CUNY Information Managers Forum

Red Hat, Inc

Introductions

- **Shawn Wells <swells@redhat.com>**
  Federal Solutions Architect
- **Mark St. Laurent <mstlaure@redhat.com>**
  Federal Solutions Architect / Security SME / Forensics Expert
- **Michael Brown <mbrown@redhat.com>**
  Federal Solutions Architect / Identity Management SME

Agenda

Time	Topic	Speaker
9:30 – 10:00	Meet and Greet - Breakfast	All
10:00 - 11:00	RHEL5 Overview	Shawn
11:00 - 12:00	RHEL & SELinux	Dave, Richard
12:00 - 12:45	Lunch & Learn – (SELinux Live Lab: Designing your own Policies) (OPTIONAL)	Red Hat
12:45 - 14:30	Securing the Infrastructure, Continud (Incident Response)	Mark
14:30 - 15:30	Enterprise Directory Server	Mike
15:30 – 16:00	Certificate Management	Mike

Red Hat, Inc

- Headquarters: Raleigh, NC
- Founded 1993
- Public 1999 (NYSE: RHT)
- Operating in 27 countries
- Over 2200 Employees worldwide
- Over 50% are engineers
- 80% Government/Commercial Linux Market Share
- 40+% Year over Year Growth (For 23 straight quarters)

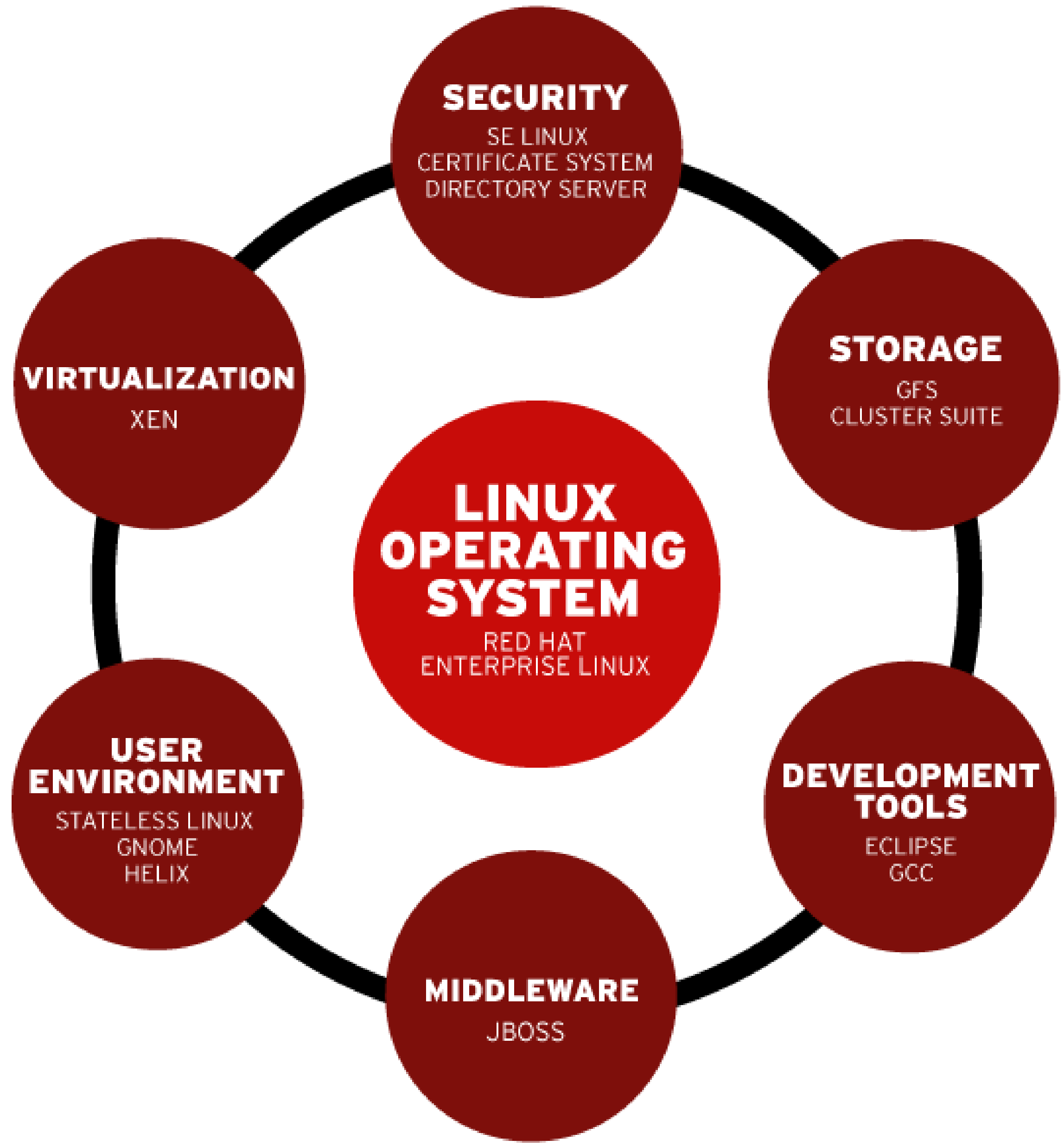
BEA WebLogic

Veritas

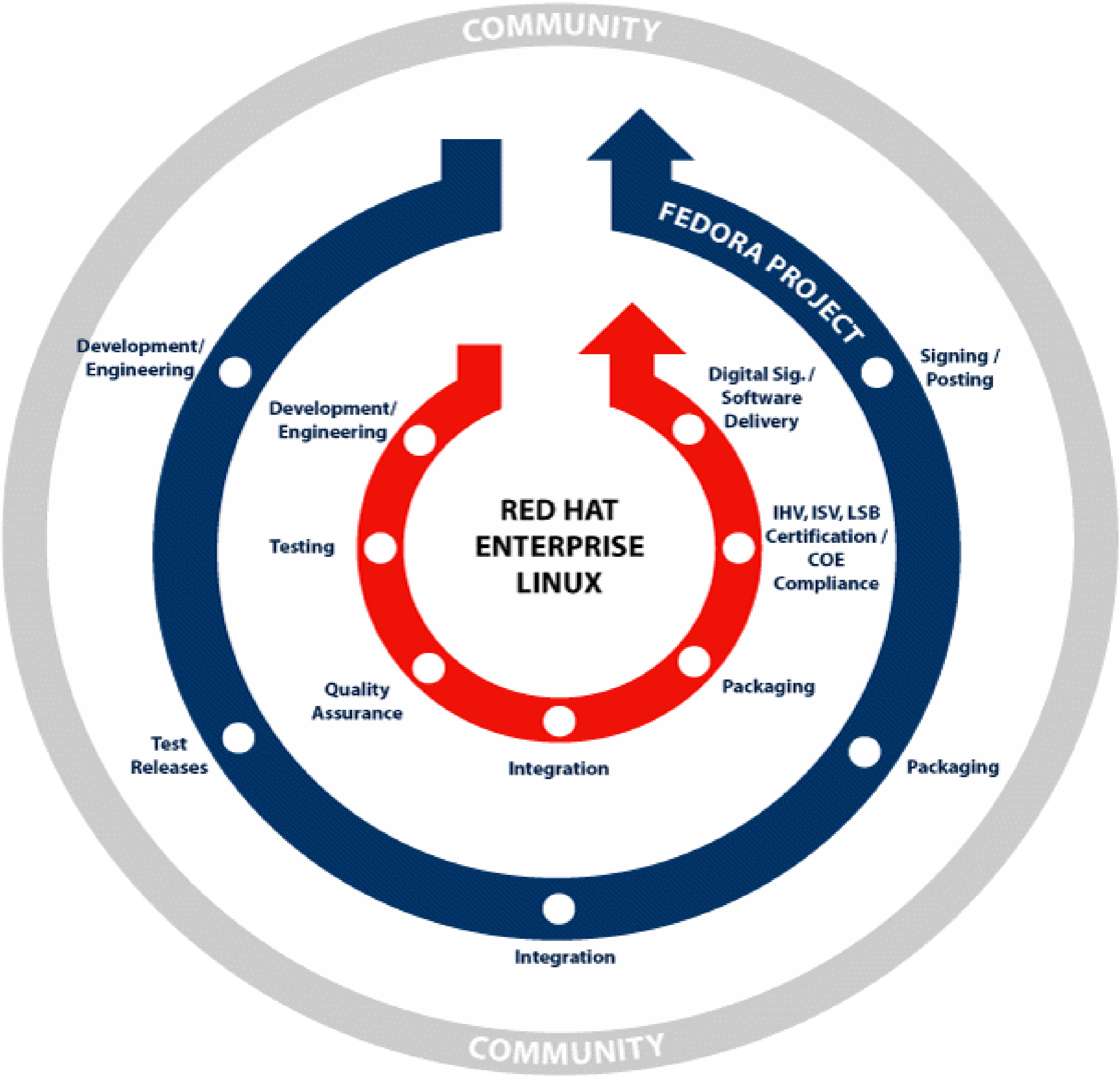
VMWare

EMC Powerpath

SUN Solaris



Red Hat Development Model



Open Source as a Security Innovation

1. More eyes on the code, therefore less security bugs

Bugs per 1000 Lines of Code

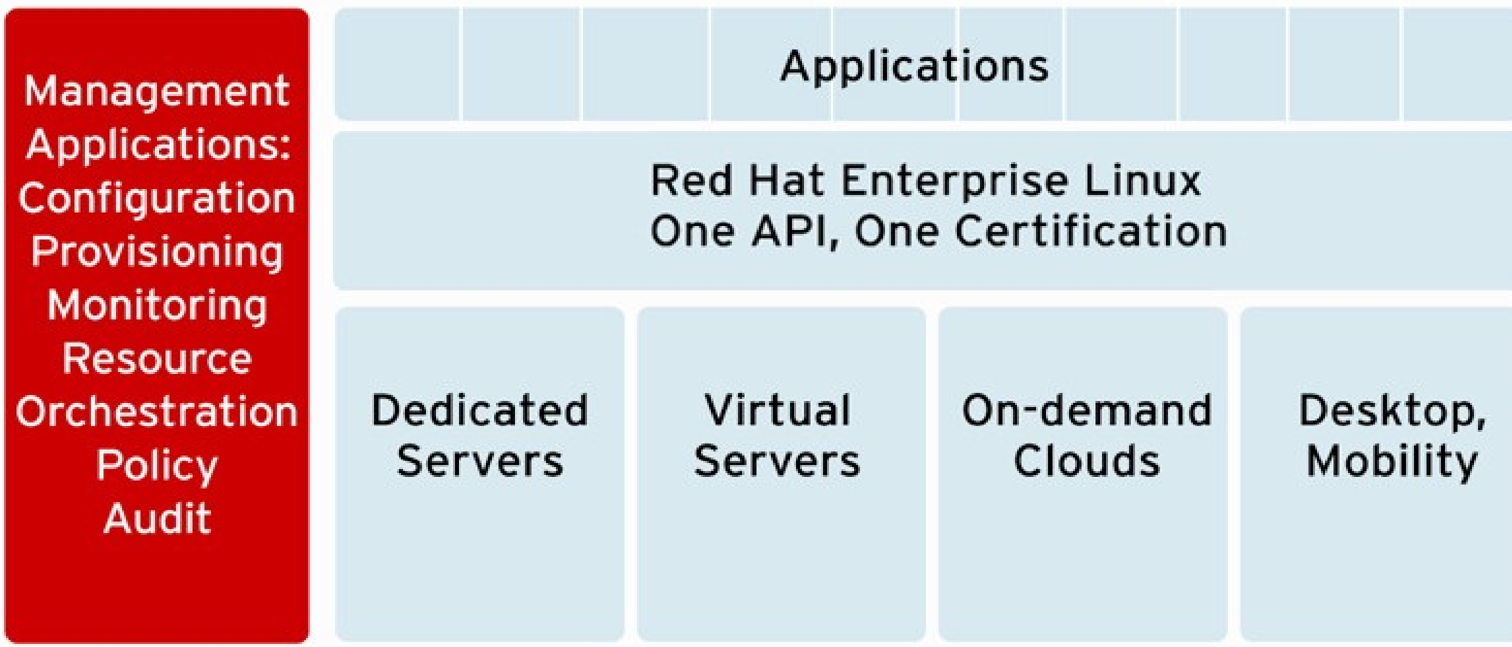
Linux 2.6 Kernel	0.17	Stanford University/Cover
Proprietary Software	10 to 20	Carnegie Mellon Cylab

Wired Magazine, Dec 2004

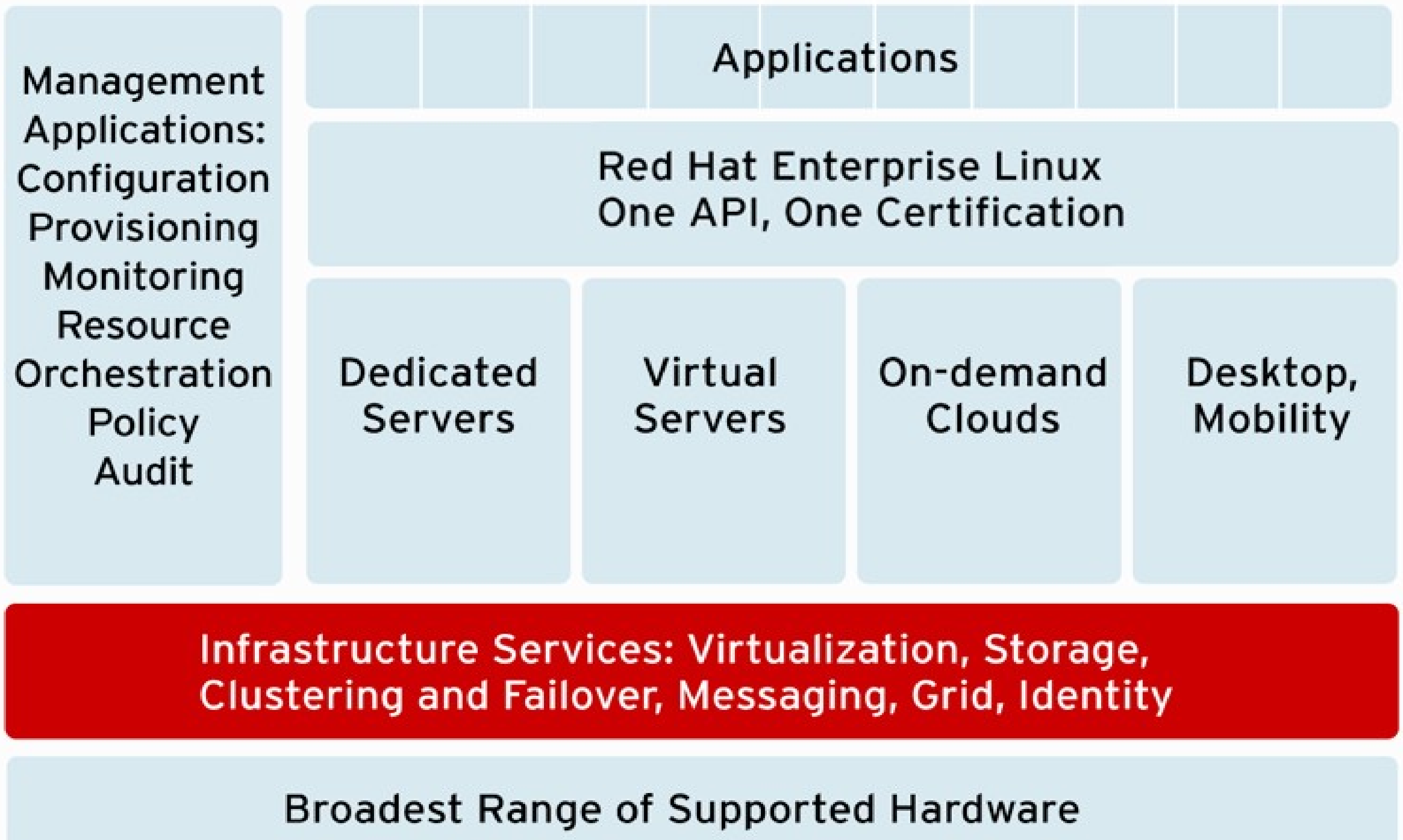
2. Red Hat's rapid response to any vulnerabilities

Time from a critical issue being known to the public until the day that a fix is available via RHN
Red Hat Enterprise Linux 4, Feb 2005-Feb 2006

CONSISTENT TOOL SET SPANS ALL DEPLOYMENT MODELS



AUTOMATION, MOBILITY, AND QUALITY OF SERVICE BUILT IN



redhat.

#1 IN VALUE. AGAIN.

CIO INSIGHT

#1 FOUR YEARS RUNNING IN ENTERPRISE SOFTWARE

#1 MEETING COMMITMENTS ON TIME AND ON BUDGET

97% said they would buy FROM RED HAT AGAIN.

#1 OVERALL IN 3 OF THE LAST 4 YEARS

#1 MEETING EXPECTATIONS FOR LOWERING COST

TOP 10 FOR ENTERPRISE SOFTWARE 2007

RANK 07	RANK 06	RANK 05	VENDOR	OVERALL 07	VALUE	RELIABILITY	WOULD CONTINUE TO DO BUSINESS (%YES)
1	1	1	RED HAT	80%	80%	80%	97%
2	2	2	Citrix Systems	76%	76%	76%	93%
3	-	-	Adobe	73%	71%	76%	91%
4	7	6	SAP	64%	66%	62%	89%
5	6	7	Microsoft	62%	62%	61%	84%
6	8	3	Business Objects	61%	60%	62%	83%
7	5	5	Novell	60%	60%	60%	70%
8	8	10	Oracle *(Including Hyperion)*	58%	57%	59%	79%
9	11	9	CA	52%	51%	54%	68%
10	10	8	Cognos	51%	50%	52%	80%

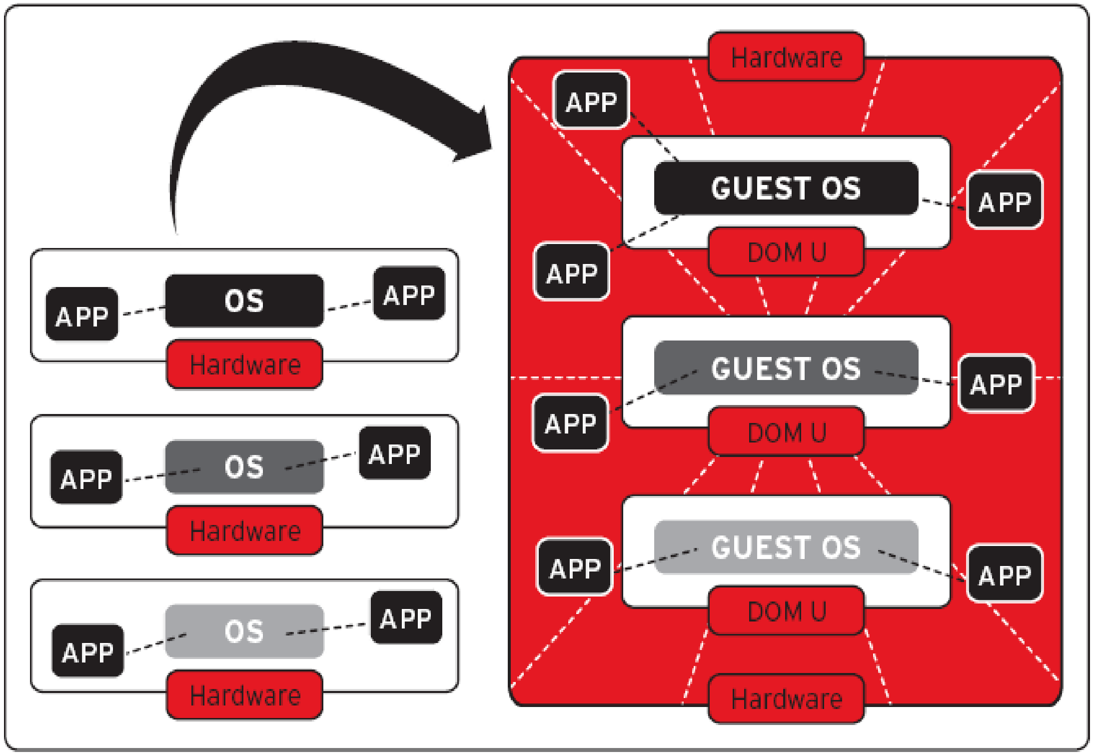
Visit http://www.redhat.com/promo/vendor for more information

Red Hat Technology Update

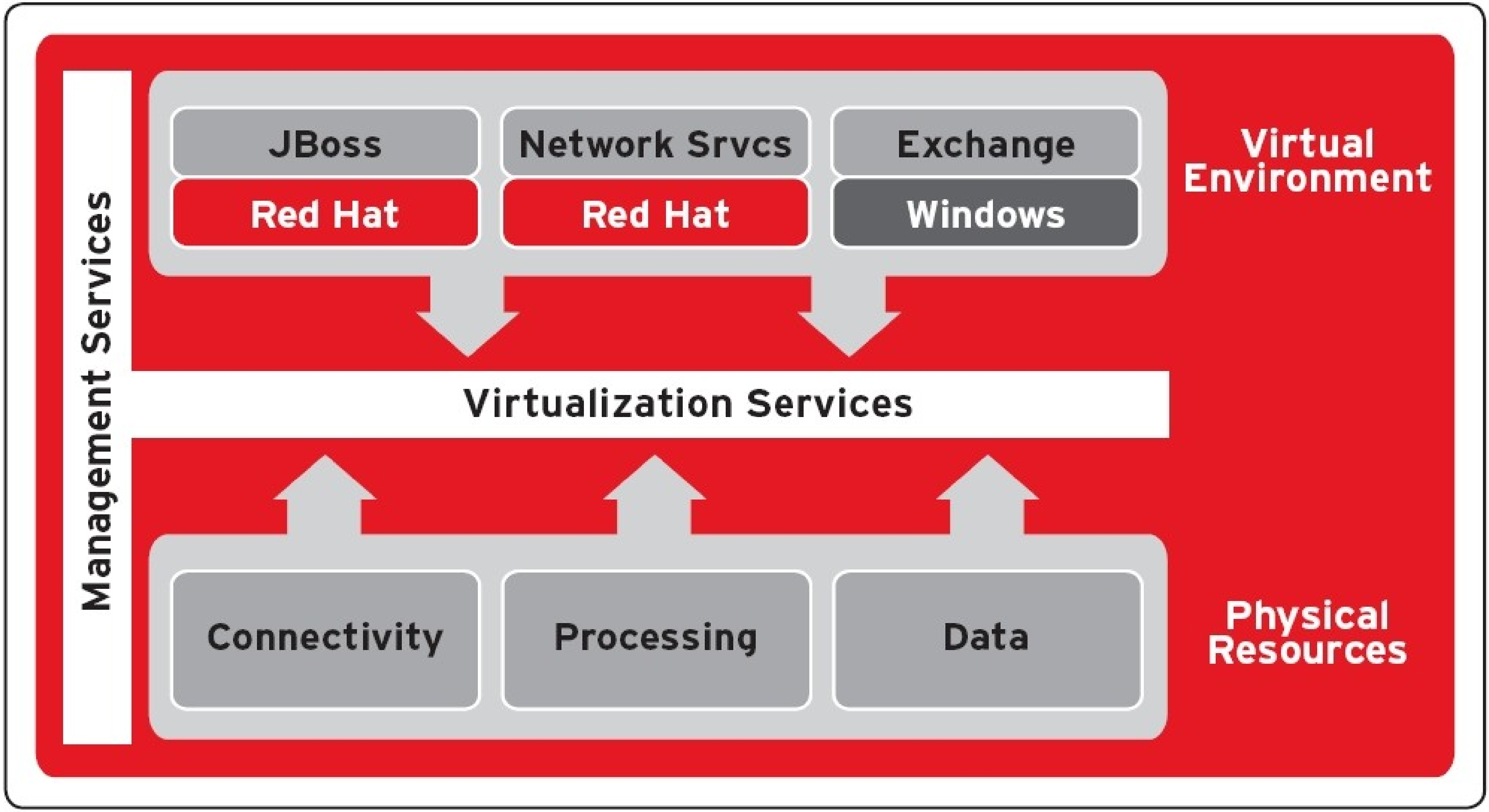
- Virtualization
- Security/MLS/Common Criteria

The Xen Hypervisor

- Flexible IT Services
- Disaster Tolerance
- Life Cycle Management
- Live Migration



Virtualization Architecture



Introduction to libvirt API

- Hypervisor agnostic
- Stable API for tool/app development
  - CIM providers; Python, C bindings, scriptable
- Allows authenticated/encrypted sessions to remote hypervisors
- Current support for
  - Xen Hypervisor
  - KVM Hypervisor
  - QEMU Hypervisor

Red Hat Security Certifications

- **NIAP/Common Criteria: The most evaluated operating system platform**
  - Red Hat Enterprise Linux 2.1 – EAL 2 (Completed: February 2004)
  - Red Hat Enterprise Linux 3 EAL 3+/CAPP (Completed: August 2004)
  - Red Hat Enterprise Linux 4 EAL 4+/CAPP (Completed: February 2006)
  - Red Hat Enterprise Linux 5 EAL4+/CAPP/LSPP/RBAC (Completed: June 2007)

- **DII-COE**
  - Red Hat Enterprise Linux 3 (Self-Certification Completed: October 2004)
  - Red Hat Enterprise Linux: First Linux platform certified by DISA

- **DCID 6/3**
  - Currently PL3/PL4: ask about kickstarts.
  - Often a component in PL5 systems

- **DISA SRRs / STIGs**
  - Ask about kickstarts.

- **FIPS 140-2**
  - Red Hat / NSS Cryptography Libraries certified Level 2

RHEL5 SELinux Enhancements

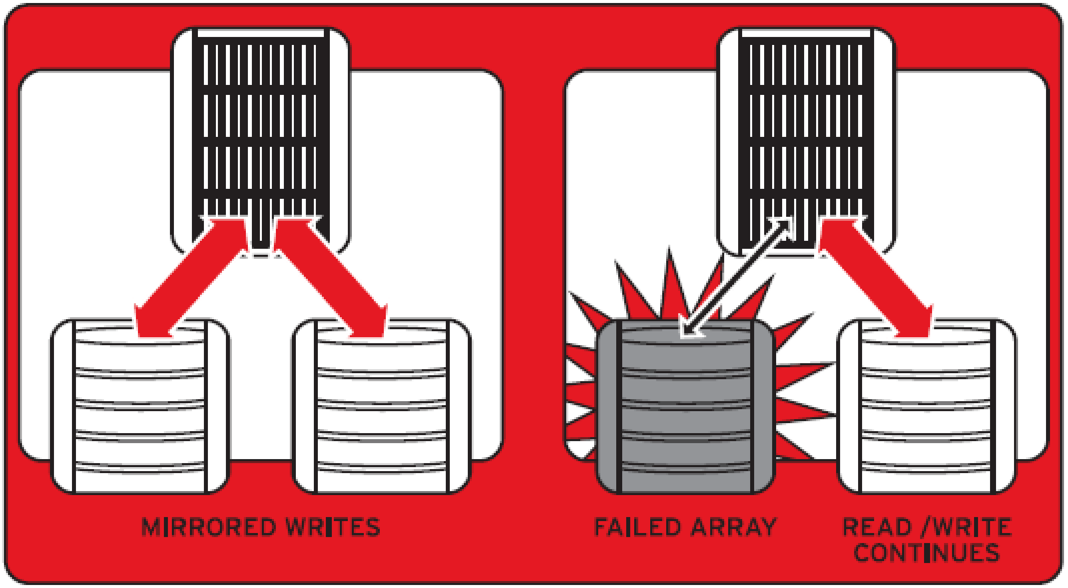
- **ExecShield**
  This enhancement can prevent any memory that was writable from becoming executable. This prevents an attacker from writing his code into memory and then executing it

- **Stack Smashing protection (Canary values)**
  The system will place a canary value at a randomized point above the stack. This canary value is verified during normal operation. If the stack has been smashed, the canary value will have been overwritten, indicating that the stack has been smashed. This is a method to detect buffer overflows early.

- **FORTIFY_SOURCE GCC option**
  When the compiler knows the size of a buffer, functions operate on the buffer to make sure it will not overflow at runtime. This works to help catch format string flaws as well as buffer overflows.

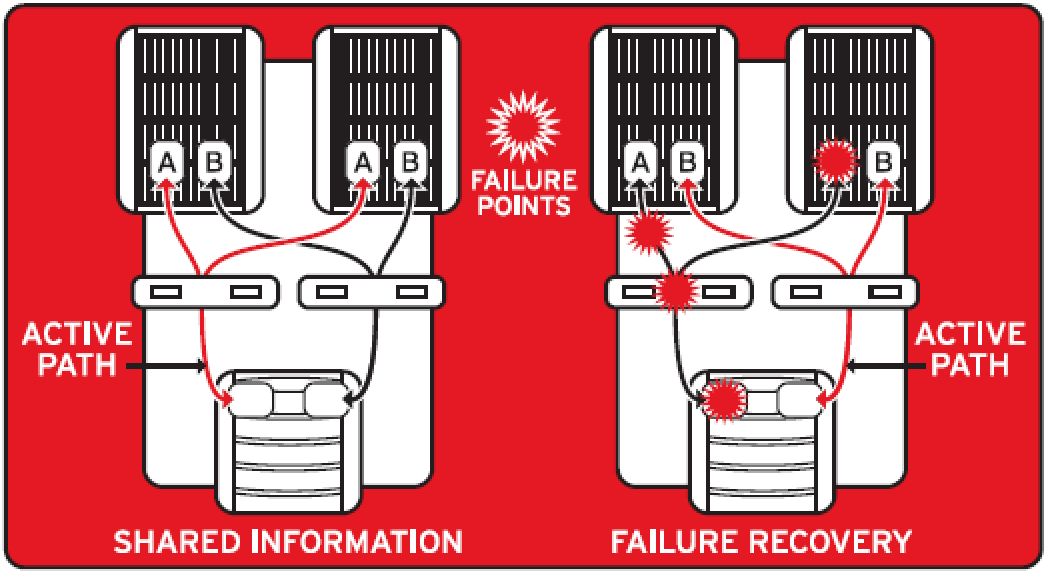
LVM Host-Based Synchronous Mirroring

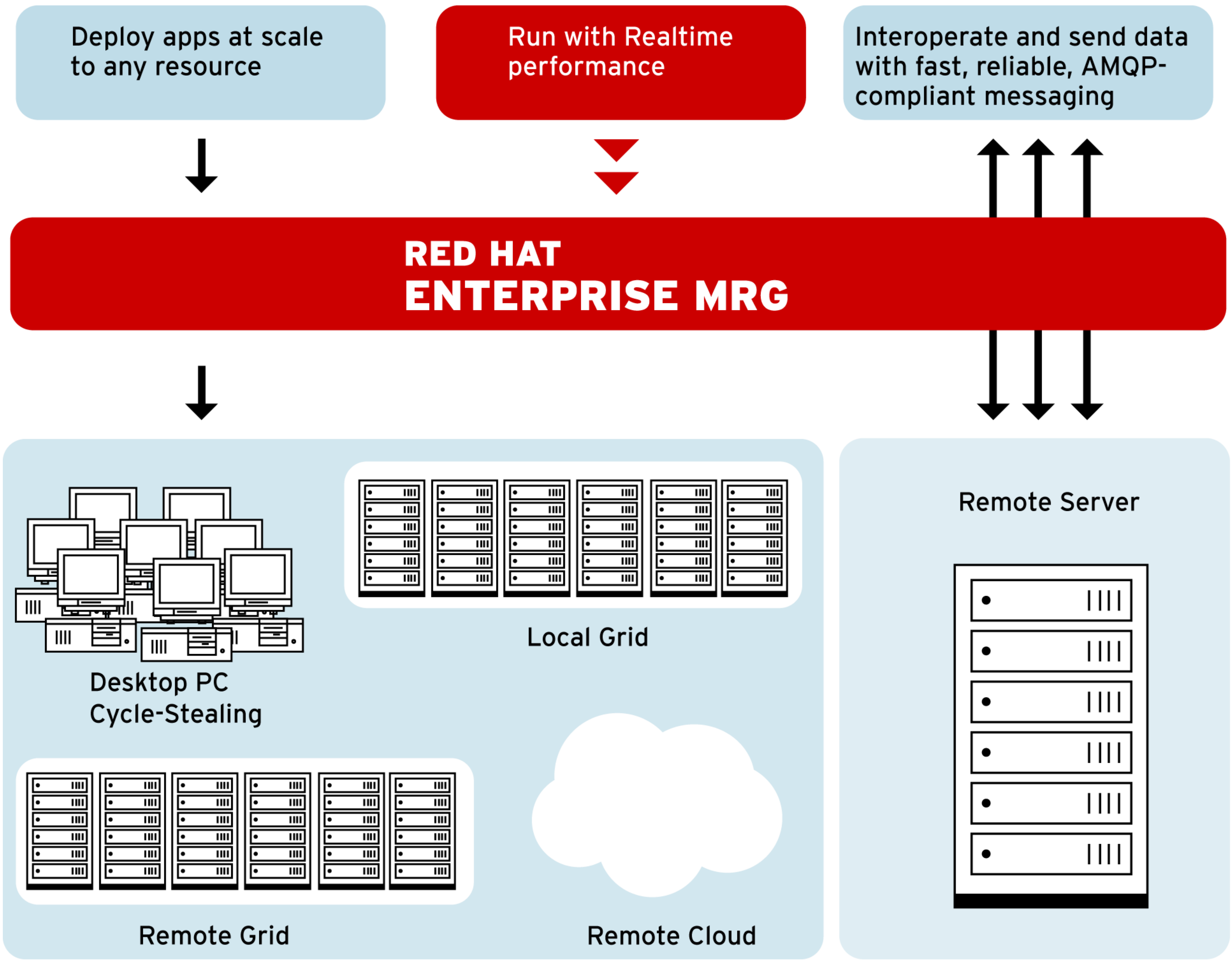
- Each write is simultaneously written to 2 or more local or SAN disks (RAID1)
- LVM automatically detects failure, uses the identical, mirrored disks or LUN
- Upon restoration, recovery process begins in background
- If minor outage, transaction log rapidly replays missed I/O



Device Mapper Multipath IO (MPIO)

- Connects & manages multiple paths through SAN to storage array
- Upon component failure, MPIO redirects traffic via redundant pathing
- Active/Active array support
- Bundled into RHEL





Deploy apps at scale to any resource
Run with Realtime performance
Interoperate and send data with fast, reliable, AMQP-compliant messaging
RED HAT
ENTERPRISE MRG
Desktop PC Cycle-Stealing
Local Grid
Remote Server
Remote Grid
Remote Cloud

MRG Realtime

- **Determinism**
  Ability to schedule high priority tasks predictably and consistently
- **Priority**
  Ensure that highest priority applications are not blocked by low priority
- **Quality Of Service** (QoS)
  Trustworthy, consistent response times
- **Proven results**
  - Average of 38% improvement over stock RHEL5
  - Timer event precision enhanced to µs level, rather than ms

MRG: Messaging

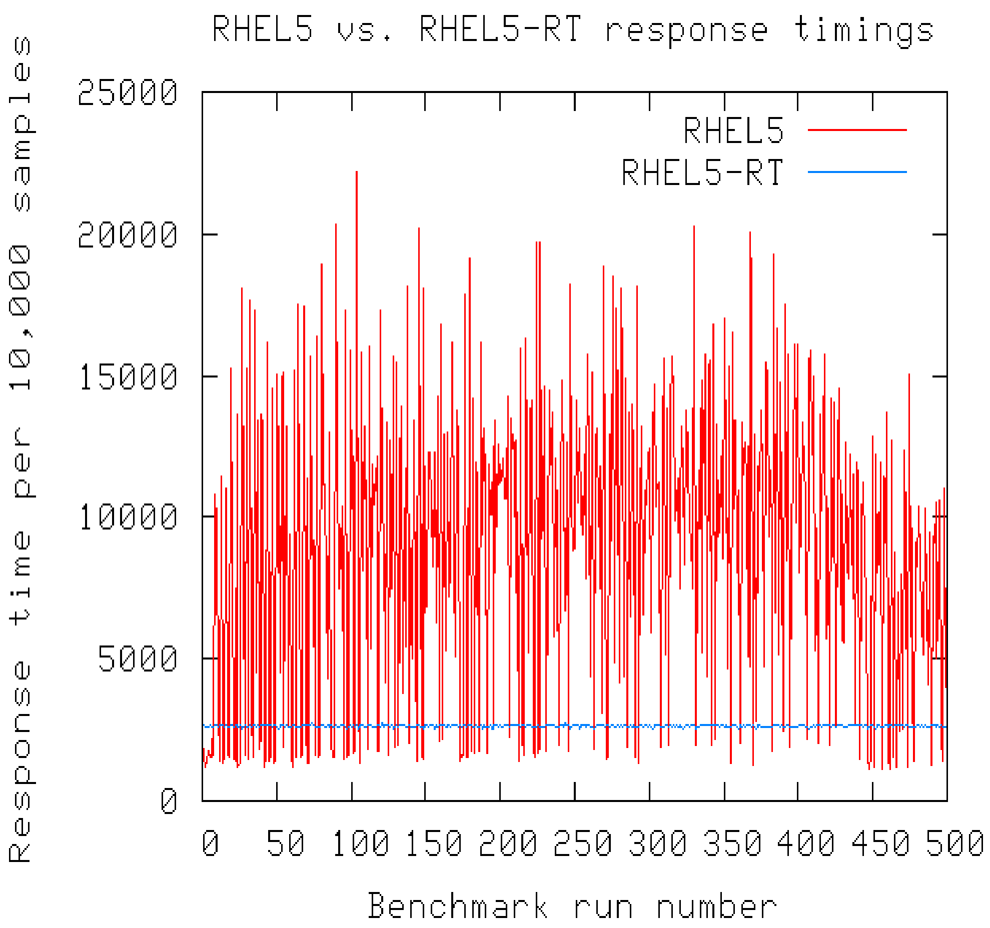
- Provides messaging that is up to 100-fold faster than before
- Spans fast messaging, reliable messaging, large-file messaging
- Implements AMQP, the industry's first open messaging standard, for unprecedented interoperability that is cross-language, cross-platform, multi-vendor, spans hardware and software, and extends down to the wire level
- Uses Linux-specific optimizations to achieve optimal performance on Red Hat Enterprise Linux and MRG Realtime
  - Takes advantage of RHEL clustering, IO, kernel, and more
  - Includes new high-performance AIO Journal for durable messaging
  - Provides native infiniband support for transient messaging

About AMQP

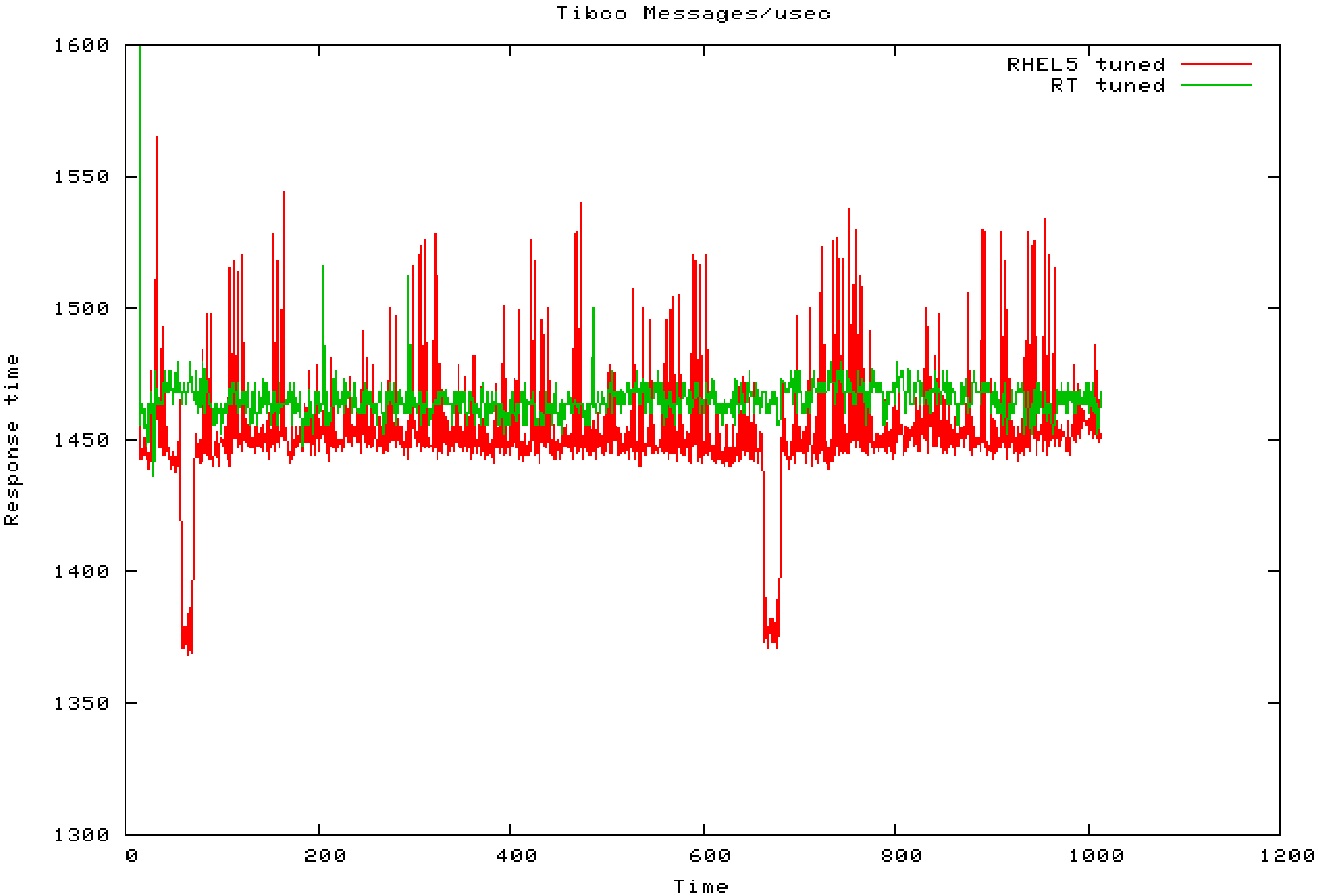
- AMQP is an open specification for messaging
  - It is a complete specification
  - Anyone may use the AMQP specification to create useful implementations without being charged for the IP rights to do so
- AMQP aims to be technology and language-neutral
  - Available in C, C++, Java, JMS, .NET, C#, Ruby, Python, etc.
  - Requires IP, and can be used with TCP, UDP, SCTP, Infiniband, etc.
- Products complying with AMQP are inter-operable
  - AMQP is a Wire-Level protocol based on the ubiquitous IP
  - Wire-level compatibility means it can be embedded in the network
  - Applications written to Product X will plug into servers running Product Y
- Red Hat is a founding member of the AMQP Working Group

MRG: Realtime

- Enables applications and transactions to run predictably, with guaranteed response times
  - Provides microsecond accuracy
- Provides competitive advantage & meets SLA's
  - Travel web site: missed booking
  - Program trading: missed trades
  - Command & Control: life & death
- Provides replacement kernel for RHEL 5.1+; x86/x86_64
- Preserves RHEL Application Compatibility



Detail zoom-in of RHEL5 vs MRG Realtime



MRG: Realtime Tools

- **MRG includes a new MRG Realtime Latency Tracer**
  - Runtime trace capture of longest latency codepaths – both kernel and application. Peak detector
  - Selectable triggers for threshold tracing
  - Detailed kernel profiles based on latency triggers
- **Existing standard RHEL5 based performance monitoring tools remain relevant**
  - Gdb, OProfile Frysk – source level debuggers & profiler
  - SystemTap, kprobe – kernel event tracing and dynamic data collection
  - kexec/kdump standard kernel dump/save core capabilities

Red Hat Enterprise MRG Availability

- MRG Announcement & Beta Launch: December 2007
  - Public beta
- MRG v1.0: Early 2008
  - RHEL-only support for MRG Messaging broker
  - MRG Grid Technology Preview
- MRG v1.1: Late 2008
  - Multi-platform support for MRG Messaging Java-based broker
  - AMQP support updated to newly available AMQP version (1.0)
  - MRG Grid support available

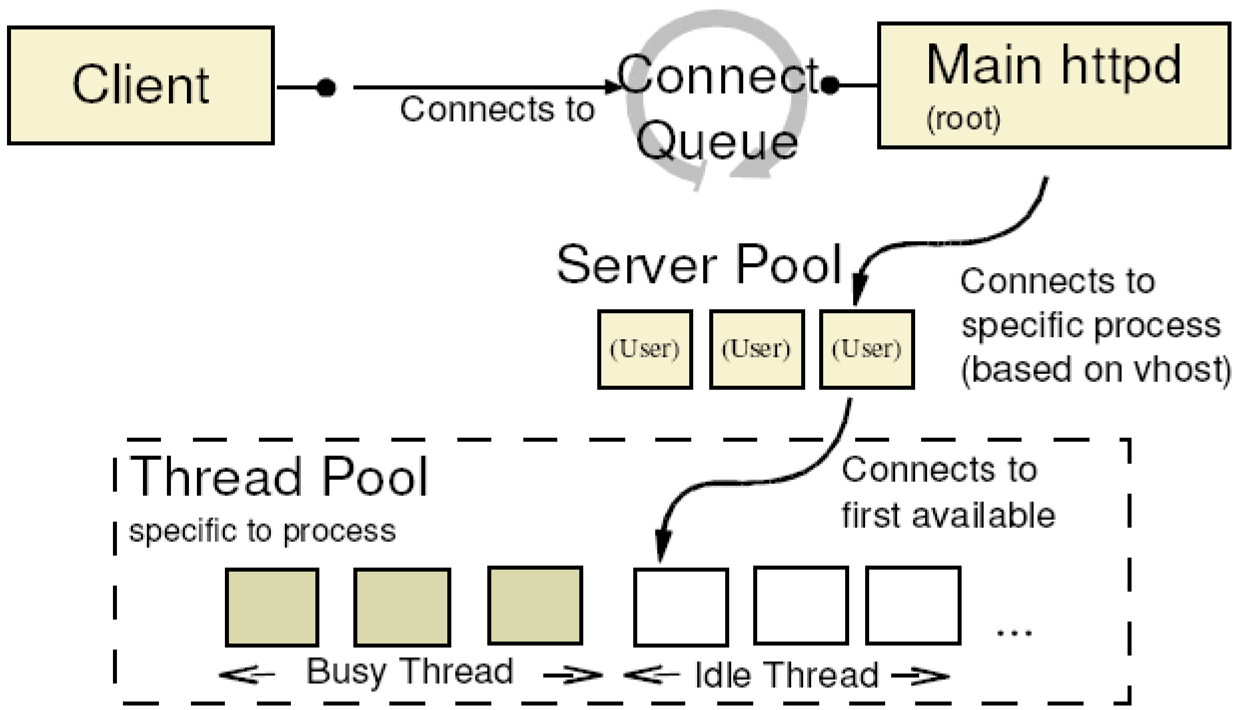
http://www.redhat.com/mrg/

MRG: Grid based off Condor

- MRG Grid is based on the Condor Project created and hosted by the University of Wisconsin, Madison
- Red Hat and the University of Wisconsin have signed a strategic partnership around Condor:
  - University of Wisconsin makes Condor source code available under OSI-approved open source license
  - Red Hat & University of Wisconsin jointly fund and staff Condor development on-campus at the University of Wisconsin
- Red Hat and the University of Wisconsin's partnership will:
  - Add enhanced enterprise features, management, and supportability to Condor and MRG Grid
  - Add High Throughput Computing capabilities to Linux

Apache Security

Worker Thread



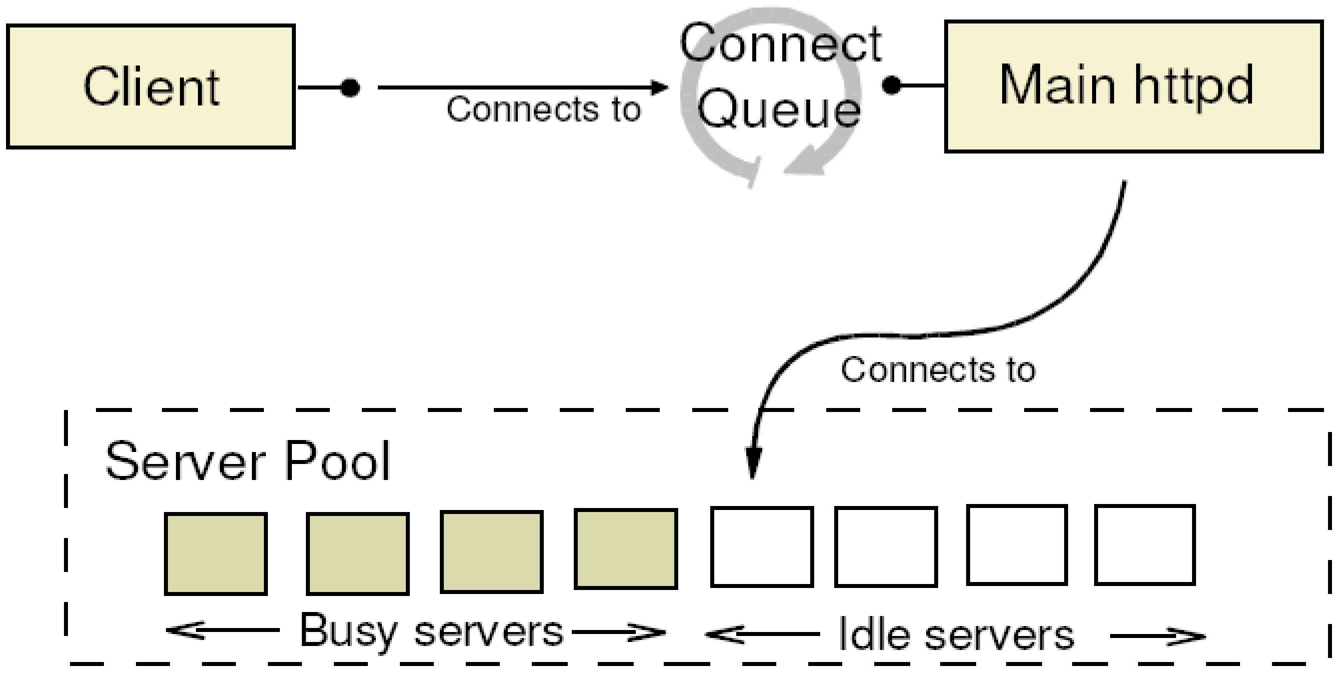
Config Example:

    ServerLimit 2
    StartServers 2
    ThreadsPerChild 3
    MinSpareThreads 2
    MaxSpareThreads 4
    MaxClients 6

- Large number of requests

- Less system resources

Prefork Threading



- Need to avoid threading (legacy)

- Problem with request will not effect others

suEXEC

- **Problem**

  When running virtual hosts all files executed as same user

- **Vulnerability**

  Malicious user may inject code into Apache to see other files on the system

- **Solution**

  Utilize suEXEC, allowing virtual hosts to be ran as alternate users

Using suEXEC

- **SuexecUserGroup**

  Sets executing process to run as alternate user

<VirtualHost www.example.com>

DocumentRoot /var/www/example.com

ServerName www.example.com

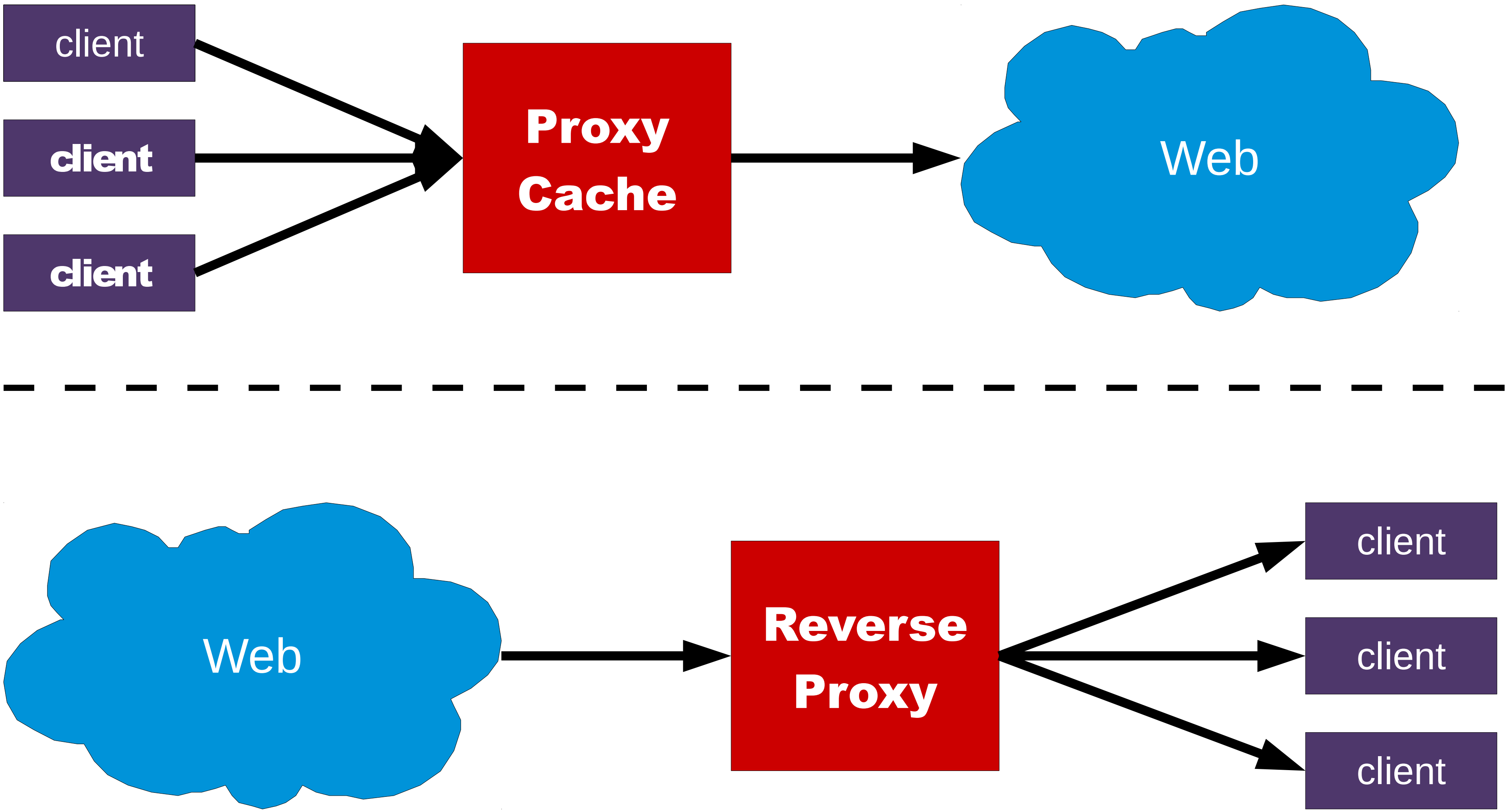
......

SuexecUserGroup *{web_user}* *{web_group}*

......

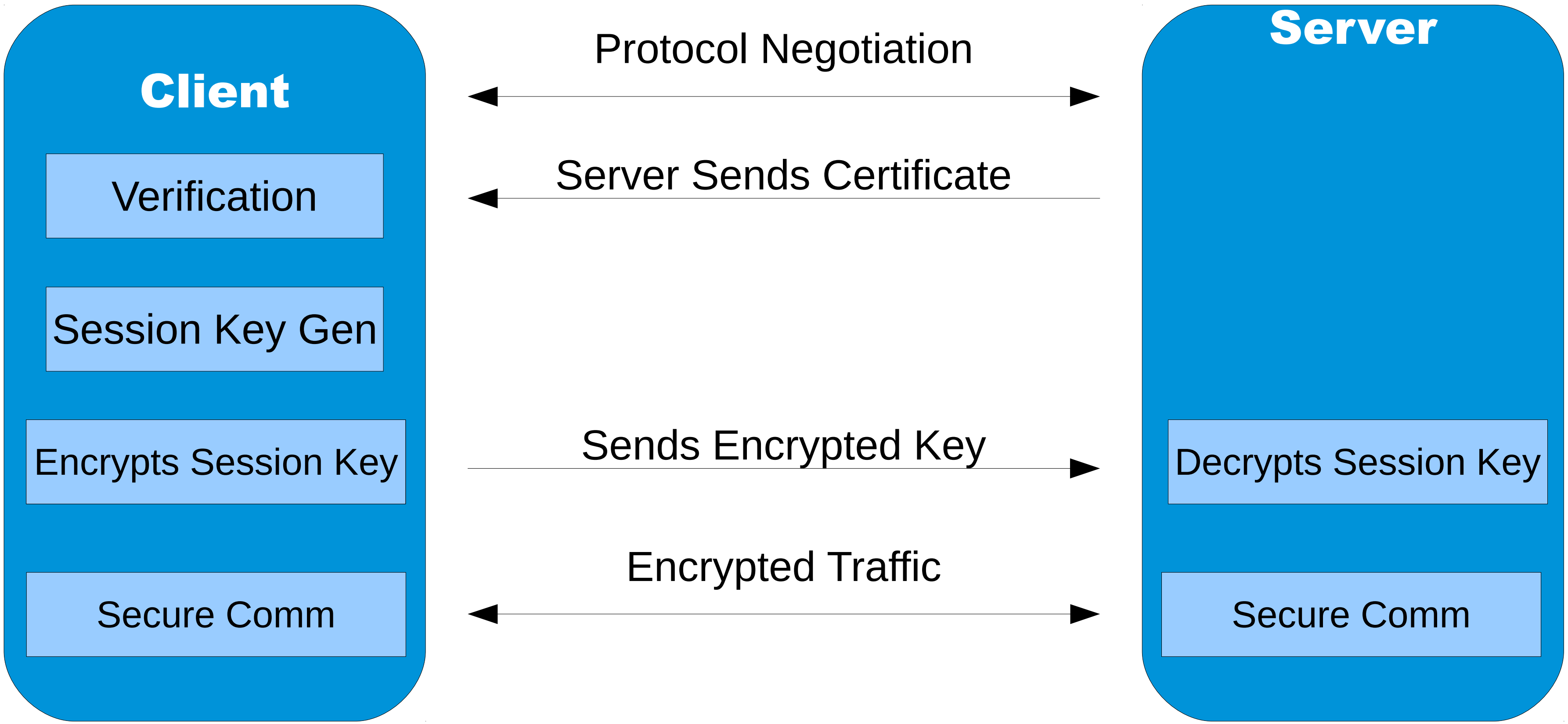
</VirtualHost>

mod_proxy


client
client
client
Proxy
Cache
Web
Web
Reverse
Proxy
client
client
client

mod_ssl

- Supports SSLv2, SSLv3, TLSv1
- Supports RSA ciphers
- 128-bit strong encryption, world wide



Open Discussion