDS 9509



**IBM 2054-E07**

MDS 9506

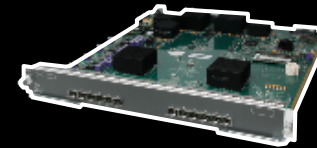


**IBM 2054-E04**

## Modules Options



4-port 10Gbps FC



12-port 4Gbps FC



24-port 4Gbps FC



48-port 4 Gbps FC



MSM 18/4 & 18/4 FIPS  
18 x 4Gbps FC + 4 x GE

# Cisco MDS 9100 & 9200 Switches

## Scaleable Edge Switching Solutions

**IBM 2053-424**



**MDS 9124**

- Support for 16 Virtual SANs (VSANs)
- Flexible port licensing
- Optional Switch or N\_Port Virtualizer (NPV) modes
- NPIV Support

**IBM 2053-434**



**MDS 9134**

- Support for 16 Virtual SANs (VSANs)
- Flexible port licensing
- Optional Switch or N\_Port Virtualizer (NPV) modes
- NPIV Support

Total 20 ports  
Port Licensing offered for  
7 servers + 3 uplinks  
14 servers + 6 uplinks  
SAN-OS firmware



**MDS FCSM for  
IBM BladeCenter**

- 18 4Gbps FC plus 4 x 1GE ports
- Concurrent FCIP & iSCSI Support
- Hardware based Compression & Encryption
- Expansion slot for any MDS module



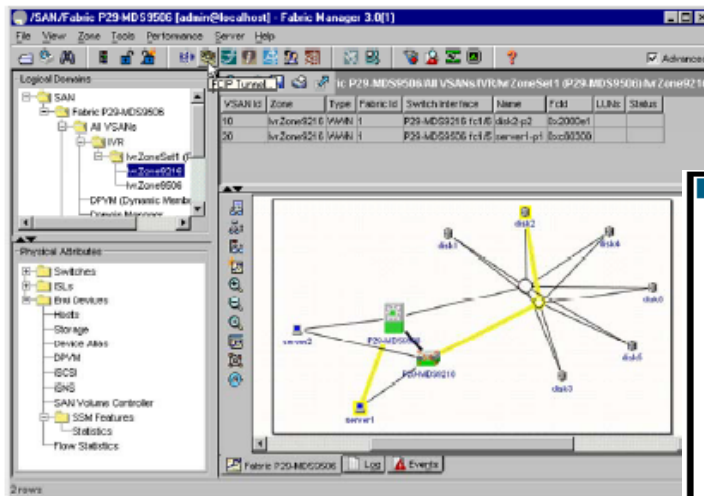
**MDS 9222i**

**IBM 2054-E01**

# Fabric Manager / Device Manager

## Navigation

- Browse devices using menu tree.
- Links and switches are highlighted on map.
- Double-click menu or map objects to see attributes.
- Nodes and Links can be:
  - Down: **red X**
  - Unmanageable: **red \**
  - Alarm: **orange dashed X**



© 2007 Cisco Systems, Inc. All rights reserved.

IC956 v3.0-1

## Device View

Menus and Toolbar

Sort Interfaces by VSAN

Device with Interface Status

Status Color Code



© 2007 Cisco Systems, Inc. All rights reserved.

IC956 v3.0-1-15

# Integration: Unified Fabric Markets Transition To Meet New Needs

## Speed

10Mb

100Mb

1Gb

10Gb

40 & 100Gb

## Services

Switched

QoS  
L3 Switching

L4-7 Svcs

Lossless

Unified  
Fabric

Shared

VLANs

PoE

L2 Multi-Pathing

## Platforms

Catalyst  
5000



Catalyst  
6500



Nexus



1994

1999

2008+

## Integration:

# What is Data Center Ethernet (DCE)?

Data Center Ethernet is an **architecture** based on a collection of **open standard Ethernet extensions** to improve and expand Ethernet networking and management capabilities in the data center .

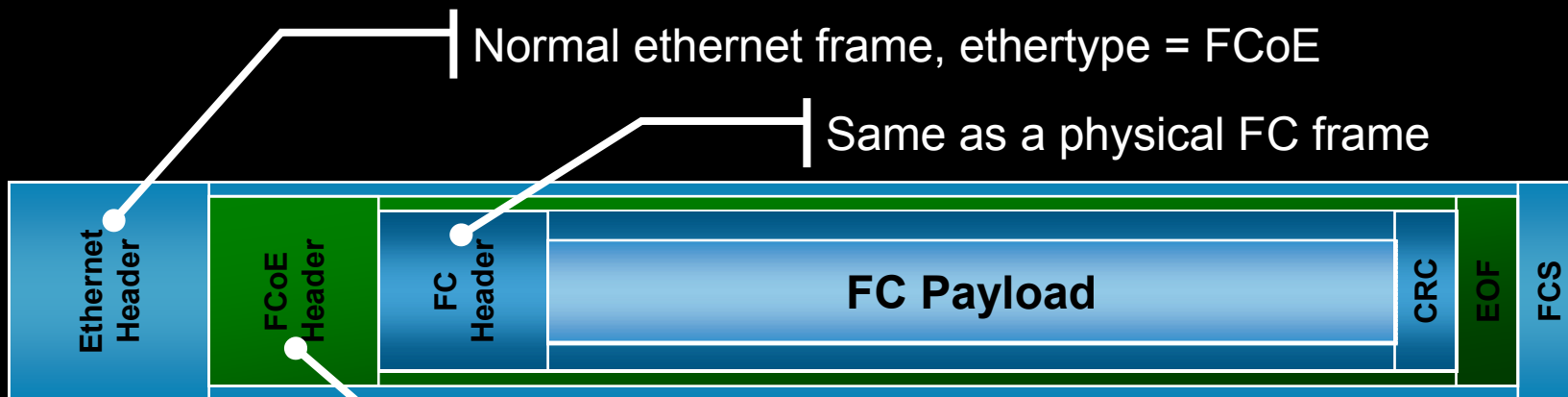
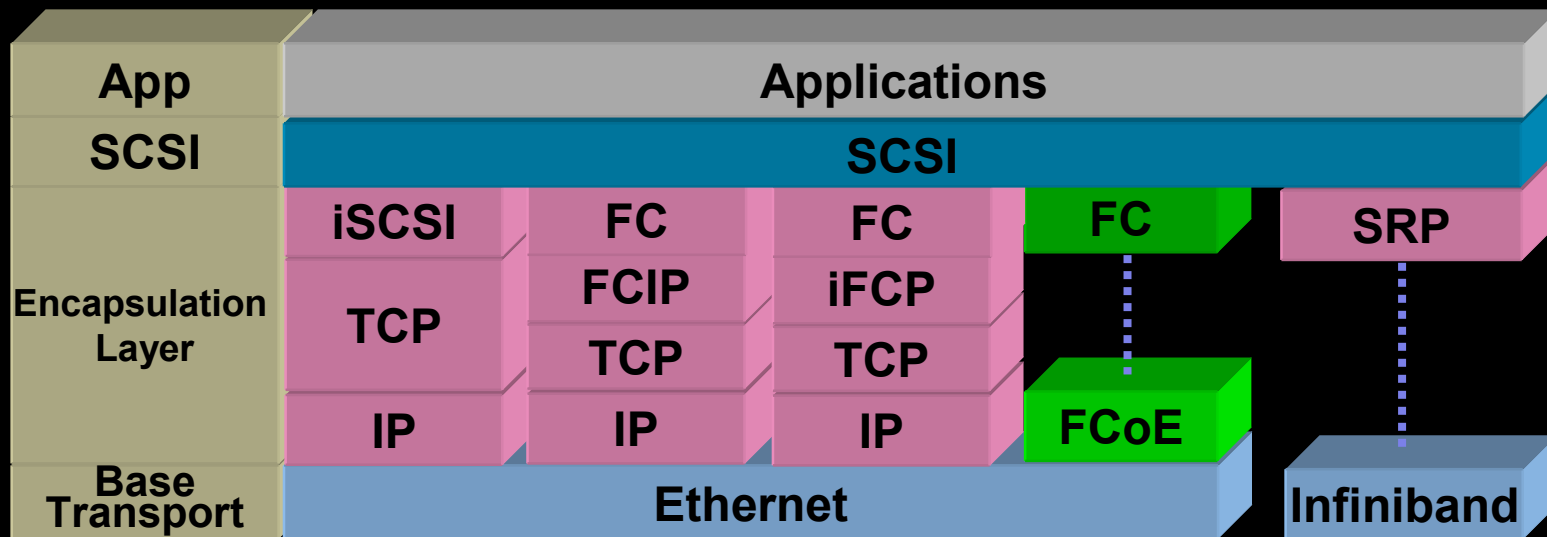
Cisco is showing **innovation** while working through the standardization process with these extensions in **open standards forums**.

# Integration: Data Center Ethernet Features

## Overview

Feature	Benefit
Priority-based Flow Control (PFC)	Provides class of service flow control. Ability to support storage traffic
CoS Based BW Management	Grouping classes of traffic into "Service Lanes" IEEE 802.1Qaz, CoS based Enhanced Transmission
Congestion Notification (BCN/QCN)	End to End Congestion Management for L2 network
Data Center Bridging Exchange	Auto-negotiation for Enhanced Ethernet capabilities DCBX (Switch to NIC)
L2 Multi-path for Unicast & Multicast	Eliminate Spanning Tree for L2 topologies Utilize full Bi-Sectional bandwidth with ECMP
Lossless Service	Provides ability to transport various traffic types (e.g. Storage, RDMA)

# Integration: Encapsulation Technologies





# Integration

## FCoE Specification progress

- Cisco submitted FCoE proposal on May 22 as a joint proposal among 16 companies

Adopted by ANSI T11 FC-BB5 in June 2007; full ratification by mid-2008

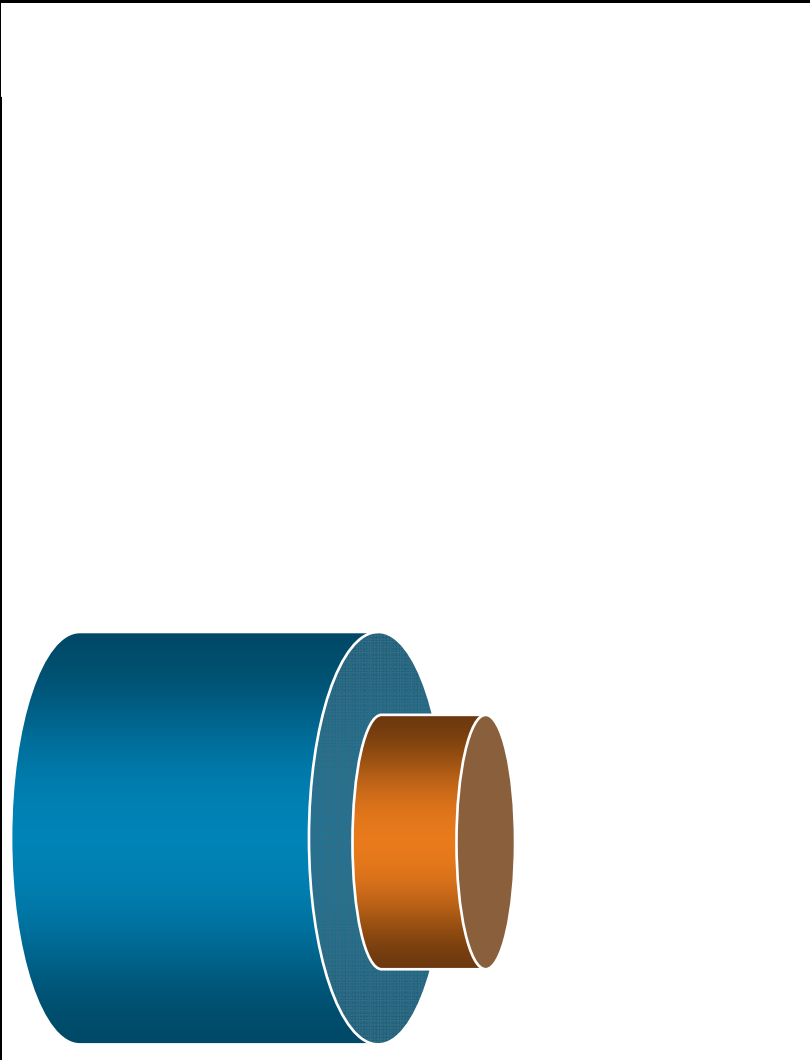
Frame format agreed upon by T11 in August

Support from entire storage and switching industry: EMC, HDS, HP, IBM, Sun, Brocade, NetApp, Cisco, Emulex, Qlogic, Nuova, Intel

- Follow INCITS ANSI-T11 progress ([www.t11.org/fcoe](http://www.t11.org/fcoe))



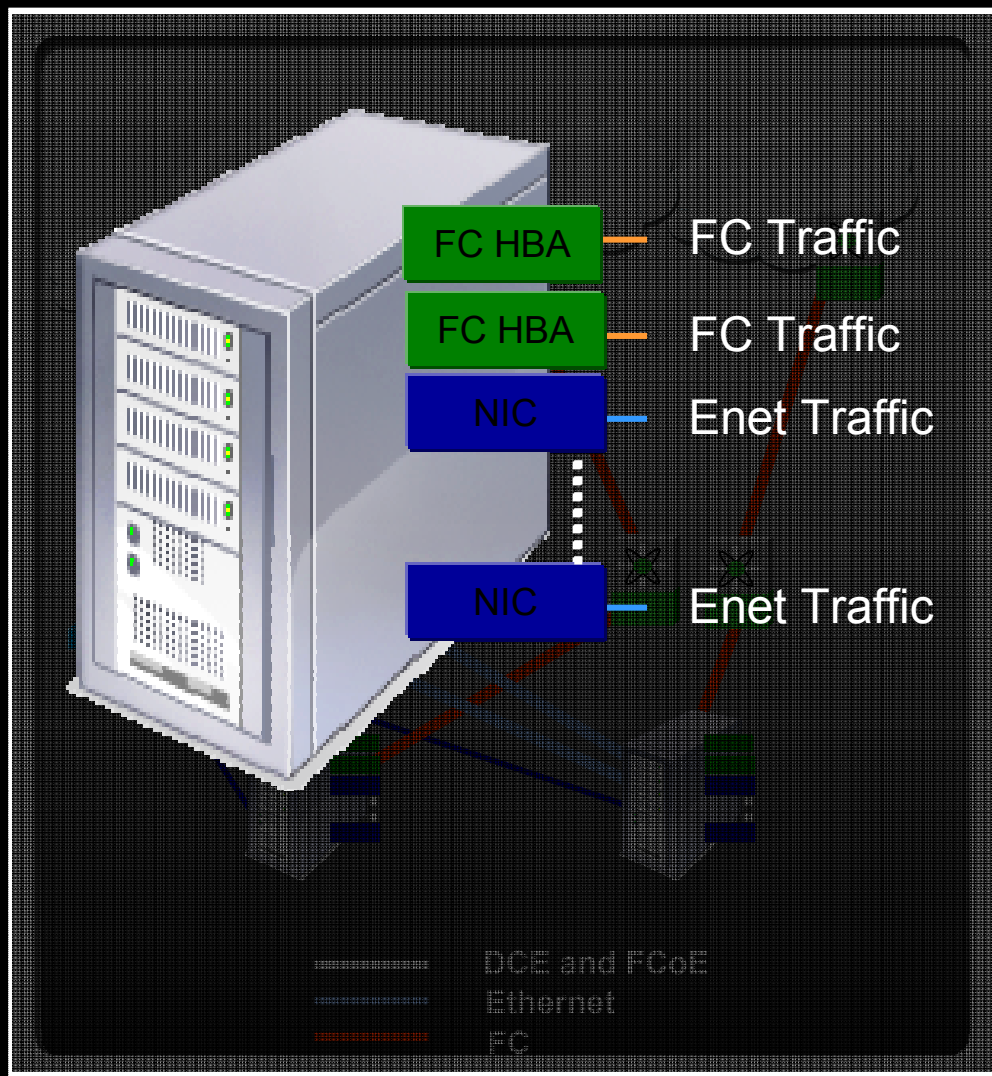
# First Steps in Building a Unified Fabric Fibre Channel over Ethernet (FCoE)



## Benefits

- Fewer Cables
  - Both block I/O & Ethernet traffic co-exist on same cable
- Fewer adapters needed
- Overall less power
- Interoperates with existing SAN's
  - FCoE SAN Management is completely consistent with FC SAN management
- No Gateway required
  - Simple encapsulation and de-encapsulation at wire speed

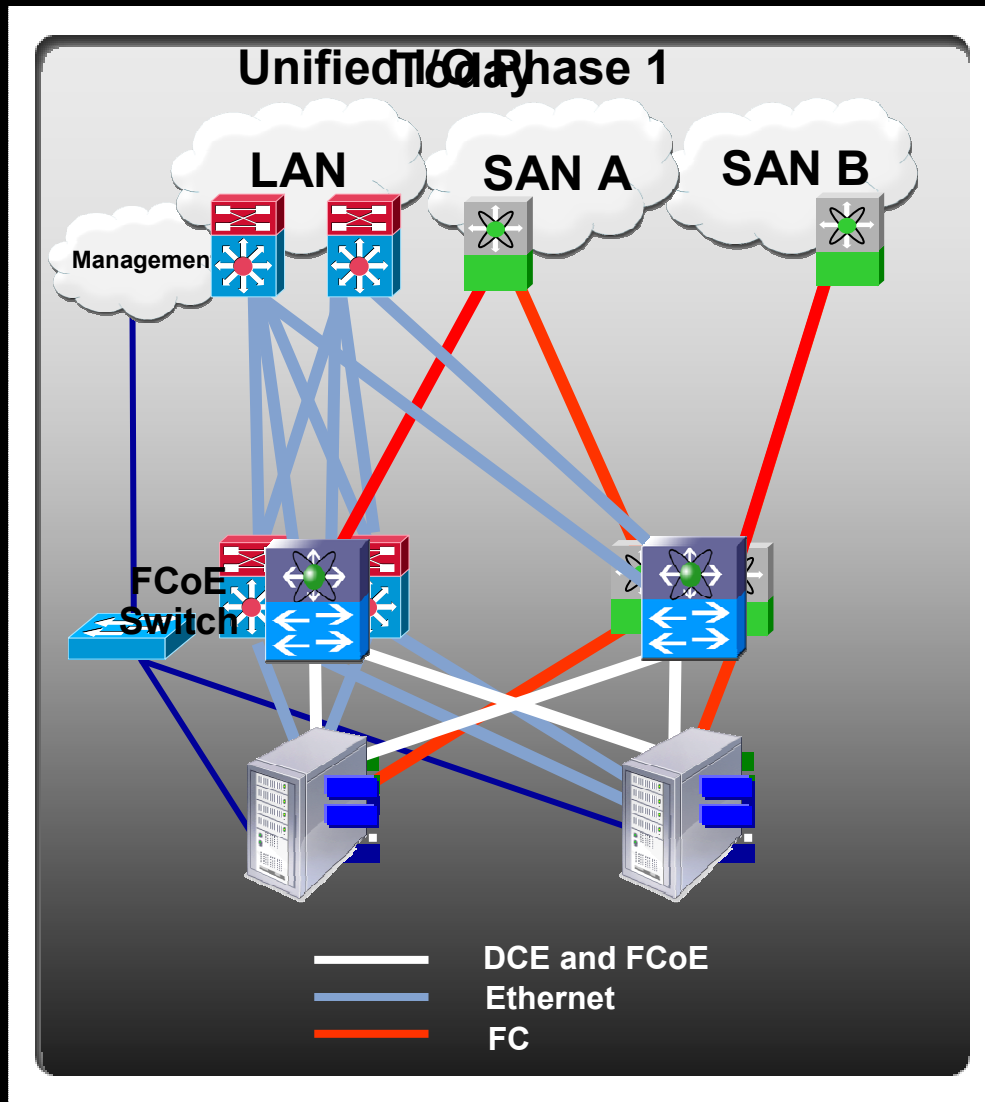
# Integration: I/O Consolidation Use Case



## Today:

- Parallel LAN/SAN Infrastructure
- Inefficient use of Network Infrastructure
- 5+ connections per server – higher adapter and cabling costs
  - Adds downstream port costs; cap-ex and op-ex
  - Each connection adds additional points of failure in the fabric
- Longer lead time for server provisioning
- Multiple fault domains – complex diagnostics
- Management complexity – firmware, driver-patching, versioning

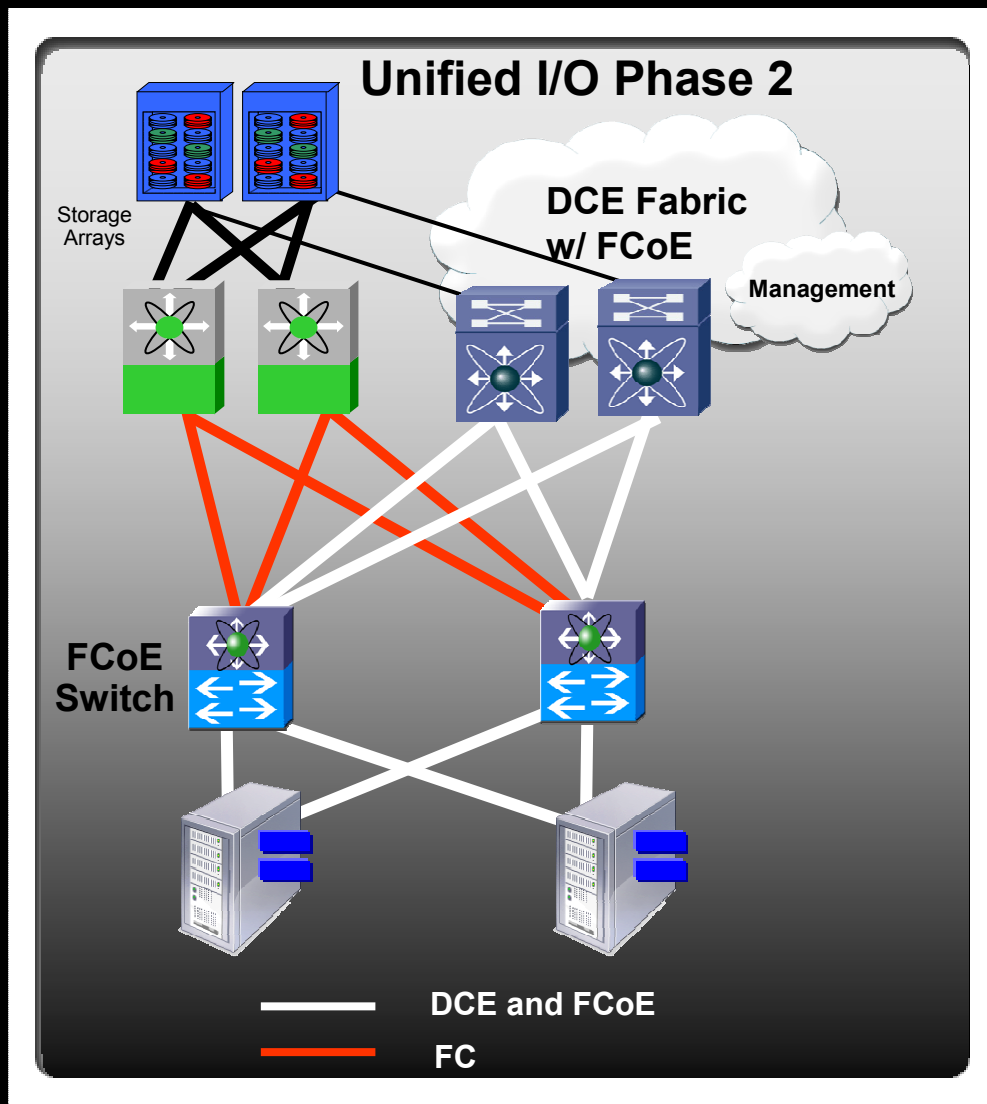
# Integration: I/O Consolidation Use Case Cisco Nexus Series Switch



## Today Unified I/O Phase 1

- Parallel LAN/SAN Infrastructure
- Reduction of server adapters
- Inefficient use of Network Infrastructure
- Simplification of access layer & cabling
- Gateway for implementation might be installed base of existing LAN and SAN adapter and cabling costs
- L2 Multihoming Access – Distribution Adds downstream port costs, capex and op-ex
- Fewer cables connection adds additional points of failure in the fabric
- Investment Protection (LANs and SANs)
- Consistent Operational Model
- Consistent time for server provisioning
- Multiple fault domains – complex diagnostics
- Management complexity – firmware, driver-patching, versioning

# Integration: Unified Fabric Use Case Cisco Nexus Series Switch



## Unified I/O Phase 2

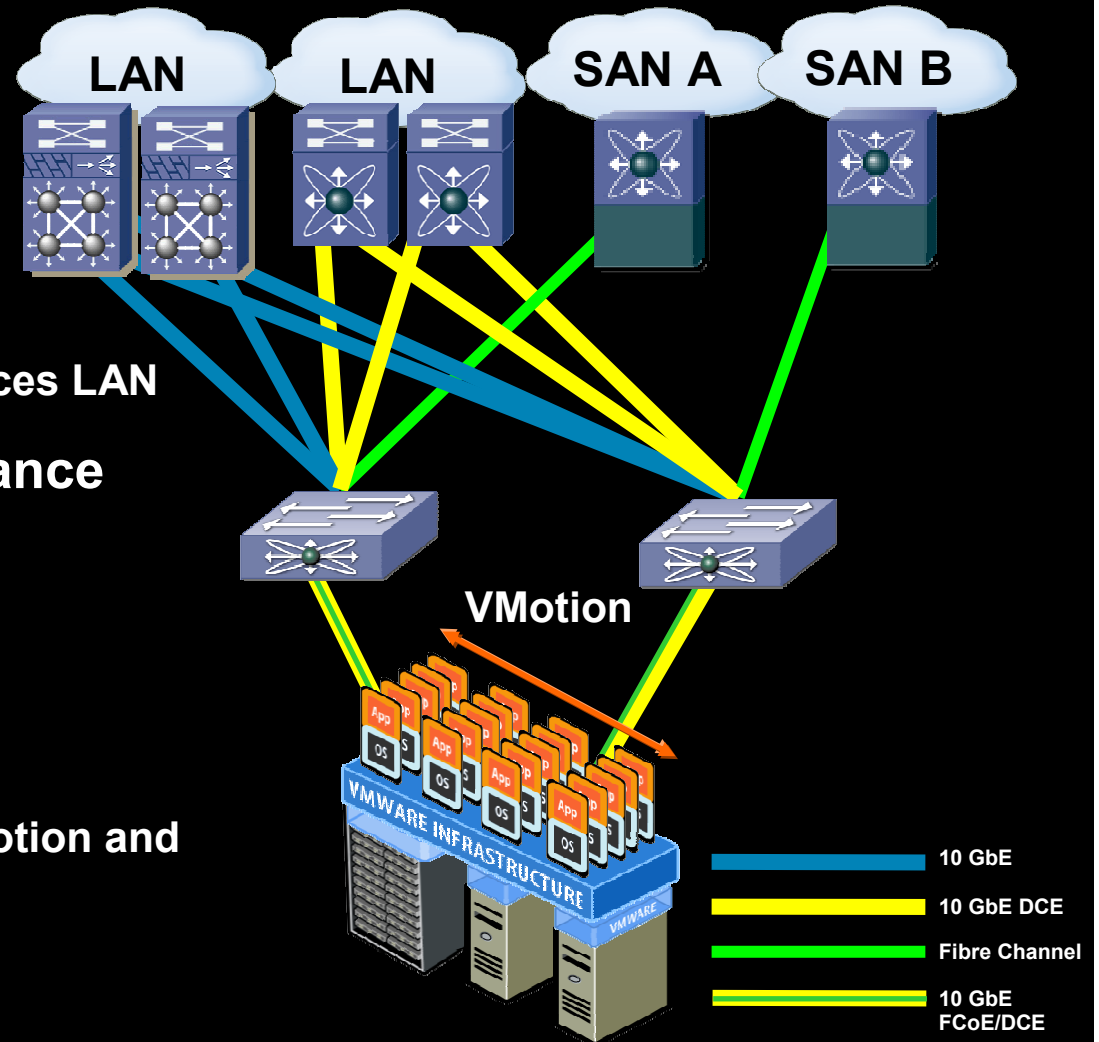
- Elimination of parallel network infrastructure
- L2/L3 Multipathing end to end
- Faster infrastructure provisioning
- Lower TCO
- Disk array access via DCE or Native FC

# Integration: VM-Optimized Services

- Enables convergence of multiple traffic types
  - Virtual Machines LAN
  - Virtual Machines SAN
  - Hypervisor Mgmt LAN
  - Virtual Infrastructure Services LAN

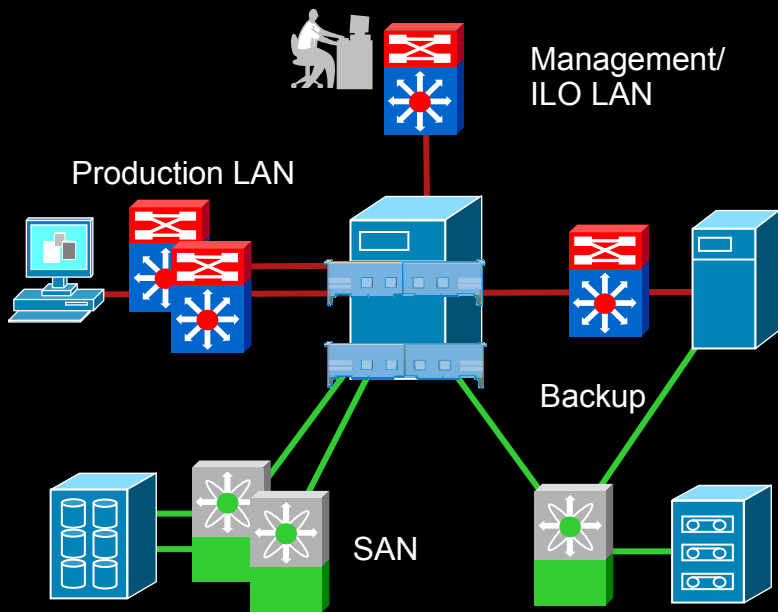
- Scales VM LAN performance
  - Increase I/O bandwidth
  - Increase VM density

- Accelerates Virtual Infrastructure Services
  - Live VM migrations via VMotion and DRS features
  - Enable additional services



# Unified I/O & Unified Fabrics

## Today



### Multiple...

- Networks & Fabrics
- Switches
- NICs/HBAs
- Cables/Connections
- Management Tools & Domains

Reduced OpEx  
Reduced CapEx

### Unified

- Networks & Fabrics - FCoE
- Data Center Switching
- Converged Network Adapter
- Cabling/Connections – fewer, higher speed
- Management Tools & Domains

# Introducing the Cisco Nexus 7000 Series

## Built for the Data Centre



Zero Service Disruption design  
Graceful systems operations  
Integrated lights-out management

High density 10GE Today  
Lossless fabric architecture  
Dense 40GbE/100GbE ready  
Unified Fabric Ready

Virtualized control and data plane  
15Tb+ switching capacity  
Efficient physical and power design

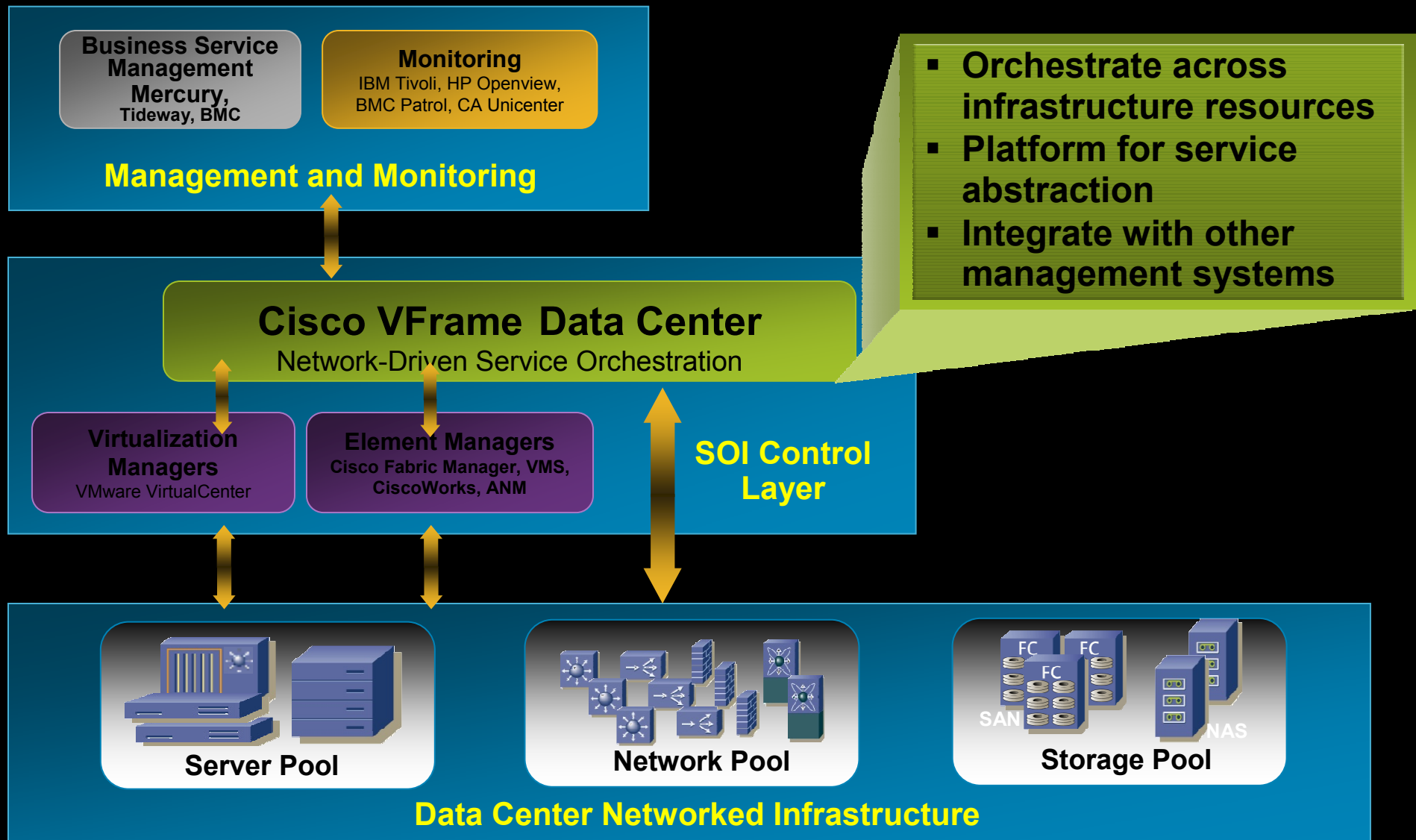
Operational  
Continuity

Transport  
Flexibility

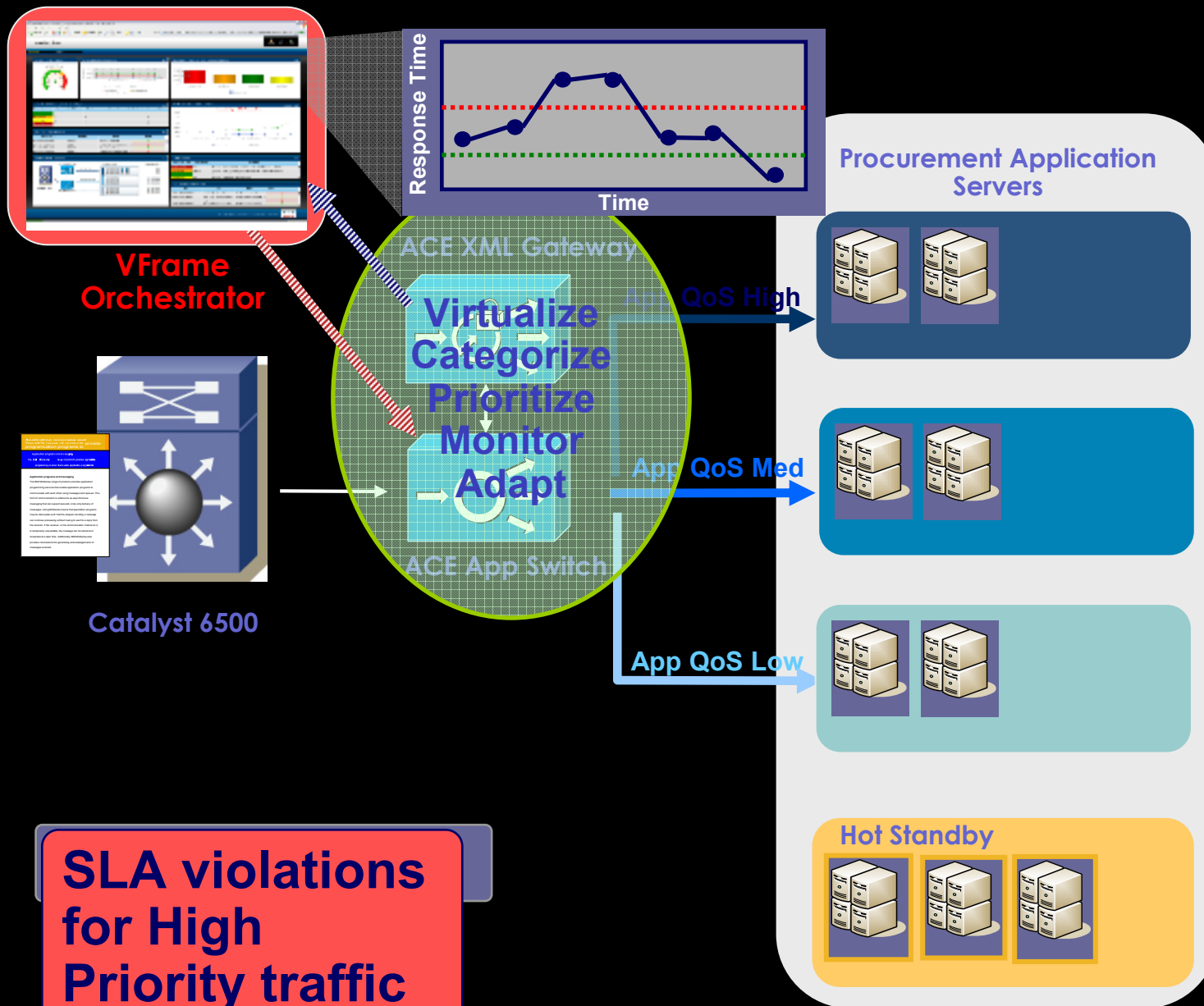
Infrastructure  
Scalability



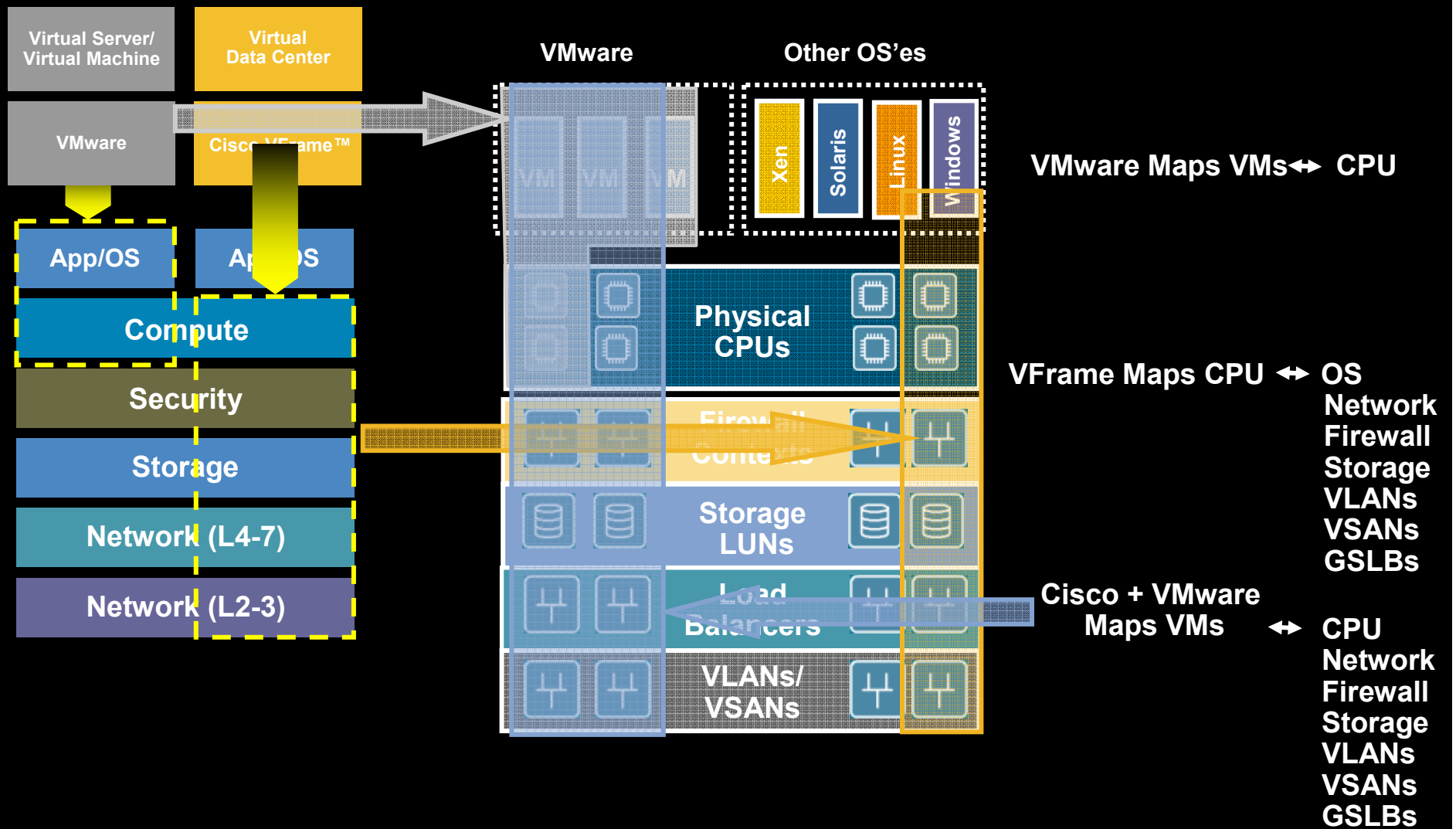
# Automation: Cisco VFrame Data Center Helps Build the Foundation for Service-Oriented Infrastructure (SOI)



# The Adaptive Data Center 3.0

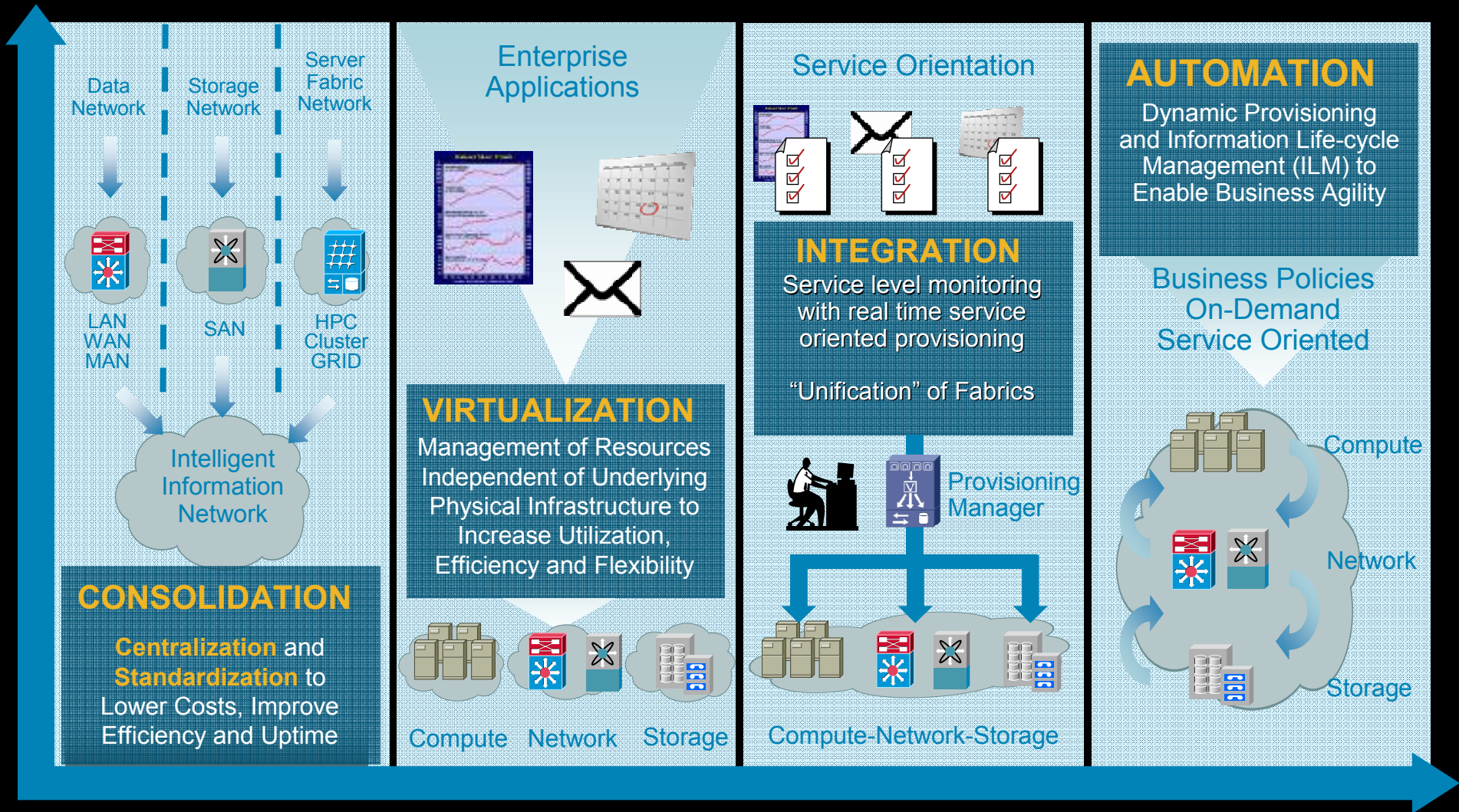


# Cisco VFrame™ and VMware Adaptive Orchestration



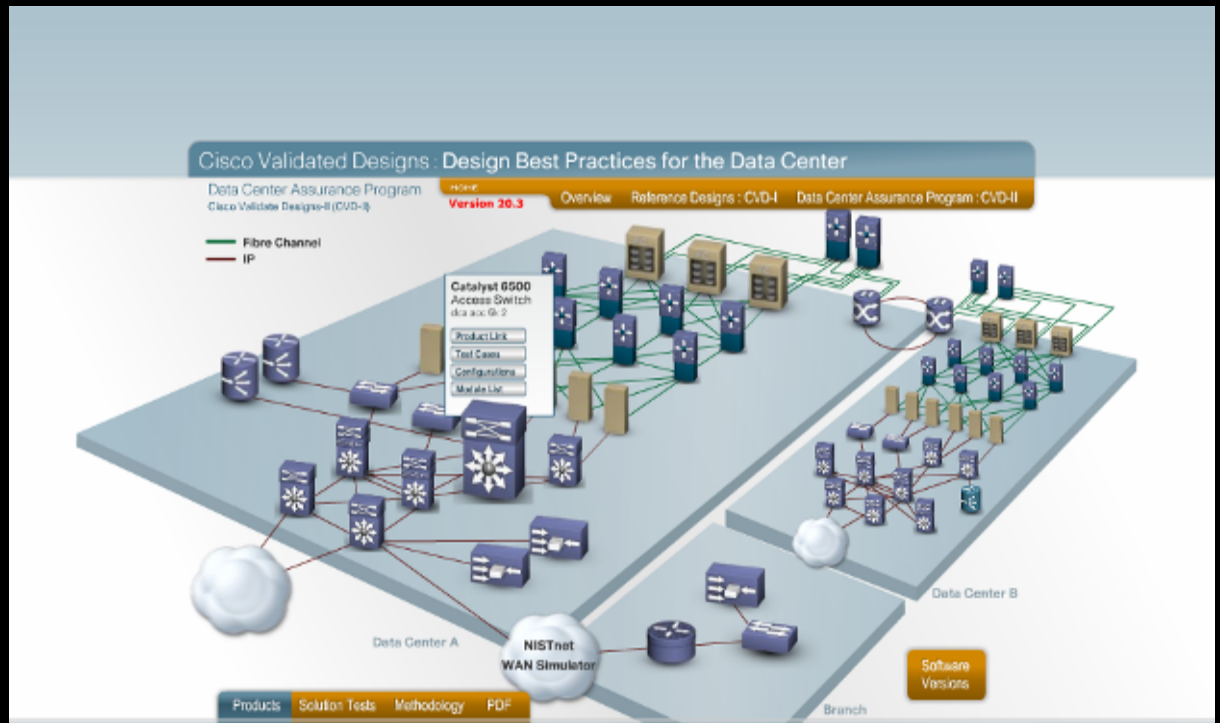
# Evolution of the Data Centre Infrastructure

## A Phased Approach...



# Data Center Assurance Program

- Design Best Practices
- Real-world Tested Configurations
- Downloadable Spec's and Results
- Full Test Plan and Documentation Kit
- Intuitive 3D graphical interface
- Testing updated Quarterly



<http://www.cisco.com/go/datacenter/dcap>

- Best Practice Design Zone
- Integrated Discussion Forum
- Operational Best Practices'

# Data Center Assurance... Collaboration / 2.0

## Cisco Validated Designs : Design Best Practices for the Data Center

Home

HOME

Version 20.3

Overview

Reference Designs : CVD-I

Data Center Assurance Program : CVD-II

### Welcome to the Cisco Data Center Networking best practices interactive tool.

This tool is provided to help users gain access to the design and test information in an intuitive, interactive way. To find the network design guidance you need for a specific data center project, go to the CVD-I tab and navigate the topology. To access the test descriptions, results and device configurations of the latest fully tested data center network architecture go to the CVD-II tab. Navigate the topology to find the tests and configurations associated with any specific solution or device. We hope you find this tool helpful for locating the information you need to complete a successful data center network deployment.

#### Overview

Cisco Data Center Networking design best practices, based on extensive research, testing and customer engagements are provided to help accelerate and lower the cost of designing and deploying Cisco data center networking technologies.

[Learn More](#)

#### Reference Designs

For customers at the planning and design stages of a data center project, Cisco reference designs describe the considerations associated with designing and deploying specific solutions and offer system level guidance, based on testing, and customer engagements.

[Learn More](#)

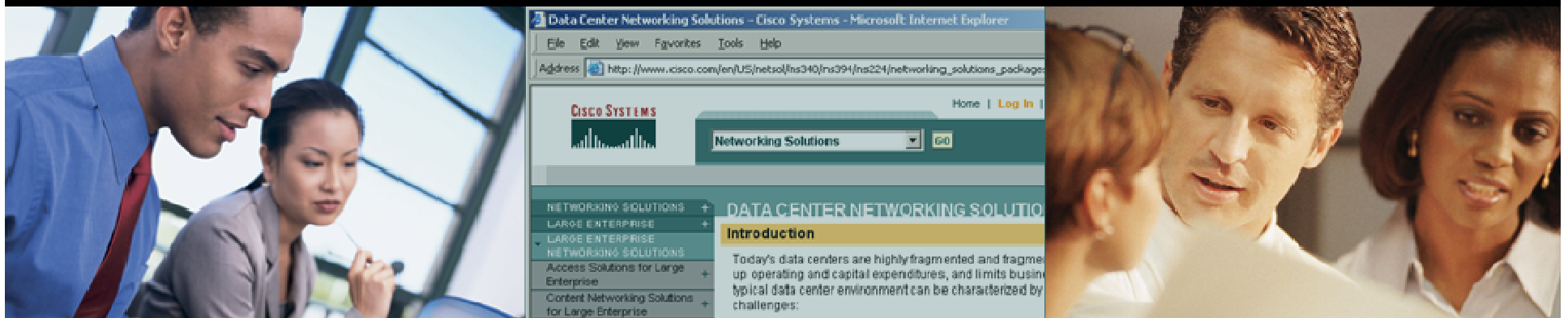
#### Data Center Assurance Program

For customers at the design and implementation stages of a data center networking project the data center assurance program provides validated configurations, test results and software versions that can be used as a baseline.

[Learn More](#)

# Additional Information

<http://www.cisco.com/go/datacenter>









# Data Loss Prevention


## State of the Market



**TEMPTATION.**

To stumble into somebody else's computer system. To be someplace you're really not supposed to be. And to get the

get to start with. That's it. From there, it's up to you. If you're clever enough and smart enough, you could discover a world



**HACKER**<sup>™</sup>

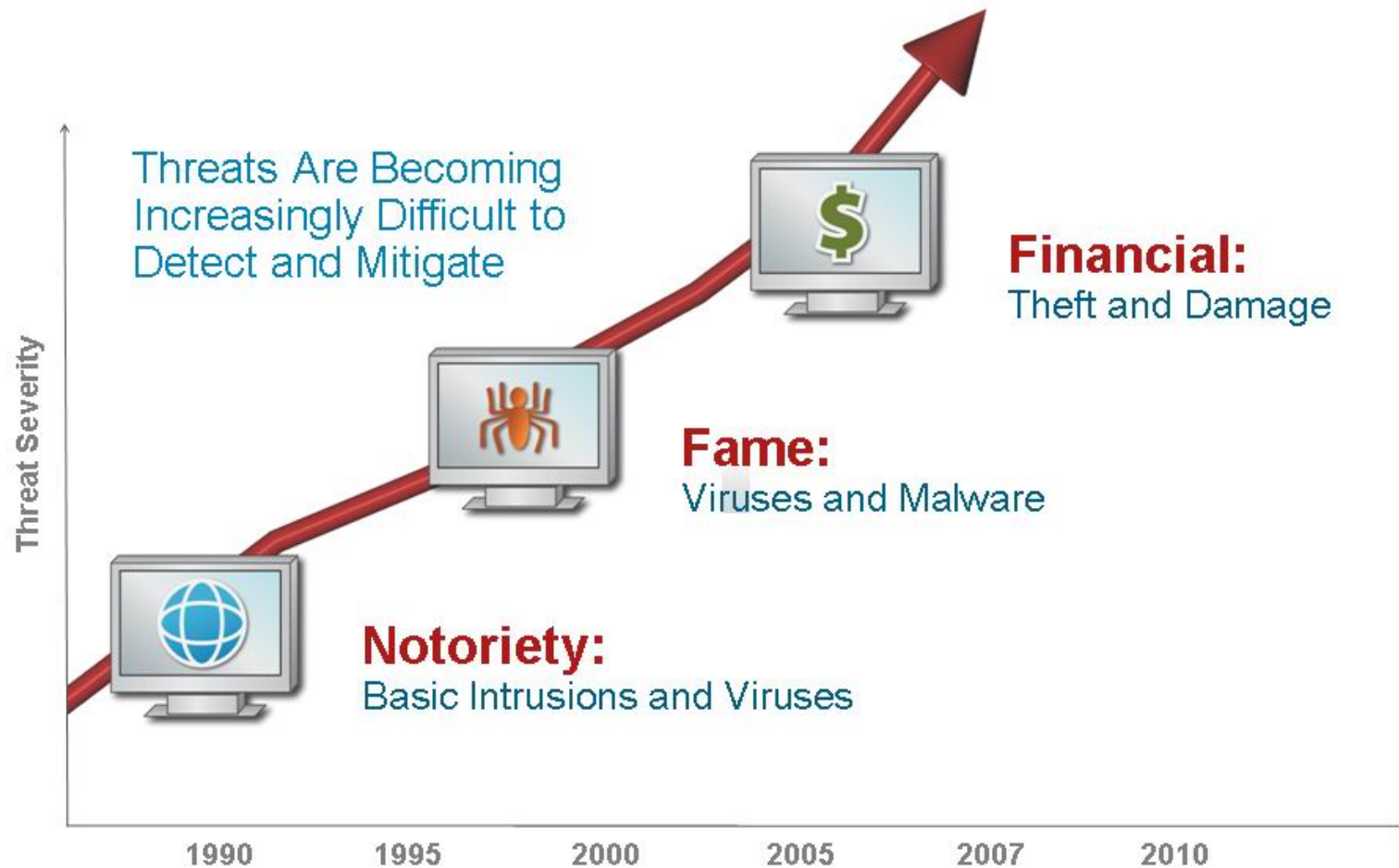
strange feeling that it really does matter. "LOGON PLEASE:" is all you

you've never before experienced on your computer. Very tempting.

*By Steve Catronight*

**ACTIVISION**  
HOME ENTERTAINMENT SOFTWARE

# The Evolution of Intent A Shift to Financial Gain



# Some Recent Data Loss News...

## Your Data & the

Courtesy of [Network Computing](#)

### How P2P leaks happen and what **Tape Loss Stuns UK Retail Giant**

**It's a tale of the (stolen) tapes over at major British pharmacist Boots**

MARCH 17, 2008 | What might have been a minor serious security incident when the personal data of

#### **LendingTree sues over data breach**

The mortgage broker says two former employees stole data.  
By Joseph Menn

Los Angeles Times Staff Writer

April 24, 2008

#### **Five Southern California home lenders in suit seeking loans through LendingTree Inc.,**

The suit, filed Monday in Orange County, matches prospective home buyers with limited access to consumer information.

APRIL 24, 2008 | [By James Rogers](#), April 24, 2008, 5:25 PM

Major U.K. chemist (drug store) chain [Boots](#) has joined the growing list of organizations suffering an [embarrassing storage snafu](#) after tapes containing personal details of thousands of customers and employees were stolen.

The tapes, which were stolen from a security subcontractor's car in the city of Bristol, contained the details of some 35,000 people, according to media reports. Boots has 1,500 stores in the U.K. and Ireland.

The records reportedly include the bank details of 27,000 customers of Boots' dental service, which is operated by [Medisure](#), as well as the personal details of some 8,000 Boots employees.

Neither Boots nor Medisure would respond to *Byte and Switch* requests for comment on the theft, which follows a string of headline-grabbing data breaches on both sides of the Atlantic. In the U.S. [the Universities of Miami and Virginia](#) recently suffered tape and laptop thefts, and the [the Swedish armed forces](#) were left reeling when a USB drive containing military secrets turned up at a public library earlier this year.

Lost tapes have been in the U.K. media spotlight since late last year, when Prime Minister Gordon Brown's government revealed that two disks containing personal details of 25 million people were [lost by that country's equivalent of the IRS](#).

The information on Boots' customers and employees was held on two tapes, according to a report in the U.K. [Metro](#) newspaper, which suggested that the data would not be easily accessible.

"The data on these tapes is technically complicated and only accessible with specialist IT equipment and software," a Medisure spokeswoman told *Metro*. "It was not stored on standard software or CDs and cannot be used on any home-style PC or laptop."

Police officers from Bristol's [Avon & Somerset Constabulary](#) are currently investigating the theft of the tapes.

*Have a comment on this story? Please click "Discuss" below. If you'd like to contact Dark Reading's editors directly, [send us a message](#).*

# What Does DLP Mean To Customer's Business?



## Customers Ticked Off Over Breach Notification

### Majority of customers have had their data exposed more than once, study says

APRIL 17, 2008 | Consumers are mad as hell about corporate security breaches, and they aren't going to take it anymore. Well, about a third of them aren't, anyway.

Some 31 percent of customers who have been notified of the possible exposure of their personal information have terminated their relationship with the breached company, according to a study published earlier this week by the Ponemon Institute and security vendor ID Experts.

More than half of the respondents (55 percent) said they have been notified more than once over the last two years about a breach involving their personal data. Eight percent said they have received four notifications or more.

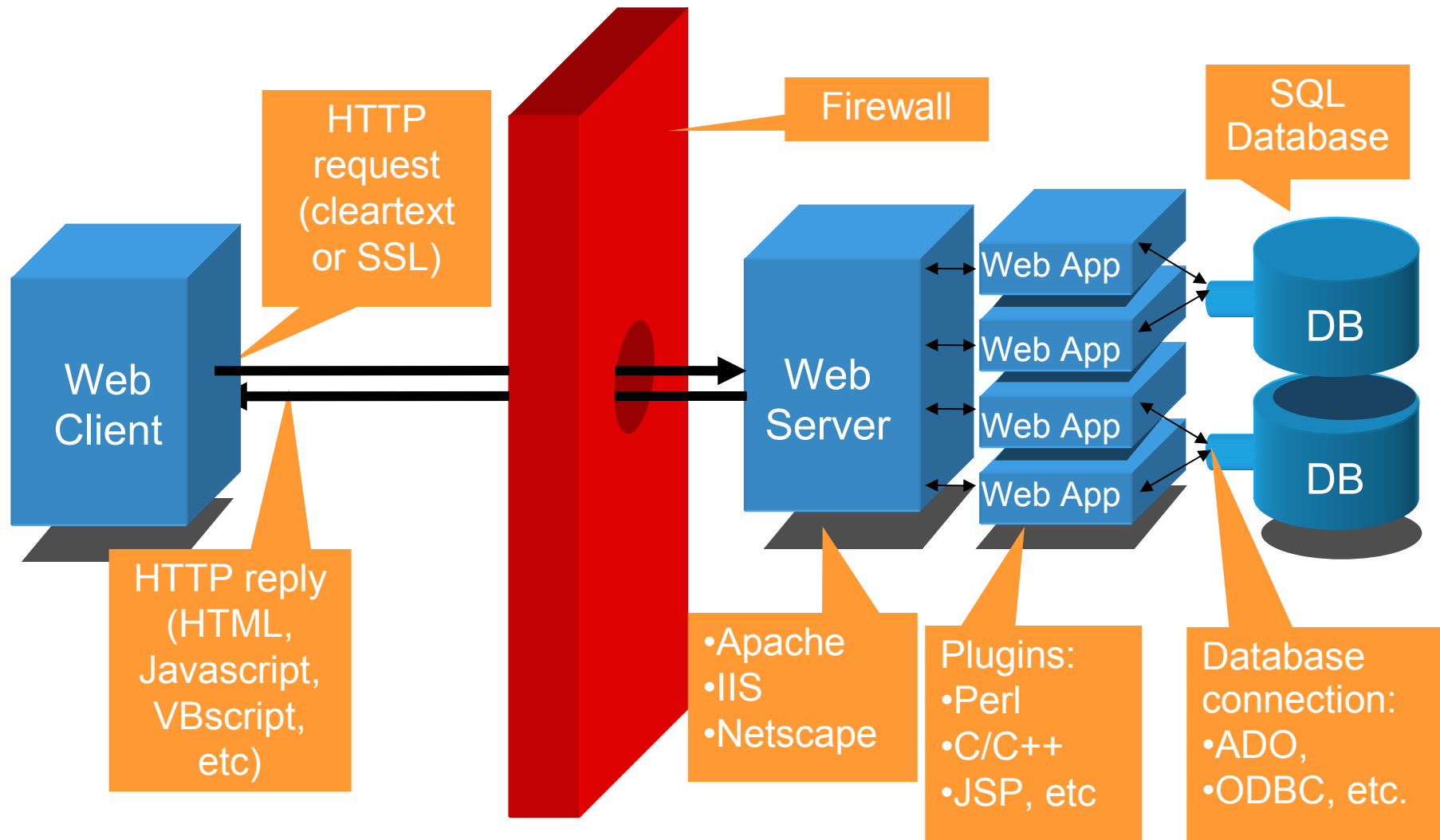
In the study, consumers also groused about the way they were notified of the breaches. More than 55 percent of respondents said they received their notifications more than one month after the incident, and more than 50 percent of respondents rated the timeliness, clarity, and quality of the notifications as either fair or poor.

Only 2 percent of respondents who had been notified of a data breach said they had definitely experienced identity theft as a result of the breach. Sixty-four percent said they weren't sure if they had fallen victim to identity theft.

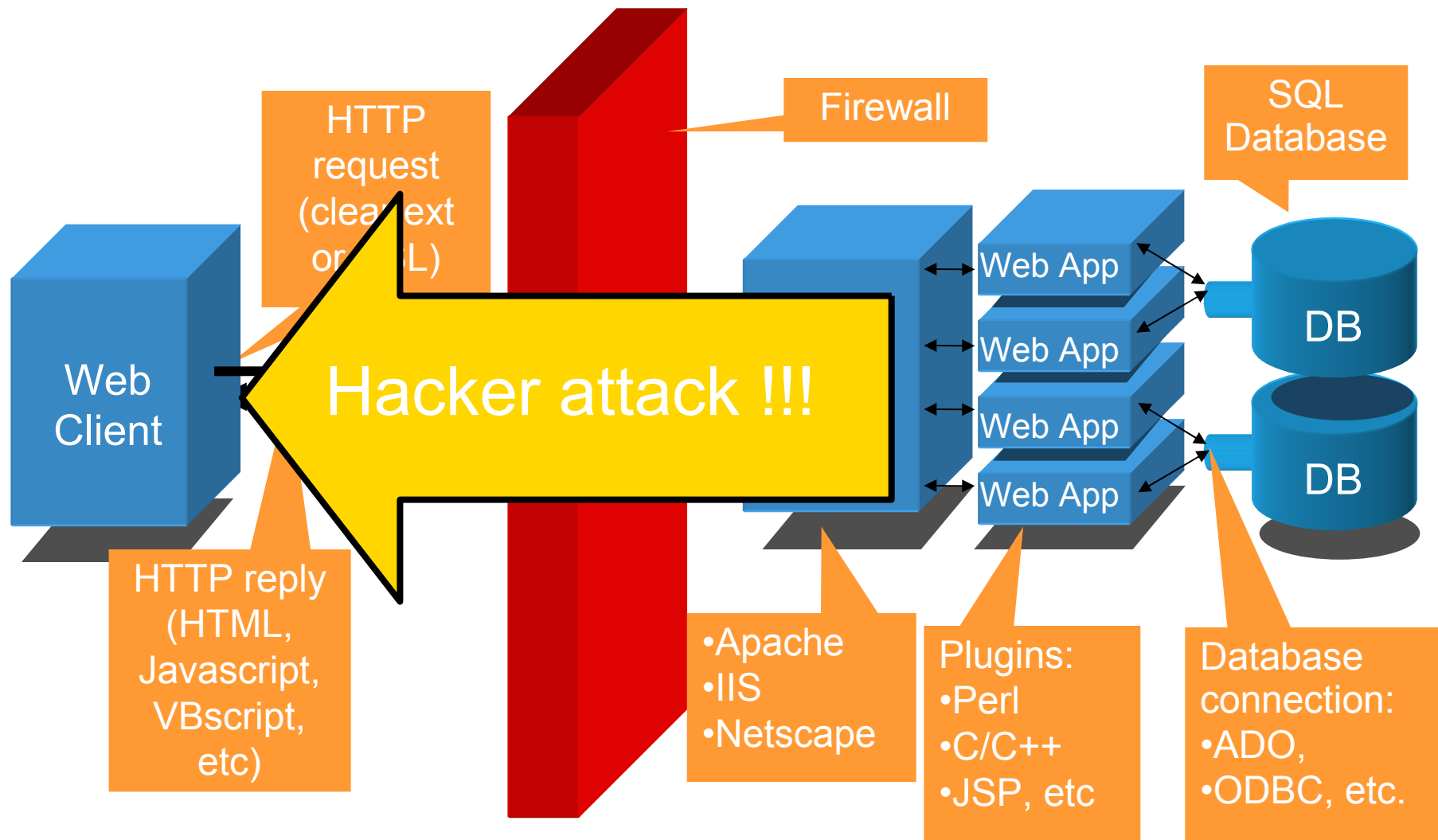
Twenty-six percent of respondents took no action after being notified of a breach. Fifty-seven percent said they lost trust and confidence in the breached organization.

— Tim Wilson, Site Editor, [Dark Reading](#)

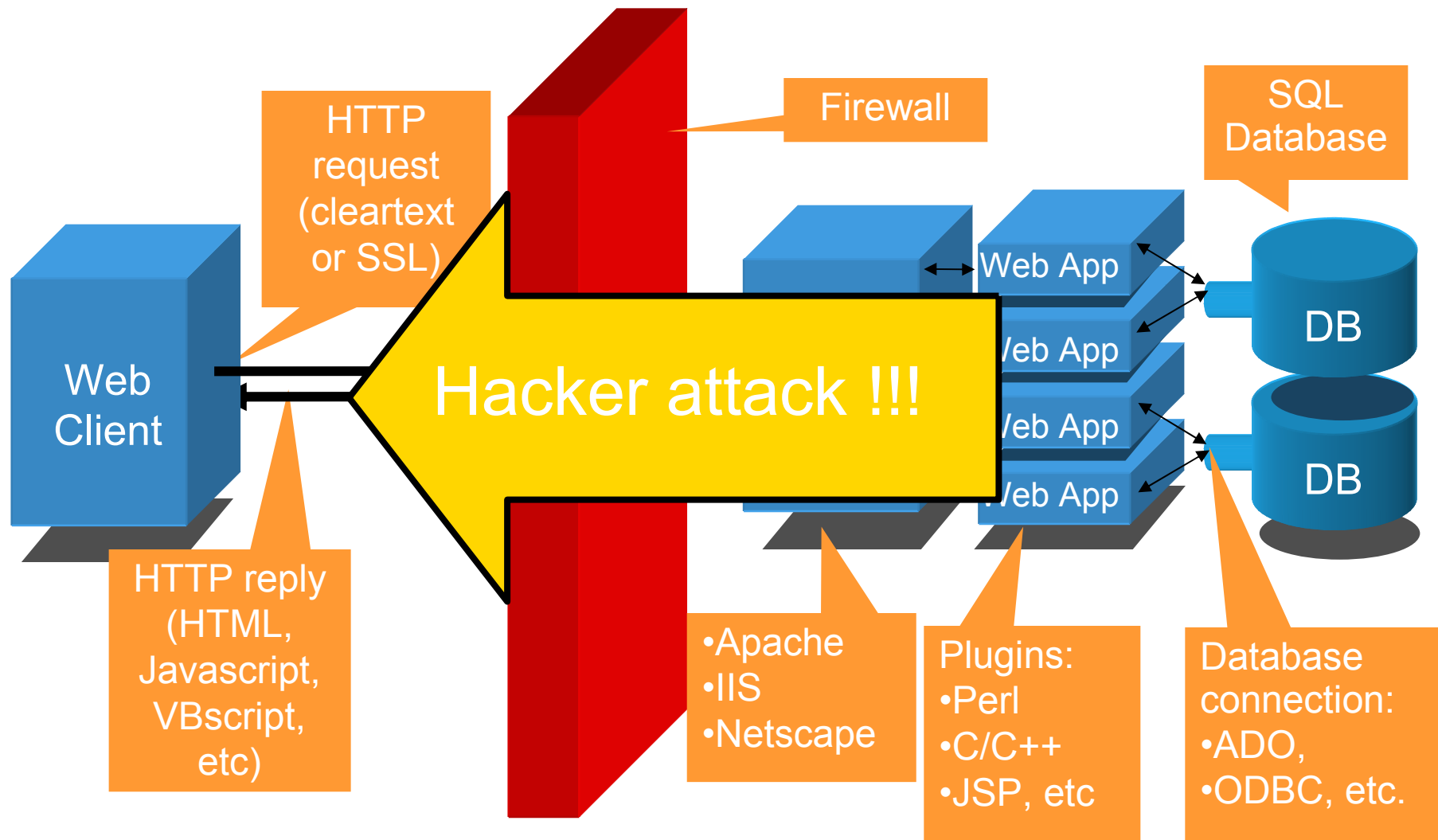
# Web servers vulnerable points



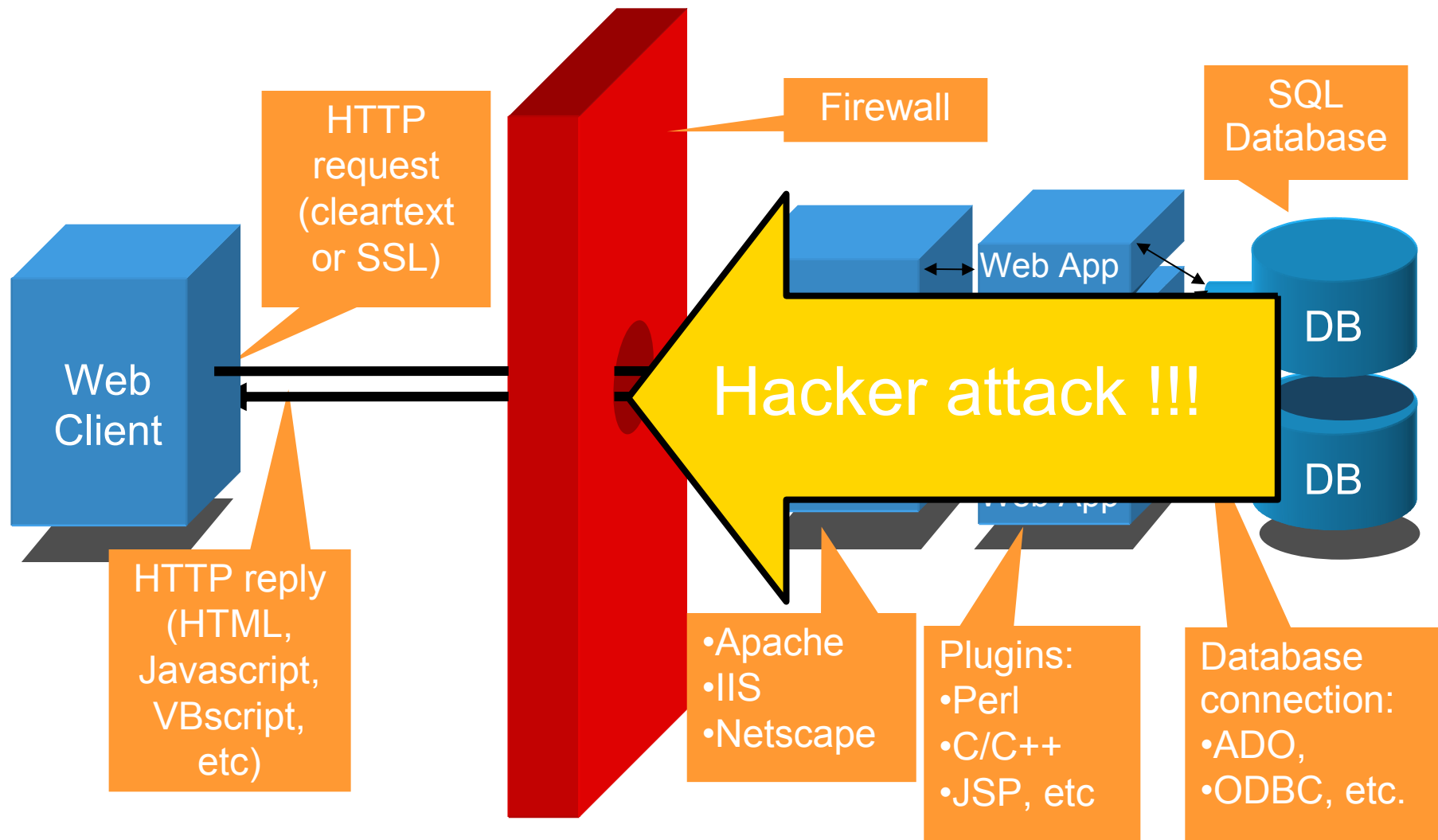
# Web browser



# SSL / protected lines

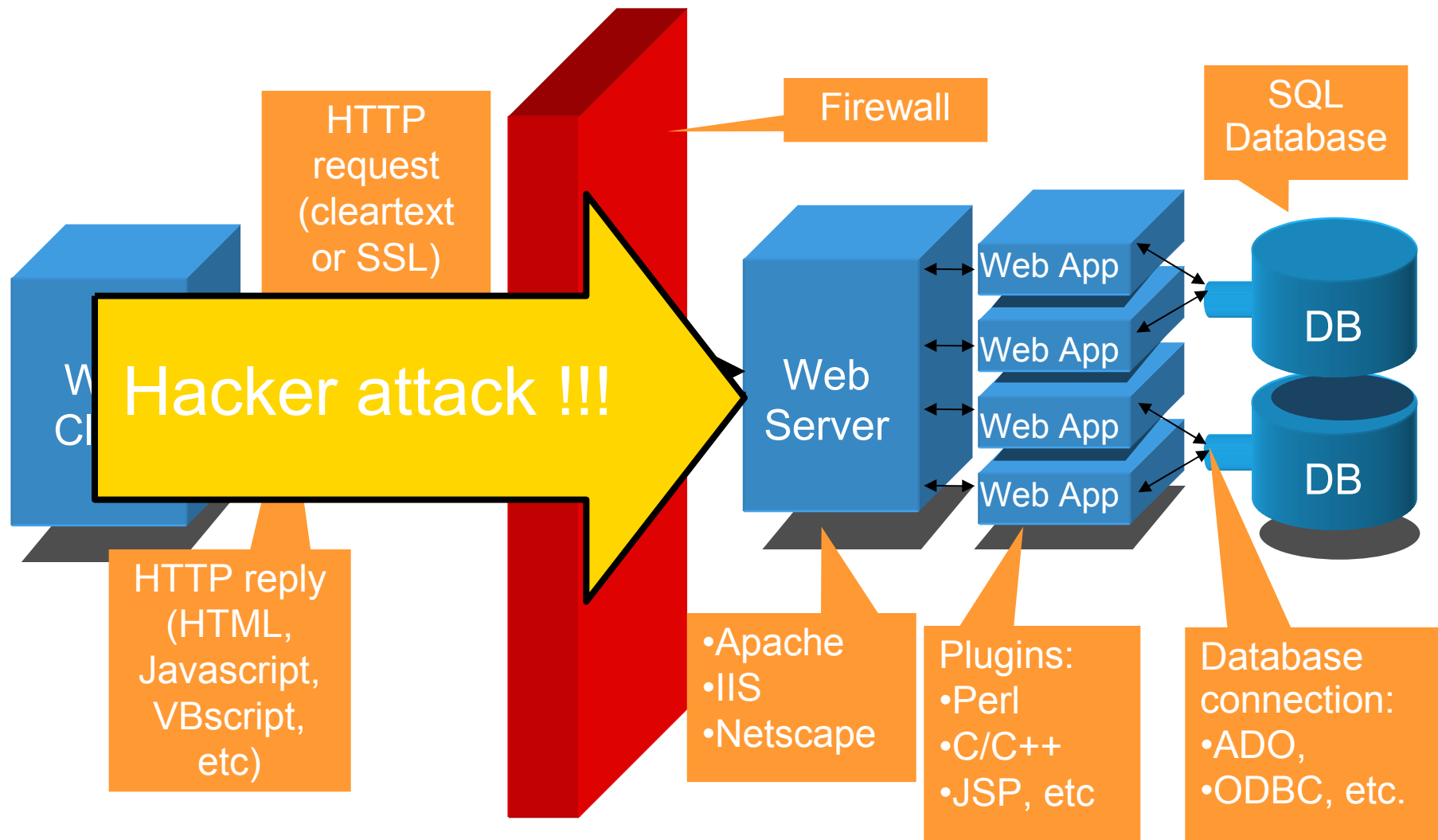


# Firewalls / Routers

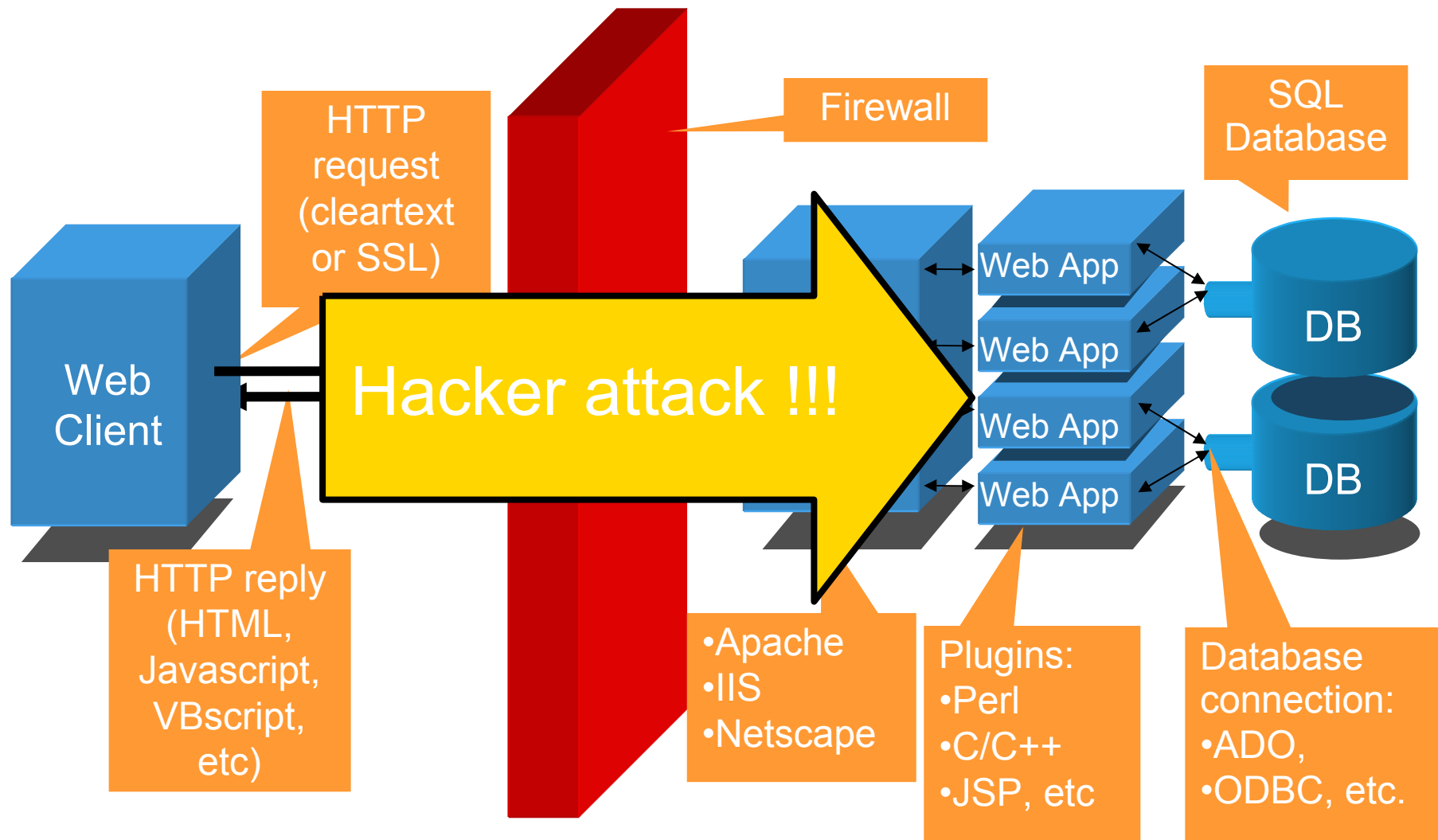




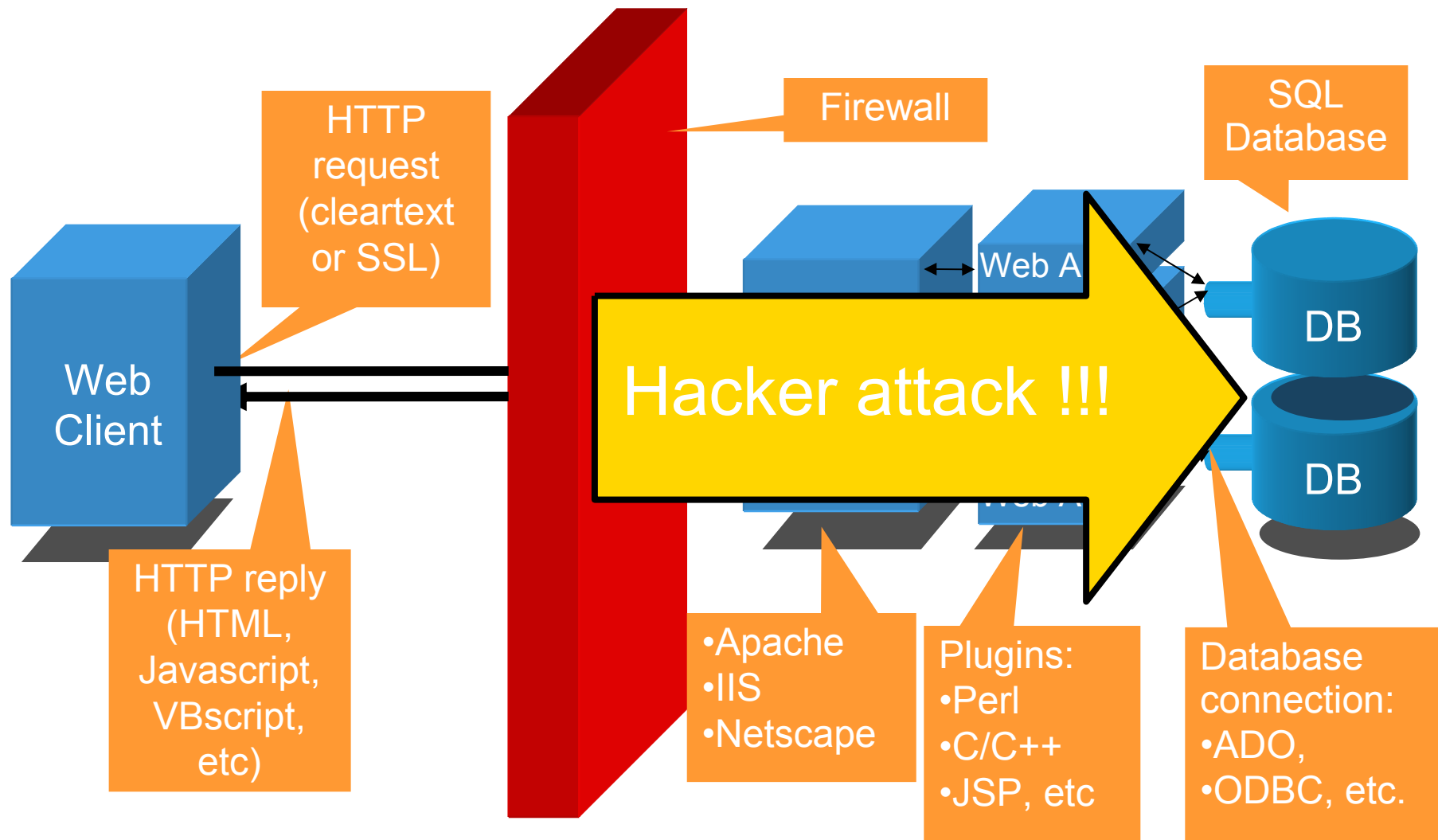
# Web server / OS



# Web applications

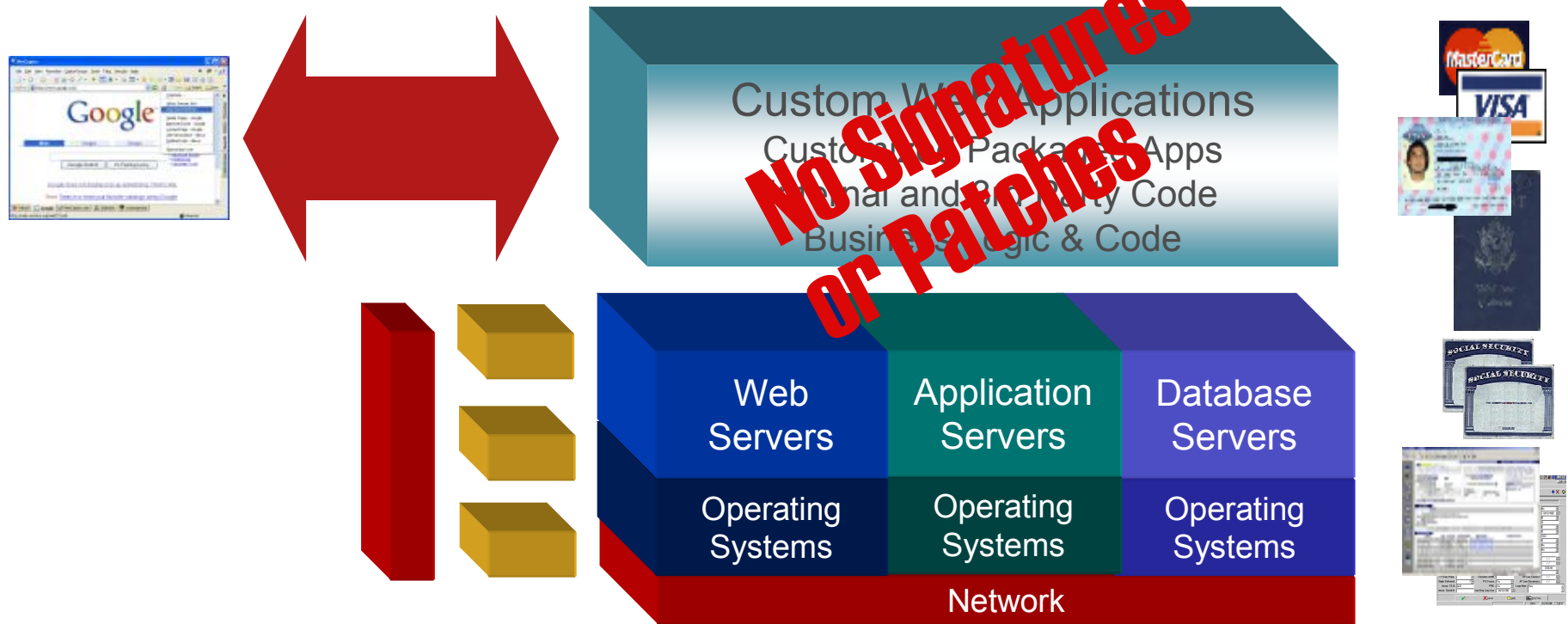


# Databases



# Focus of today's attacks

75% of Attacks Focused Here



No magic signatures or patches for your custom PHP script

# PCI-DSS 6.5 & 6.6



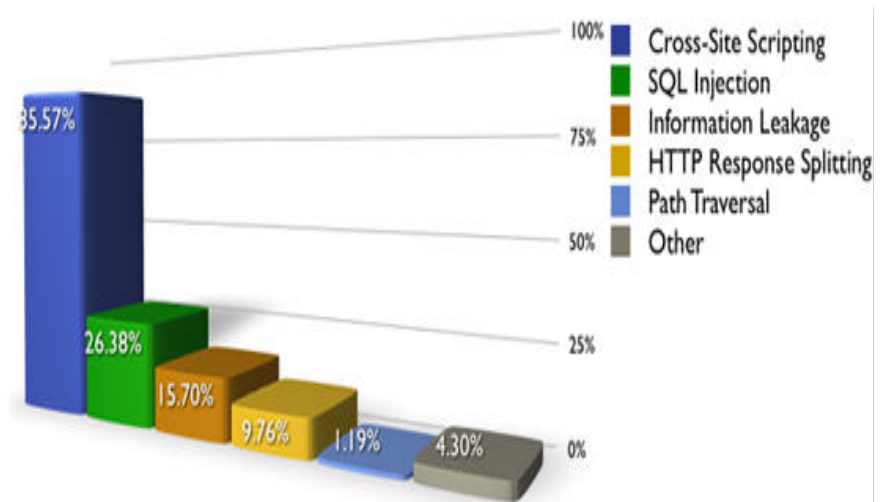
- Two sections of Payment Card Industry Data Security Standard focus on web application security: 6.5 and 6.6
- Section 6.6 mandates you install a Web App Firewall by end of June 08 to protect your applications against OWASP Top 10 attacks

- 6.5 Develop all web applications based on secure coding guidelines such as the Open Web Application Security Project guidelines. Review custom application code to identify coding vulnerabilities. Cover prevention of common coding vulnerabilities in software development processes, to include the following:
- 6.5.1 Unvalidated input
  - 6.5.2 Broken access control (for example, malicious use of user IDs)
  - 6.5.3 Broken authentication and session management (use of account credentials and session cookies)
  - 6.5.4 Cross-site scripting (XSS) attacks
  - 6.5.5 Buffer overflows
  - 6.5.6 Injection flaws (for example, structured query language (SQL) injection)
  - 6.5.7 Improper error handling
  - 6.5.8 Insecure storage
  - 6.5.9 Denial of service
  - 6.5.10 Insecure configuration management
- 6.6 Ensure that all web-facing applications are protected against known attacks by applying either of the following methods:
- Having all custom application code reviewed for common vulnerabilities by an organization that specializes in application security
  - Installing an application layer firewall in front of web-facing applications.
- Note: This method is considered a best practice until June 30, 2008, after which it becomes a requirement.*

# OWASP - 2007 Top Ten Attack List

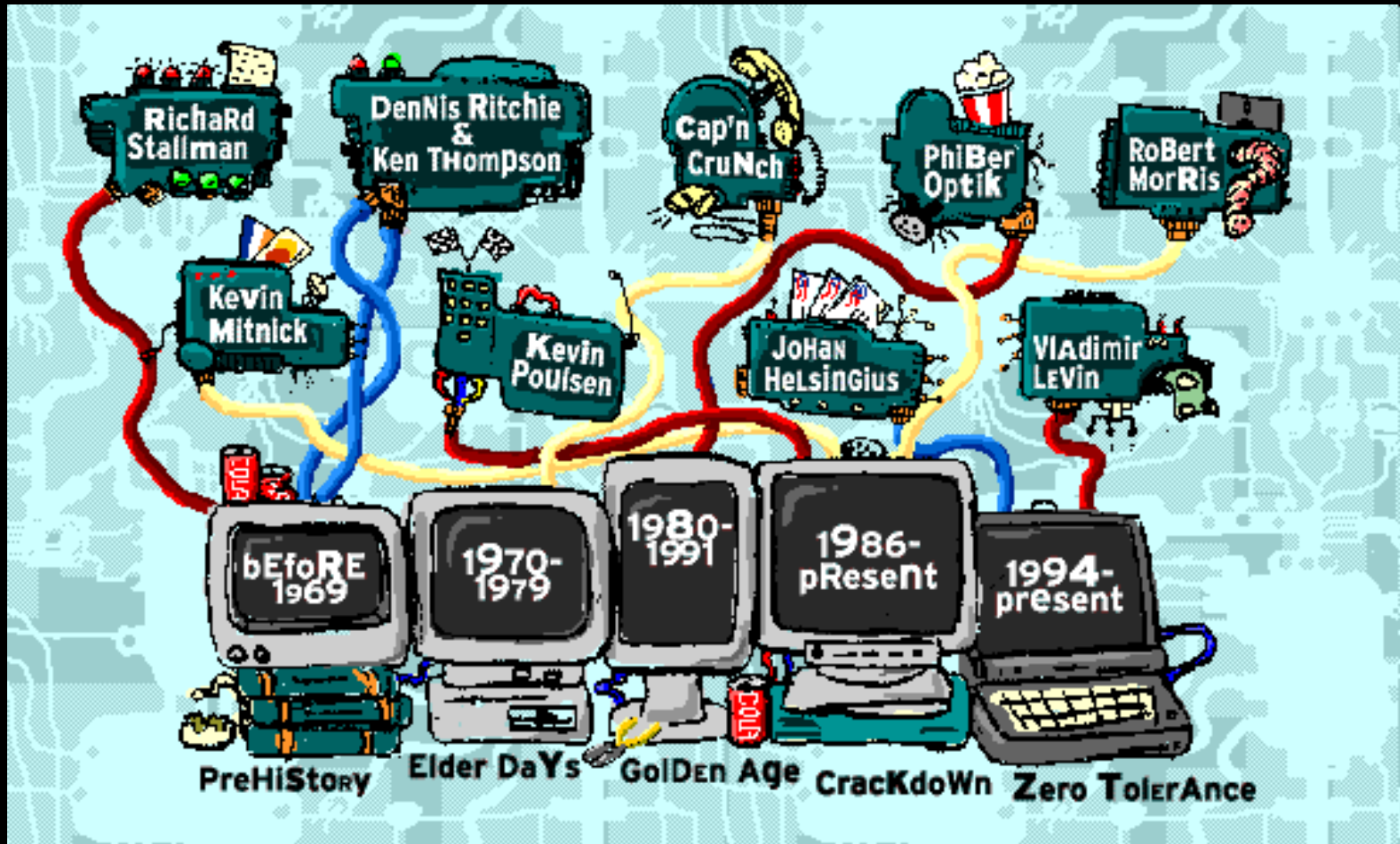
- A1 – Cross Site Scripting (XSS) .....
- A2 – Injection Flaws.....
- A3 – Malicious File Execution .....
- A4 – Insecure Direct Object Reference .....
- A5 – Cross Site Request Forgery (CSRF) .....
- A6 – Information Leakage and Improper Error Handling .....
- A7 – Broken Authentication and Session Management .....
- A8 – Insecure Cryptographic Storage.....
- A9 – Insecure Communications .....
- A10 – Failure to Restrict URL Access .....

Percentage of websites vulnerable by class (Top 5)



# ACE Cisco Web App - Firewall in action

## *An example using XSS*

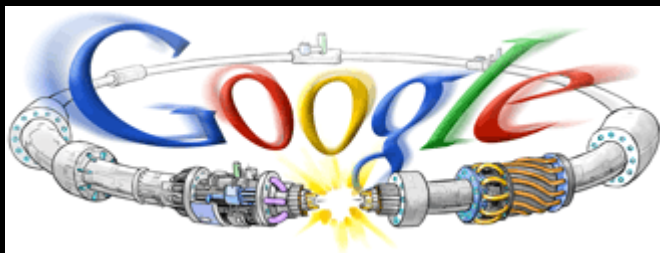
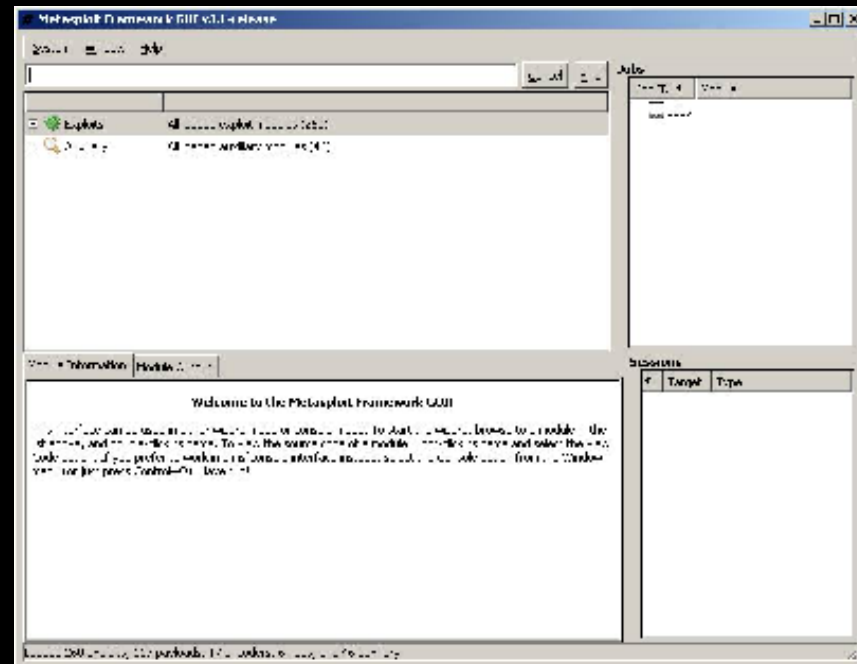
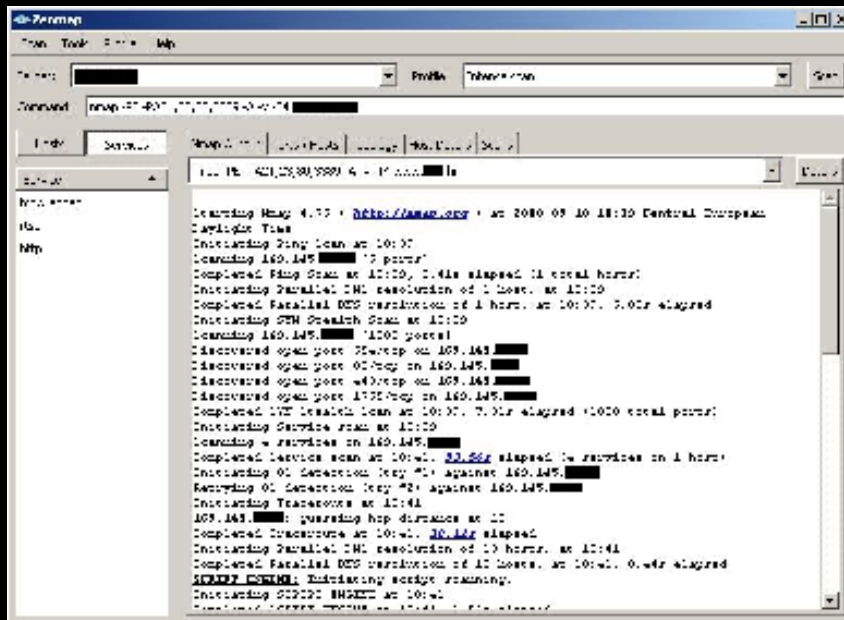


# Old gadget

Dimenzije: 27 cm x 22 cm x 1.9 cm  
Težina: 293 g

Tools: Google, Nmap, Metasploit

# ThinkPad X21





# New gadget

Dimenzije: 11.5 cm x 6.1 cm x 1.16 cm

Težina: 135 g



# New gadget



```

T-Mobile 10:05
Last login: Wed Sep 10 10:04:41 on ttty1
iPhone:~ mobile$ login
login: root
Password:
Last login: Wed Sep 10 10:05:02 on ttty1
iPhone:~ root# ifconfig
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 16384
    inet 127.0.0.1 netmask 0xff000000
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    inet 144.254.108.116 netmask 0xfffffa0 broadcast 144.254.108.127
    ether 00:1f:5b:45:bb:c6
ip1: flags=8011<UP,POINTOPOINT,MULTICAST> mtu 1450
    inet 87.252.131.22 --> 87.252.131.22 netmask 0xffffffff
ip2: flags=8011<UP,POINTOPOINT,MULTICAST> mtu 1500
iPhone:~ root#
    
```

```

T-Mobile 10:05
iPhone:~ root# nmap
Nmap 4.50 ( http://insecure.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sP: Ping Scan - go no further than determining if host is online
  -PN: Treat all hosts as online -- skip host discovery
  -PS/PA/PU [portlist]: TCP SYN/ACK or UDP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
    
```

```

T-Mobile 10:18
Last login: Wed Sep 10 10:16:13 on ttty3
iPhone:~ mobile$ msfconsole
    
```



```

msf >
=[ msf v3.2-release
+ -- --=[ 275 exploits - 122 payloads
+ -- --=[ 17 encoders - 6 nops
      =[ 52 aux
msf >
    
```

# Introducing Cisco's ACE Web App Firewall

- Builds on top of industry-leading ACE XML Gateway platform
- Simple software upgrade to install Web Application Firewall



---

Web Application Firewall

Protects your custom HTTP/HTML applications  
from high-impact web-borne attacks

---

SOA/Web Services/XML Threat Defense Secures and offload web services transactions

Extensive HTML and XML application security

# Cross-Site Scripting (XSS) attacks

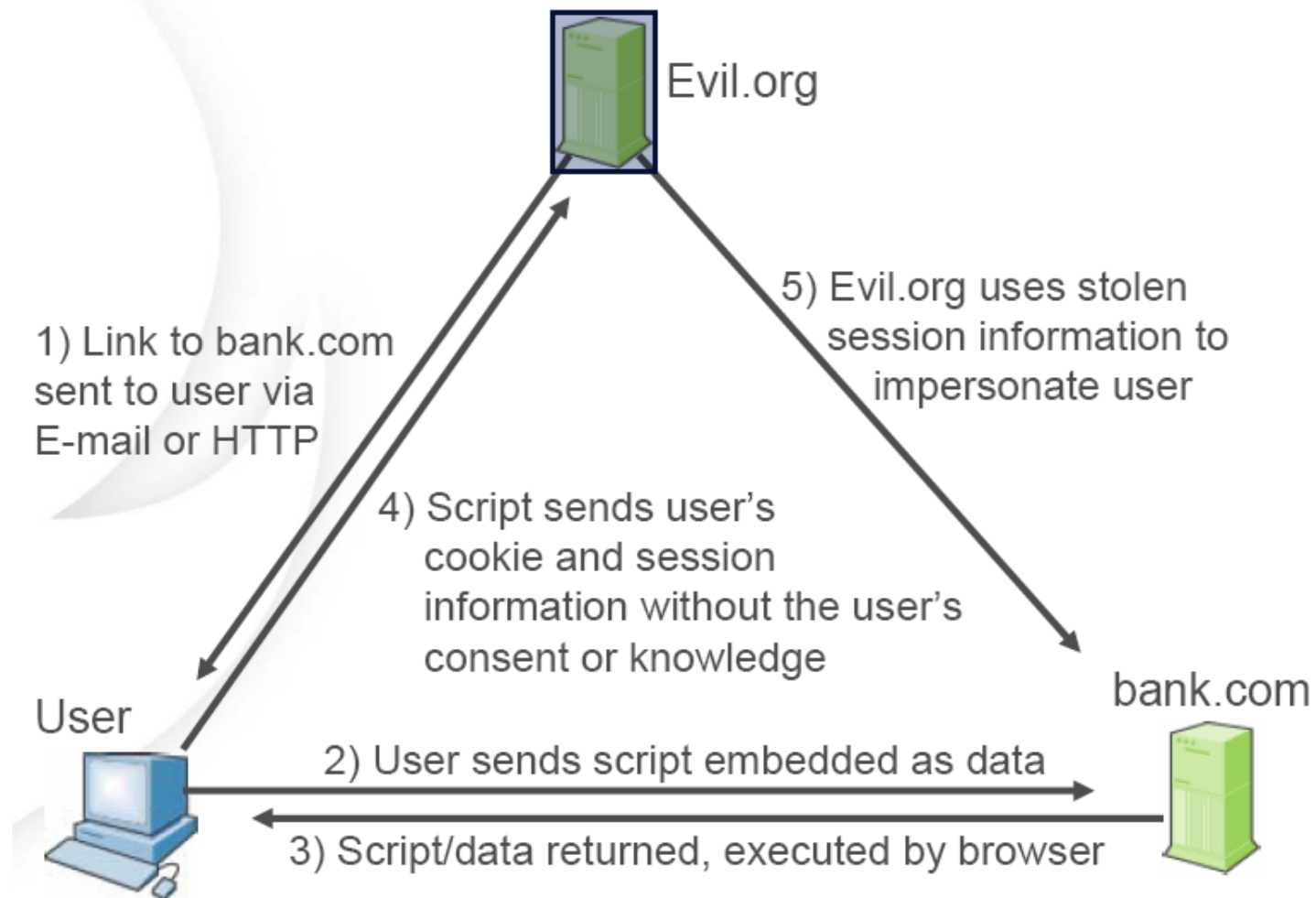
- **What is it?**

- A malicious script is echoed back into HTML returned from a trusted web site. The scripts executes locally on the client.
- Extremely widespread – some experts estimate 70%-80% of websites are vulnerable

- **What are the implications?**

- Web Site Defacement
- Session IDs stolen (cookies exported to hacker's site)
- Browser security compromised – control given to hacker
- All data sent between client and server potentially hijacked

# The XSS attack process



# Getting started with the Cisco ACE WAF

ACE XML Manager CISCO WEB APPLICATION FIREWALL administrator | Logout | Help

Subpolicy Shared Deploy Policy...

★ Manager Dashboard

Policy

- HTTP Ports & Hostnames
- Destination HTTP Servers
- Virtual Services**
  - Access Control
  - LDAP Servers
  - Exception Mapping Defaults
  - Denial-of-Service Protection
  - Content Screening Defaults
- Virtual Web Apps** >>
  - Web App Firewall Profiles
  - Web App Firewall Rules
- Policy Management
  - Subpolicies
- Resources
- Reports & Tools
  - Message Traffic Log
  - Web App Firewall Incidents
  - Event Log
  - Service Health
  - Performance Monitor
  - Cache Manager
  - Compliance Report
  - Service Directory
- Administration

Virtual Web Apps > New Virtual Web App

NEW VIRTUAL WEB APP

Basic Virtual Web App Wizard

Web App URL:

Web App Group: test

Firewall Profile: Basic Profile

Create in Monitor Mode

Save Changes Cancel

Specify the IP/name of the backend server

Call the WAF wizard

Monitor means the WAF alerts but doesn't block – extremely convenient if you're leery of deploying inline

# Getting started with the Cisco ACE WAF

The screenshot displays the Cisco ACE XML Manager interface for configuring a new virtual web application. The top navigation bar includes the Cisco logo, 'ACE XML Manager', 'CISCO WEB APPLICATION FIREWALL', and user information 'administrator | Logout | Help'. A 'Deploy Policy...' button is located in the top right.

The left sidebar contains a navigation menu with the following sections:

- ★ **Manager Dashboard**
- ▣ **Policy**
  - HTTP Ports & Hostnames
  - Destination HTTP Servers
  - Virtual Services**
    - Access Control
    - LDAP Servers
    - Exception Mapping Defaults
    - Denial-of-Service Protection
    - Content Screening Defaults
  - Virtual Web Apps** >>
    - Web App Firewall Profiles
    - Web App Firewall Rules
  - Policy Management**
    - Subpolicies
- ▣ **Resources**
- ▣ **Reports & Tools**
  - Message Traffic Log
  - Web App Firewall Incidents
  - Event Log
  - Service Health
  - Performance Monitor
  - Cache Manager
  - Compliance Report
  - Service Directory
- ▣ **Administration**

The main content area is titled 'Virtual Web Apps > New Virtual Web App'. It features a 'NEW VIRTUAL WEB APP' header and a 'Full Virtual Web App Editor' dropdown menu. The configuration fields are as follows:

- Web App Group:** test
- Virtual URL Request Filter:**
  - Port/Hostname: http://\* (Default HTTP port)
  - Path: /
  - Matching Mode: prefix (dropdown menu showing options: prefix, exact, regex)
  - Methods: ignore
  - HTTP Headers: ignore
  - Parameters: ignore
- Destination Server:** Server: http://172.25.89.140 (172.25.89.140)
- Firewall Profile:** Profile: Basic Profile (dropdown menu with a 'details' link) and a 'Monitor Mode' checkbox.

An orange callout box labeled 'Profile' has a red arrow pointing to the 'Basic Profile' dropdown menu. At the bottom, there are 'Save Changes' and 'Cancel' buttons.

# Protecting the web site from XSS

The screenshot displays the Cisco ACE XML Manager interface. The top navigation bar includes the Cisco logo, 'ACE XML Manager', 'CISCO WEB APPLICATION FIREWALL', and user information: 'Authenticated by Reactivity administrator | Logout | Help'. The main content area is titled 'Web App Firewall Profiles > Test profile'. It features a left-hand navigation menu with categories like 'Manager Dashboard', 'Policy', 'Virtual Services', 'Virtual Web Apps', 'Policy Management', 'Resources', 'Reports & Tools', and 'Administration'. The 'Web App Firewall Profiles' menu item is highlighted. The main configuration area shows the 'Test profile' details, including a 'Name: Test profile' and a 'Description:'. Below this is the 'FIREWALL CONFIGURATION' section, which is divided into 'Active Security' and 'Message Rewrite' sub-sections. The 'Active Security' section lists various security features with their status and an 'edit' link for each:

Active Security		
HTTP Header Processing	...	[ edit ]
HTTP Exception Mapping	not configured	[ edit ]
Referer Enforcement	disabled	[ edit ]
Cookie Security	cookies processing is disabled	[ edit ]
Data Overflow Defense	...	[ edit ]

The 'Message Rewrite' section includes:

Message Rewrite		
CARDNUMBERREWRITING	-- disabled --	[ edit ]

Below the 'Message Rewrite' section is the 'Message Inspection' section, which lists several injection types, all of which are currently disabled:

Message Inspection		
SSIINJECTION	-- disabled --	[ edit ]
COMMANDINJECTION	-- disabled --	[ edit ]
LDAPINJECTION	-- disabled --	[ edit ]
CROSSSITESCRIPTING	-- disabled --	[ edit ]
SQLINJECTION	-- disabled --	[ edit ]

At the bottom of the configuration area, there are buttons for 'Exit to Profiles List', 'Duplicate', and 'Remove'. A red arrow points from an orange callout box labeled 'XSS protection' to the 'CROSSSITESCRIPTING' entry in the Message Inspection table.



# Fine-tuning a security profile

ACE XML Manager | CISCO WEB APPLICATION FIREWALL | administrator | Logout | Help

Subpolicy: Shared | Deploy Policy...

Manager Dashboard

- Policy
  - HTTP Ports & Hostnames
  - Destination HTTP Servers
  - Virtual Services
    - Access Control
    - LDAP Servers
    - Exception Mapping Defaults
    - Denial-of-Service Protection
    - Content Screening Defaults
  - Virtual Web Apps
    - Web App Firewall Profiles >>
    - Web App Firewall Rules
  - Policy Management
    - Subpolicies
- Resources
- Reports & Tools
  - Message Traffic Log
  - Web App Firewall Incidents
  - Event Log
  - Service Health
  - Performance Monitor
  - Cache Manager
  - Compliance Report
  - Service Directory
- Administration

Web App Firewall Profiles > Test profile > Configure

Rule Group: CROSSSITESCRIPTING

**RULE GROUP: CROSSSITESCRIPTING** (XSS rules level)

Mode: Enabled

Level: strict (basic, moderate, strict)

Actions

Event Log: Info-level Event

Response: Return an HTTP Error Response - 400 Client Error (Action to take when a XSS is detected)

Save Changes | Cancel

Return an HTTP Error Response - 400 Client Error  
Return an HTTP Error Response - 500 Server Error  
Return a Custom HTTP Error Response  
Allow Message

# Profile ready to be deployed

**Web App Firewall Profiles > Test profile**

---

**GENERAL**

Name: Test profile  
Description:

**FIREWALL CONFIGURATION**

**Active Security**

HTTP Header Processing	...	[ edit ]
HTTP Exception Mapping	map responses with codes 500	[ edit ]
Referer Enforcement	disabled	[ edit ]
Cookie Security	sign cookies	[ edit ]
Data Overflow Defense	...	[ edit ]

**Message Rewrite**

CARDNUMBERREWRITING	-- disabled --	[ edit ]
---------------------	----------------	----------

**Message Inspection**

SSIINJECTION	-- disabled --	[ edit ]
COMMANDINJECTION	-- disabled --	[ edit ]
LDAPINJECTION	-- disabled --	[ edit ]
CROSSSITESCRIPTING	enabled strict info	[ edit ]
SOLINJECTION	enabled strict info	[ edit ]

[Exit to Profiles List](#)

XSS protection enabled with level strict

# Associate the profile to the web site

**Virtual Web Apps > test** ?

---

**WEB APP GROUP** [ [EDIT](#) ]

Name: test  
Default Profile: Basic Profile

**VIRTUAL WEB APPS** [ [ADD A VIRTUAL WEB APP](#) ]

Virtual URL: http://\*/ [ [edit](#) ] [ [delete](#) ]  
Destination: http://foobarfoo2k.cisco.com

⊕ **Firewall Profile:** [Test profile](#)

⊕ **Firewall Modifiers (1)** [ [add modifier](#) ]

[Exit to Virtual Web Apps](#) [Disable Virtual Web App](#) [Switch to Monitor Mode](#) [Turn Off Monitor Mode](#)  
[View Logs](#) [Remove](#)

Profile "Test" mapped to our web site

# Deploy the policy to the WAF gateway(s)

The screenshot shows the Cisco ACE XML Manager interface. The top navigation bar includes the Cisco logo, 'ACE XML Manager', 'CISCO WEB APPLICATION FIREWALL', and user information 'administrator | Logout | Help'. Below the navigation bar, there is a 'Subpolicy' dropdown set to 'Shared' and a 'Deploy Policy...' button. The main content area is titled 'Policy Manager > Deploy > Step 1 of 3: Review Changes'. It contains a message: 'Please review the changes in the current working compared to the previously deployed version before continuing.' The content is organized into sections: 'WAFHANDLER' with a 'Changed' status and a list item 'http://\*/' with a 'detailed differences' link; and 'WAFPROFILE' with a 'New' status and a list item 'Test profile'. At the bottom of the main content area are two buttons: 'Continue to Next Step >' and 'Exit to Policy Manager'. A red arrow points from a text box to the 'Test profile' link.

**WAFHANDLER**  
**Changed** - these are different between the previously deployed version and the current version:  
! [http://\\*/](#) [detailed differences](#)

**WAFPROFILE**  
**New** - these exist in the current version, but not the previously deployed version:  
+ [Test profile](#)

[Continue to Next Step >](#) [Exit to Policy Manager](#)

Deltas between current applied policy and proposed one are highlighted

# Verification of successful deployment

Subpolicy **Shared** Deploy Policy...

**Manager Dashboard**

- Policy**
  - HTTP Ports & Hostnames
  - Destination HTTP Servers
  - Virtual Services**
    - Access Control
    - LDAP Servers
    - Exception Mapping Defaults
    - Denial-of-Service Protection
    - Content Screening Defaults
  - Virtual Web Apps**
    - Web App Firewall Profiles
    - Web App Firewall Rules
- Policy Management** >>
  - Subpolicies
- Resources**
- Reports & Tools**
  - Message Traffic Log
  - Web App Firewall Incidents
  - Event Log
  - Service Health
  - Performance Monitor
  - Cache Manager
  - Compliance Report
  - Service Directory
- Administration**

**Policy Manager > Deploy > Step 3 of 3: Compile and Deploy**

This policy is compiled and can now be deployed. To deploy a different policy, load it from the [Policy History](#).

[ [check all](#) | [unchecked all](#) ]

	ACE XML Gateway	Version	Licensed	Compiled Policy Timestamp & ID	Policy Description	
<input type="checkbox"/>	171.69.45.233	6.0Alpha5-2008-02-05T19	yes	Feb 13 2008 01:24:20 AM PST ea6b569bce4cd863		
	ACE XML Gateway	Version	Licensed	Deployed Policy Timestamp & ID	Deployed Policy Description	Status
<input type="checkbox"/>	171.69.45.233	6.0Alpha5-2008-02-05T19	yes	Feb 13 2008 01:24:21 AM PST ea6b569bce4cd863	--	Up to date

**timestamps**

**Policies can be deployed to N gateways**

# The web site is under attack!

## Web App Firewall Incidents

Group by Virtual Web App -- all records --

Update View Incident records are available for the last 12 minutes CSV Export Raw Data

Description	Incidents	%
Incidents By Virtual Web App at Feb 13 2008 01:50:35 AM PST	4	100.0%
test	4	100.0% [ events ]
http://*/	4	100.0% [ events ]
CrossSiteScripting	1	25.0% [ events ]
Data Overflow	2	50.0% [ events ]
SqlInjection	1	25.0% [ events ]

Immediate incident report view

# Let's drill down

## Event Log Viewer

**Current Manager Event Logging** alert, error, warning, notice [ [edit](#) ]  
**Current ACE XML Gateway Event Logging** alert, error, warning, notice, info, debug [ [edit](#) ]

During  search events logged on  for events of type  Display a maximum of  events per page [ [Update](#) ]

with message GUID   
category  (e.g., /policy/access)  
component  (e.g., core or console)  
description

**EVENT LOG SEARCH RESULTS AT FEB 18 2008 09:30:39 AM PST**

First < Prev Displaying events 1 - 8 Next > (more recent events are shown at the top)

Time (PST)	Description	Message GUID	Host	Component	Category
Feb 18 2008 09:29:41.714 AM	<b>W</b> CROSSITESCRIPTING.CrossSiteScripting(152)REQUEST_POSTPARAM['name'] detected by rule; returning error.	<a href="#">45ABFA2D000014292D980A4F08849B2D</a>	ciscowaf	reactor	/waf/incid
Feb 18 2008 09:29:41.714 AM	<b>W</b> Terminating HTTP session: 500 An error occurred	<a href="#">45ABFA2D000014292D980A4F08849B2D</a>	ciscowaf	reactor	/session
Feb 18 2008 09:29:41.714 AM	<b>W</b> An error occurred for this request: An error occurred while handling the request.	<a href="#">45ABFA2D000014292D980A4F08849B2D</a>	ciscowaf	reactor	/error

ID of the rule which caused the alert

The name of the attack vector is provided

# Detailed security event drill down

EVENT LOG SEARCH RESULTS AT FEB 18 2008 09:34:51 AM PST	
<input type="button" value="First"/> <input type="button" value=" &lt; Prev"/> Displaying events 1 - 14 <input type="button" value=" Next &gt;"/> (more recent events are shown at the top)	
Time (PST)	Description
Feb 18 2008 09:29:41.714 AM	D Awaiting new request on inbound connection
Feb 18 2008 09:29:41.714 AM	W CROSSSITESCRIPTING.CrossSiteScripting1:52:REQUEST_POSTPARAM['name'] detected by rule; returning error.
Feb 18 2008 09:29:41.714 AM	W Terminating HTTP session: 500 An error occurred
Feb 18 2008 09:29:41.714 AM	W An error occured for this request: An error occurred while handling the request.
Feb 18 2008 09:29:41.714 AM	I No policy-specific error handler for WAF.CROSSSITESCRIPTING.CrossSiteScripting1:\${SIG_MATCH_SIGID}:\${SIG_MATCH_INPUT_NAME):
Feb 18 2008 09:29:41.713 AM	I Checking limit 1
Feb 18 2008 09:29:41.713 AM	I Checking limit 0
Feb 18 2008 09:29:41.713 AM	I Checking 3 limits
Feb 18 2008 09:29:41.713 AM	I Accepted a new HTTP POST request from 171.69.141.0 for /SCRIPTS/xss.php
Feb 18 2008 09:29:41.713 AM	I HTTP POST request for /SCRIPTS/xss.php from 171.69.141.0 matched Port 'Default HTTP port'; checking for handler
Feb 18 2008 09:29:41.713 AM	I Performing normalization on '/SCRIPTS/xss.php' with mode 7211
Feb 18 2008 09:29:41.713 AM	D HTTP Trace IN: Content-Type: application/x-www-form-urlencoded Content-Length: 58  name=%3Cscript%3Ealert%28document.cookie%29%3C%2Fscript%3E
Feb 18 2008 09:29:41.711 AM	D HTTP Trace IN: POST /SCRIPTS/xss.php HTTP/1.1 Host: foobarfoo2k.cisco.com User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8.1.12) Gecko/20080201 Firefox/2.0.0.12 Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5 Accept-Language: en-us,en;q=0.5 Accept-Encoding: gzip,deflate Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7 Keep-Alive: 300 Connection: keep-alive Referer: http://foobarfoo2k.cisco.com/SCRIPTS/xss.php Cookie: cec_user_id=cpaggen; SMIDENTITY=zv5hvjchtfb9t4nGfXC5vs0zQJXocY3BBaVM0802pEHDUDb4mPyEBkbj0dOq+xQ//TRZiz0UpMcRa3IWnmLDn3PaHSz74dXFY3ILI

Full dump of incoming request



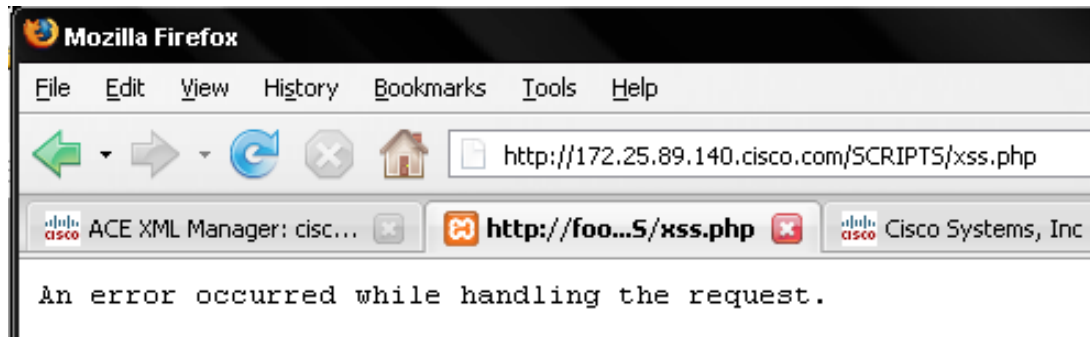
# Fine-tuning a security profile

Web App Firewall Attack Signatures		
Signature ID	Pattern	Info
<input type="checkbox"/> CreditCardNumber		
CreditCardNumber.1		{name=15DigitsCreditCardNumber, regex=\b[[:digit:]]{4}([[:digit:]]{6}\1[[:digit:]]{5}\b}
CreditCardNumber.2		{name=16DigitsCreditCardNumber, regex=\b[[:digit:]]{4}([[:digit:]]{12}\1[[:digit:]]{4}\b}
<input type="checkbox"/> CrosssiteScriptingXSSAttack		
CrosssiteScriptingXSSAttack.1	type	{nocase=true, name=type (opt) text (opt) javascript:, regex=\btype\b\W*?\btext\b\W*?\bjava?scrip
CrosssiteScriptingXSSAttack.10	onmouseover	{nocase=true, name=onmouseover (opt)=, regex=\bonmouseover\b\W*?=-}
CrosssiteScriptingXSSAttack.100	mocha:	{nocase=true, name=mocha:, regex=\bmocha:}
CrosssiteScriptingXSSAttack.101	style	{nocase=true, name=style = followed by expression (, regex=\bstyle\b\W*?=.*\bexpression\b\W*}{}
CrosssiteScriptingXSSAttack.102	settimeout	{nocase=true, name=settimeout (opt)(, regex=\bsettimeout\b\W*}{}
CrosssiteScriptingXSSAttack.103	src	{nocase=true, name=src (opt) javascript:, regex=\bsrc\b\W*?\bjavascript:}
CrosssiteScriptingXSSAttack.104	src	{nocase=true, name=src (opt) vbscript:, regex=\bsrc\b\W*?\bvbscript:}
CrosssiteScriptingXSSAttack.105	src	{nocase=true, name=src (opt) shell:, regex=\bsrc\b\W*?\bshell:}
CrosssiteScriptingXSSAttack.106	src	{nocase=true, name=src (opt) http:, regex=\bsrc\b\W*?\bhttp:}
CrosssiteScriptingXSSAttack.107	activexobject	{nocase=true, name=activexobject, regex=\bactivexobject\b}
CrosssiteScriptingXSSAttack.108	alert	{nocase=true, name=alert (opt)(, regex=\balert\b\W*}{}
CrosssiteScriptingXSSAttack.109	<body	{nocase=true, name=<body followed by(opt) background, regex=<body\b.*?\bbackground\b}
CrosssiteScriptingXSSAttack.11	onmouseout	{nocase=true, name=onmouseout (opt)=, regex=\bonmouseout\b\W*?=-}
CrosssiteScriptingXSSAttack.110	<body	{nocase=true, name=<body followed by(opt) onload, regex=<body\b.*?\bonload\b}
CrosssiteScriptingXSSAttack.111	<input	{nocase=true, name=<input followed by(opt) type (opt) image, regex=<input\b.*?\btype\b\W*?\bimage\b}
CrosssiteScriptingXSSAttack.112	<script	{nocase=true, name=<script, regex=<script\b}
CrosssiteScriptingXSSAttack.113	<meta	
CrosssiteScriptingXSSAttack.114	<!	

Hundreds of XSS rules shipped from factory

Each rule has a unique ID and a security level (basic, moderate, strict)

# What the user/hacker/victim sees



- The error message and HTTP return codes are fully customizable! You can return your own HTML code and for example redirect the hacker to the main page.



