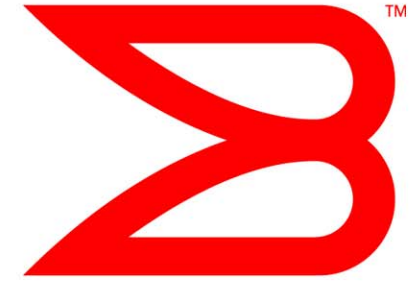


BROCADE



Accelerate Into the Future with Application Delivery

NGDC San Francisco August 2009

Gary Hemminger

Director, Product Mgmt, ADC Products

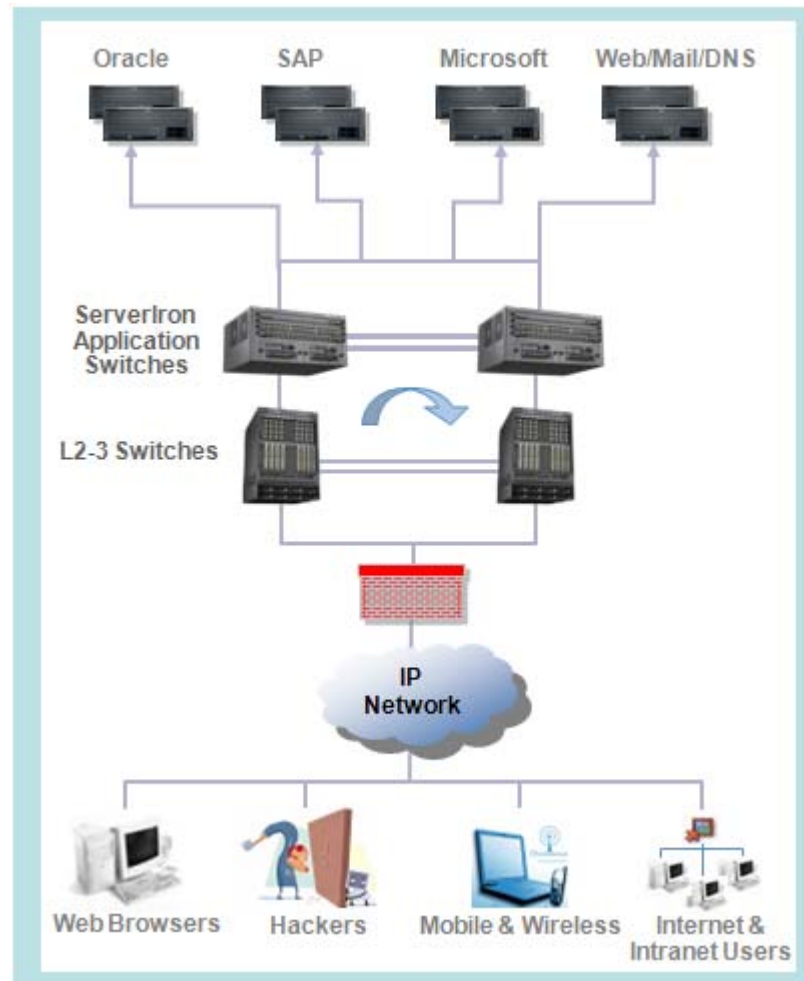
Accelerate Into the Future with Application Delivery

- Current ADC Features & Solutions
- Enterprise vs. SP Space & Requirements
- Dynamic Application to Network Interface
- Virtualizing the ADC for Application Zoning
- Repositioning the Virtualized ADC
- Policy Based Access Mgmt Support
- Scaling the ADC for 10Gig Server Connectivity
- Two Tier ADC Solutions for the Virtualized World

Application Delivery Controllers

Traditional ADC Features

- Advanced L4 load balancing & L7 content switching & rewrite
- Comprehensive Enterprise application support
- Integrated SSL acceleration
- Web performance optimization with http/TCP offload
- Full IPv4 and IPv6 switching, routing & SLB (VIP) support
- Firewall, Cache, and IDS load balancing



- Multiple high availability modes for maximum flexibility
- Advanced Security Functions (App Firewall, DoS Protection, Syn-Cookie)
- Integrated global load balancing for multi-site redundancy and scalability
- Data center class architecture and modularity for investment protection
- GUI & CLI for system and application administrators

Enterprise vs. SP ADC Requirements

Enterprise Requirements

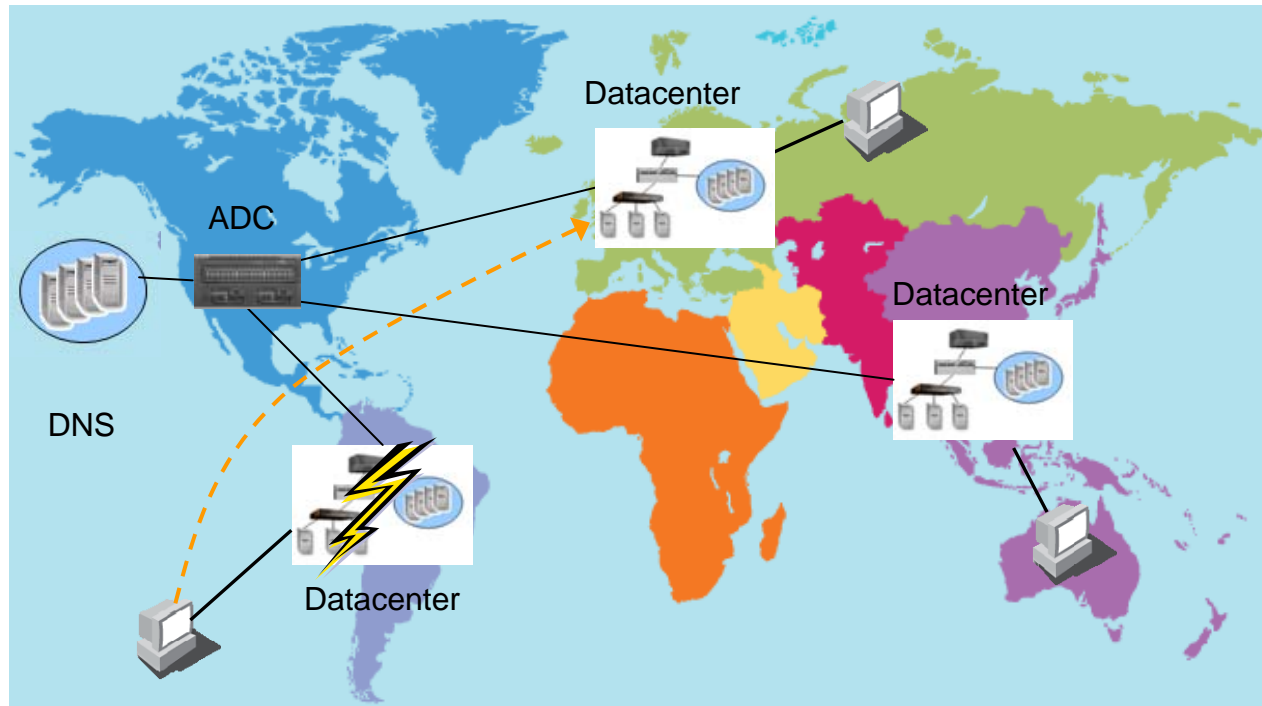
- Content Switching & Transformation
- SSL acceleration
- Server side compression
- FWLB, TCS, GSLB
- Server to ADC programmatic interface (SNMP, XML)
- L7 Scripting Capabilities
- Support for Oracle, Microsoft, SAP, and other high profile applications

SP Space & Requirements

- Telco, Software as a Service, CDN, Streaming media, IP Telephony (SIP), Wireless carriers, TLD Providers, Hosting Providers
- Very scalable, high speed L4-7 transaction rates or bulk throughput
- Server to ADC programmatic interface
- Mainly web & Infrastructure apps (DNS)
- DoS attack protection

Global Server Load Balancing

Global Datacenter Support



Global Data Center Deployment Problems

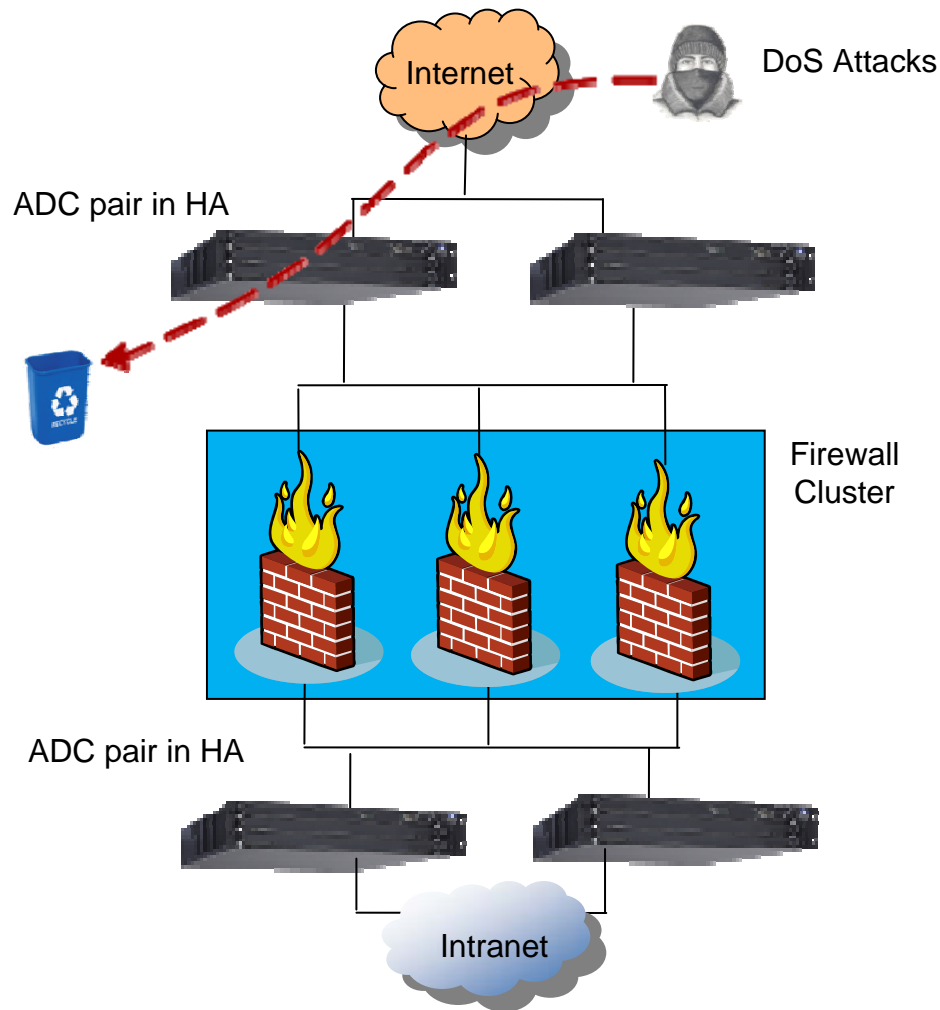
- Handling site failures transparently
- Providing best site selection per user
- Leveraging both DNS and non-DNS solutions for multisite redundancy
- Providing disaster recovery and non-stop operation

GSLB Solution

- GSLB controller works with local ADC to load-balance global data center traffic
- Incorporates site health, load, user proximity, and service response for user site selection
- Provides transparent site failover in case of disaster or service outage
- Supports route health injection using RIP/OSPF/BGP when DNS cannot easily be employed

Firewall Load Balancing

Scaling Firewalls and Providing DoS Attack Protection



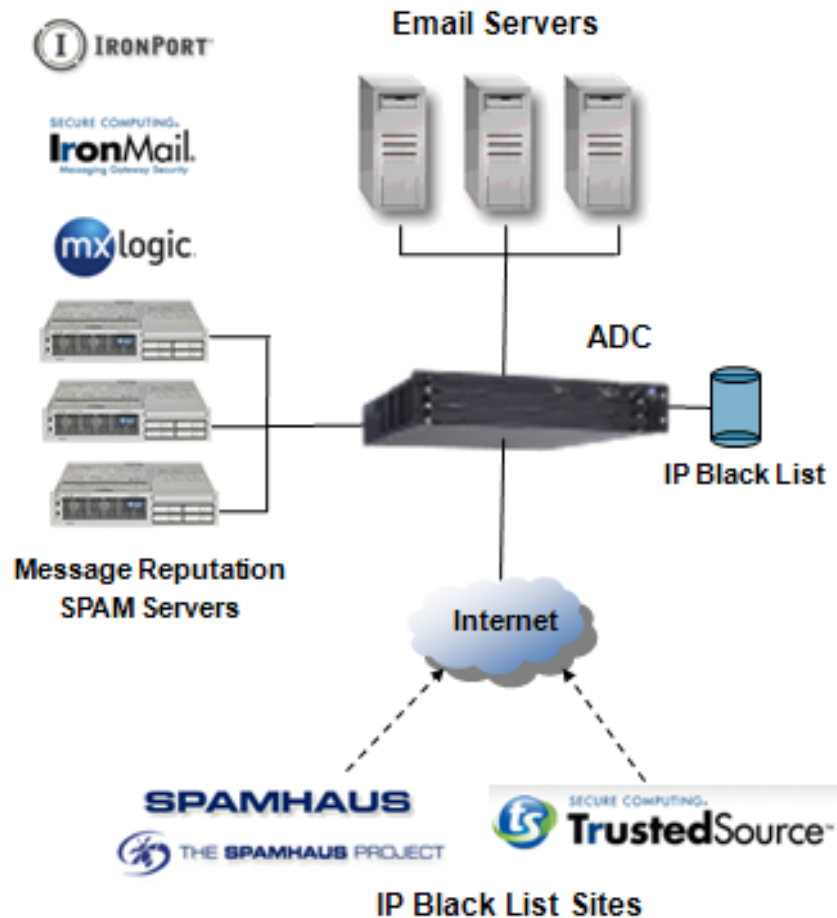
Firewall Operational Issues

- Scaling firewall bandwidth without replacing existing firewalls
- Firewalls can be “melted down” by L2-3 DoS attacks
- Firewall service needs to be 24x7 to ensure communications

FWLB Solution

- FWLB transparently supports firewall clusters
- Provides high-speed DoS protection to prevent firewall meltdown
- Can offload NAT processing from firewalls
- Ensures that firewalls can be scaled inexpensively and securely, with maximum performance
- Must support CheckPoint, Cisco, Juniper, Secure Computing, and other clustered firewall devices

Providing SPAM Mitigation & Load Balancing Service for Message Reputation & Email Servers



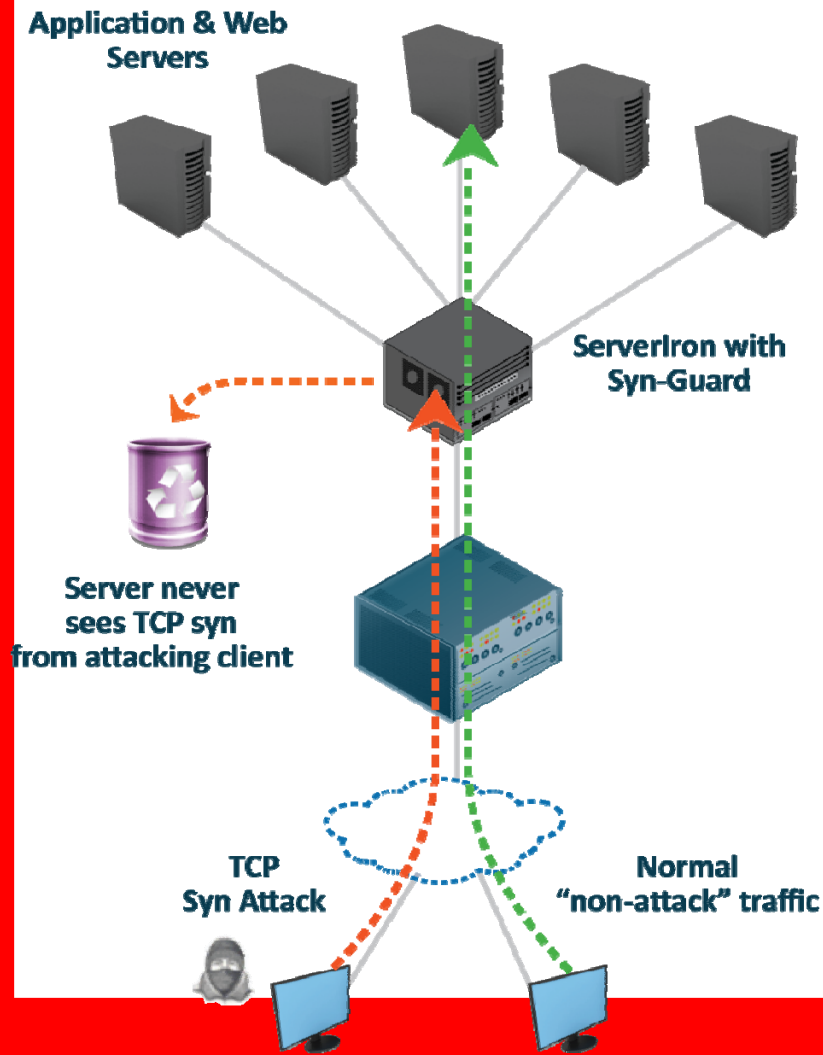
Delivering Efficient and Effective SPAM Mitigation

- Message Reputation Service is costly and difficult to scale
- Multiple servers are often needed to deal with the high volume of email and SPAM
- Some mechanism to quickly discard known SPAM from even getting to complex reputation servers should be provide

IP Black List Support

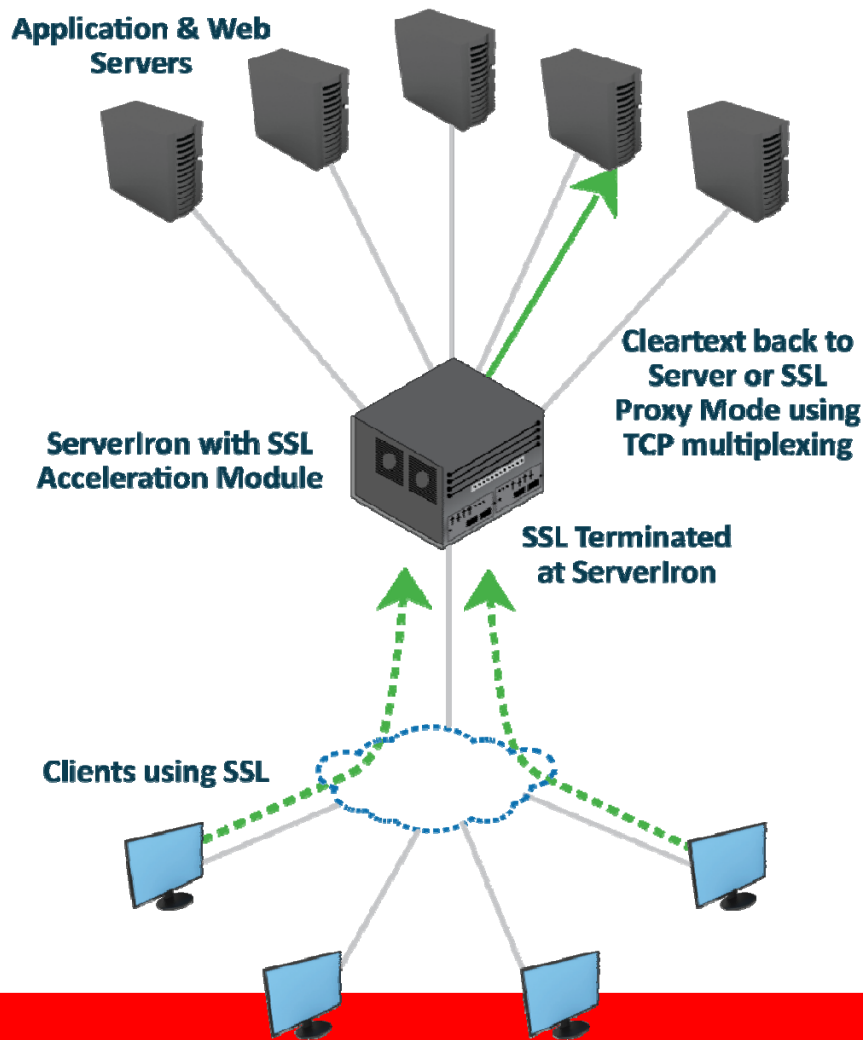
- Import IP Black Lists from a number of trusted sites
- IP Black List support eliminates up to 30% of SPAM
- This allows reputation servers to focus on more complex SPAM mitigation

Hardware Based DoS Attack Protection



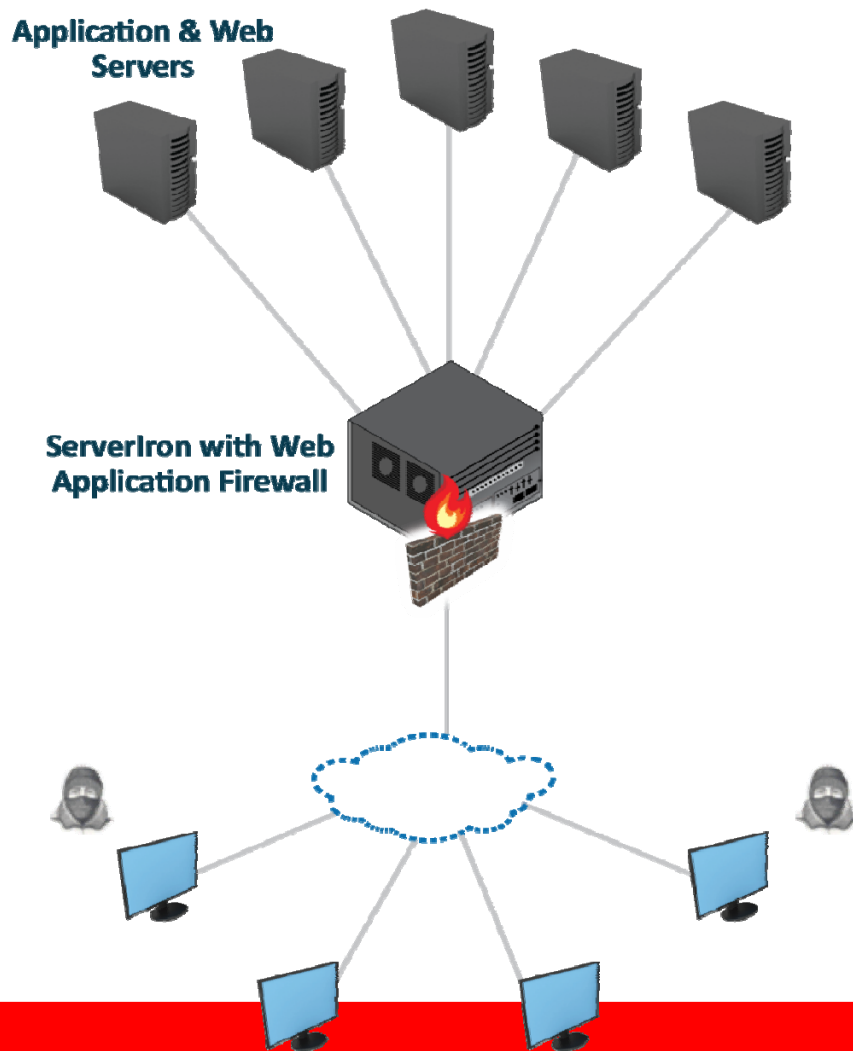
- TCP syn packet seen by ADC, which sends TCP syn ack back to client (with special sequence number)
- If no corresponding client ack seen, SI simply drops the original connection request.
- If client ack seen for original connection request, connection is then made to appropriate server
- Hardware based implementation guarantees high-speed with no CPU overhead
- Prevents Server Session Table meltdown when under attack
- Must be used in non-DSR mode
- Includes DDoS signature protection

Advanced SSL Acceleration and Offload



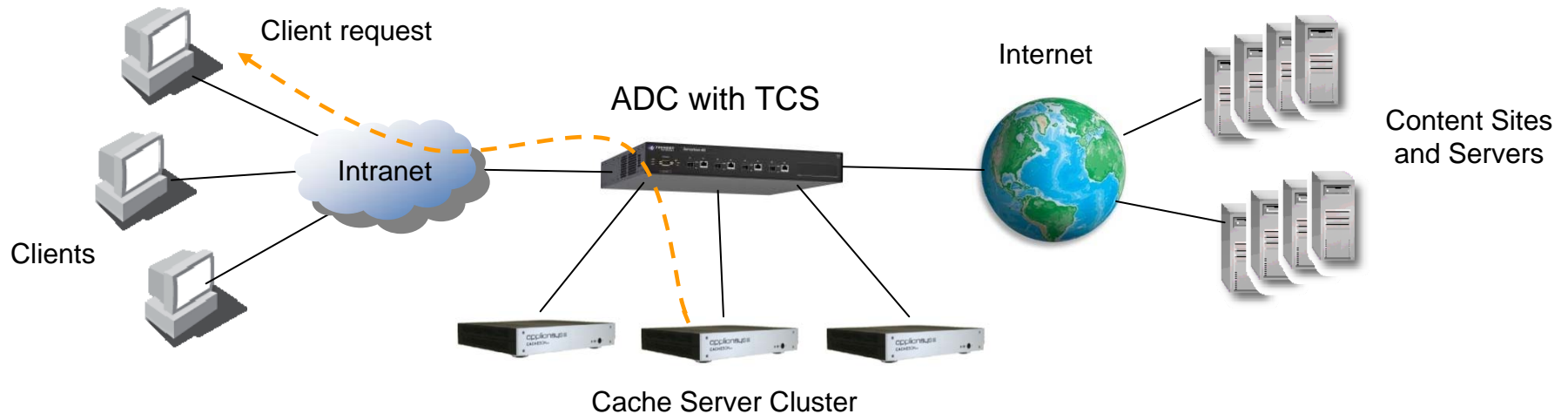
- Offloads SSL processing from Servers and speeds application responsiveness
- SSL is terminated on the ADC, and client traffic is delivered to server via a single TCP connection
 - Server no longer must process SSL, and TCP connection management is reduced
- Two modes usually provided
 - SSL terminate mode – cleartext back to server
 - SSL proxy mode – traffic is re-encrypted back to server
- Support for multiple ciphers allows added flexibility
- Performance measured in transactions per second and in bulk throughput

Enhanced Application Security with Web Application Firewall



- ⚙️ **Advanced, high-speed Web Application Firewall**
- ⚙️ **Allow /Deny/Log incoming HTTP requests based on configurable security policies**
- ⚙️ **Hides back-end application specific error information that could be used to launch additional attacks**
- ⚙️ **Prevents a range of web application attacks, including:**
 - Cookie & Parameter Tampering
 - Cross-Site Scripting
 - Buffer Overflows
 - Internal web page access
- ⚙️ **Allows cloaking to be used to replace 4xx/5xx error responses with configured responses**

Transparent Cache Switching Service



Load Balancing Cache Servers

- Cache Server is different paradigm than normal server
- Client request must be diverted from real server to cache server
- In case all cache servers down, client request must go to real server
- Scaling to multiple cache servers is not transparent to clients

Transparent Cache Switching (TCS)

- Client requests are diverted to cache servers for content
- Client requests are load balanced among cache servers
- TCS supports HTTP, FTP, and other protocols
- Client requests go directly to real servers if cache does not contain desired data
- **Bluecoat is the caching leader**

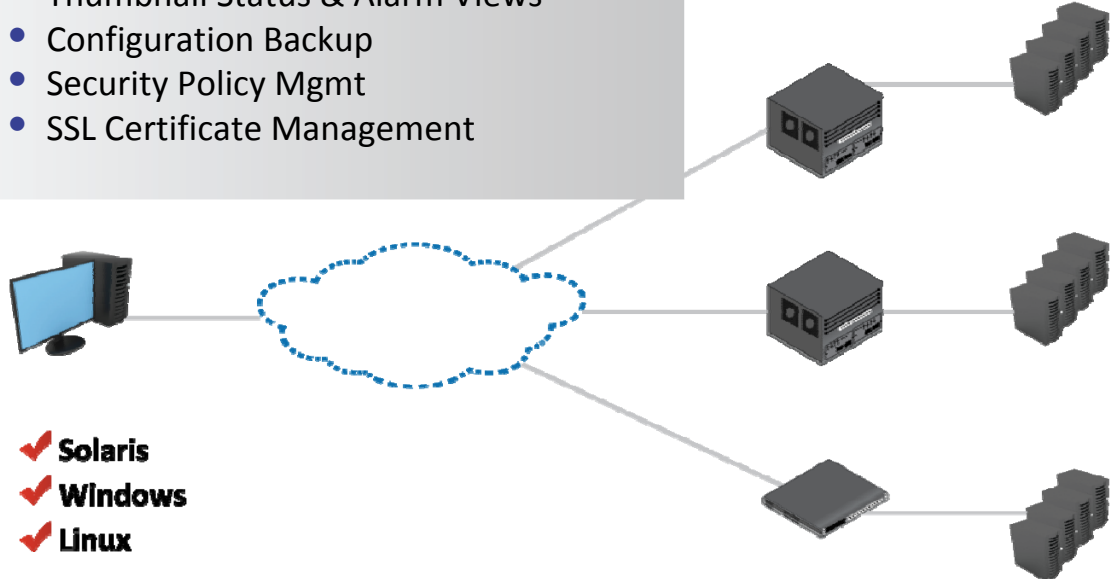
System Level Network Mgmt for ADC's

IronView Network Manager

- Security Policies
- Reports
- Events & Alarms
- Network Remediation
- Wireless Domain Management
- Configuration Management

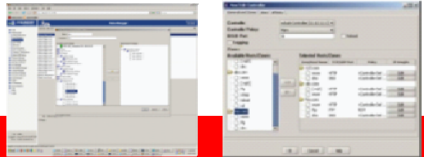
ADC System Mgmt Requirements

- Discovery & Topology Mgmt
- Configuration & Image Deployment
- Thumbnail Status & Alarm Views
- Configuration Backup
- Security Policy Mgmt
- SSL Certificate Management



- ✓ Solaris
- ✓ Windows
- ✓ Linux

GUI Based VIP & GSLB Manager



ADC's



Dynamic Application to Network Interface

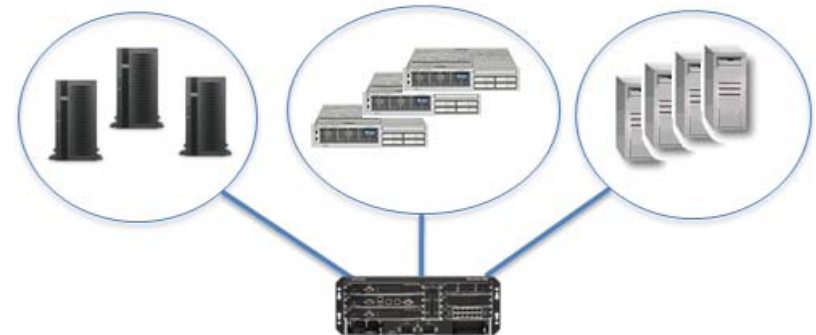
- Many application vendors now defining detailed API's (SAP, VMware, MS, Oracle) for switch/router/ADC interface
- May use XML API or SNMP for interface
- Information may include: Servers & Service Ports, Relative Capacity, State of Service, Location of Service, Group name/IP address of service
- Advantage is that ADC can interact with application to dynamically update application delivery state
- Disadvantage is that every application has its own interface specification
- Need some kind of standardization for this capability

Virtualizing the ADC for Application Zoning

- Today IT and Net Managers deploy a new pair of ADC's per application
- Problem is many ADC's underutilized (similar to today's app servers)
- Solution - Turn one ADC into multiple ADCs by virtualizing the ADC
- Advantage is a single ADC can be made to support multiple pools of application servers
- The main problem is how do you make sure each virtual instance doesn't hog the system resources?
- Hardware vs. Software Virtualization



Before - ADC's deployed per App Group



After - ADC's deployed to support multiple Apps

Virtualizing the ADC

Software Virtualization

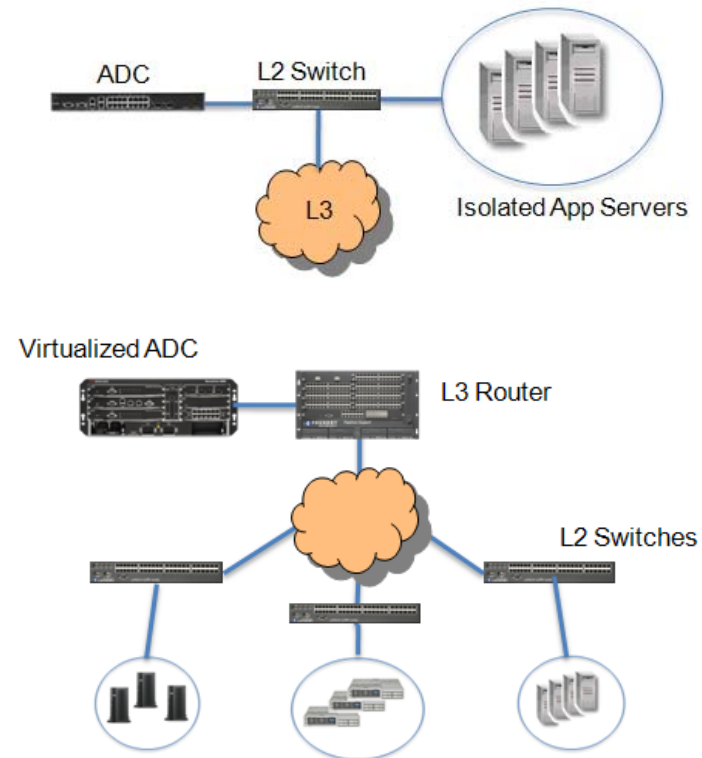
- ADC is virtualized in software
- Each virtual ADC needs to be resource constrained to prevent resource hogging
- Might use VMware & vCenter/vSphere to manage virtual ADC instances
- Software overhead may be costly for high priced ADC's

Hardware Virtualization

- ADC is virtualized on a per core basis
- Multiple core trunks provide enhanced performance & scalability
- Little to no software overhead and cores are already constrained to specified resource levels
- Difficulty is scaling to 100's of cores

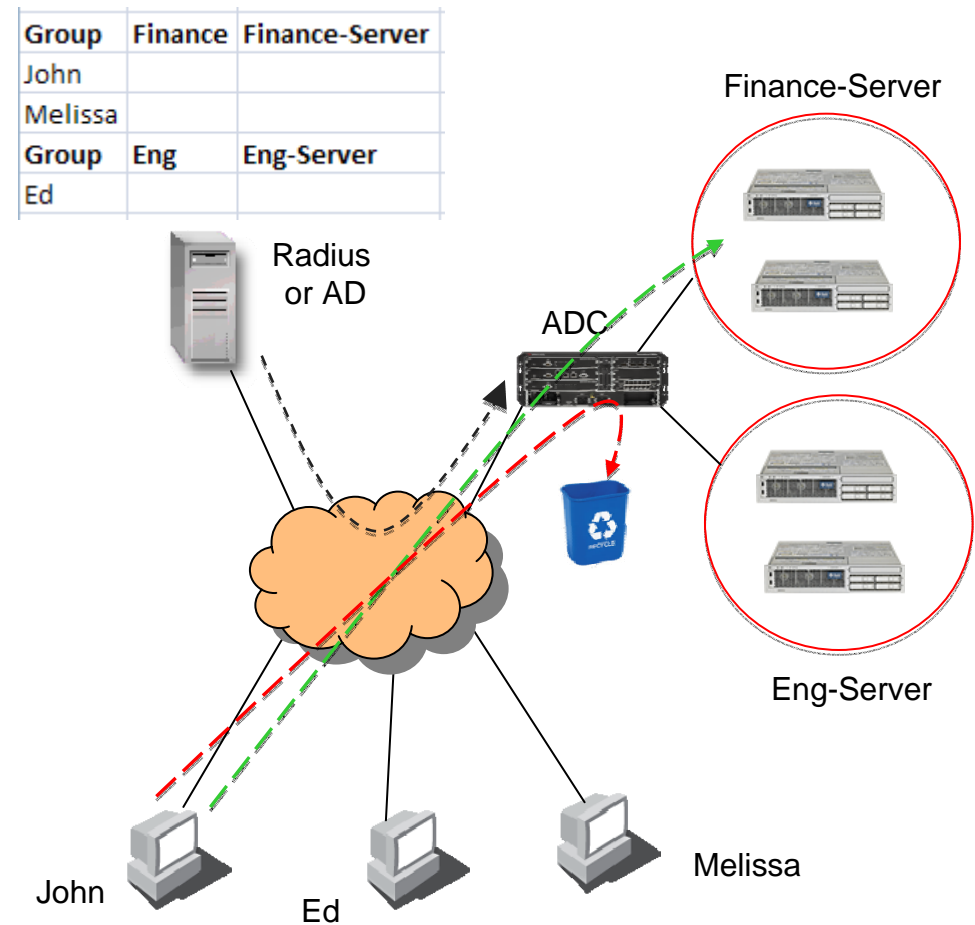
Repositioning the Virtualized ADC to Scale Application Delivery

- ADC's are typically deployed near the Servers
- To scale, ADC's will need to be deployed back in the L3 cloud
- This implies greater L3 functionality and possibly some kind of tunneling approach



Policy Based Access Management

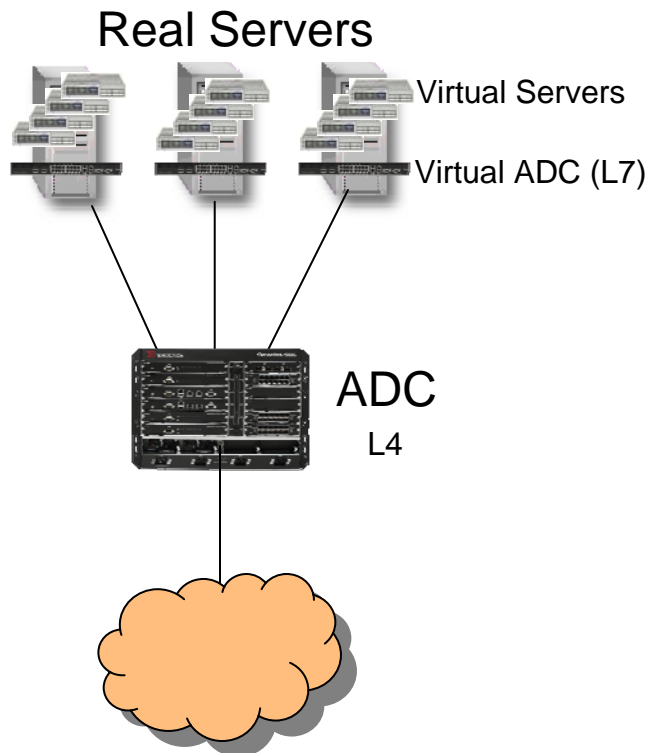
- ADC is ideally located in front of servers to provide augmented identity & security mgmt functions
- Provide AD and/or Radius functionality to download group identity access policies
- Terminate SSL or IPSEC before Server and prevent any application access not explicitly authorized
- Advantage - Offloads security processing and provides policy access mgmt application offload
- Disadvantage – Interfacing with Radius or AD can be difficult



Supporting 10G Server Connectivity

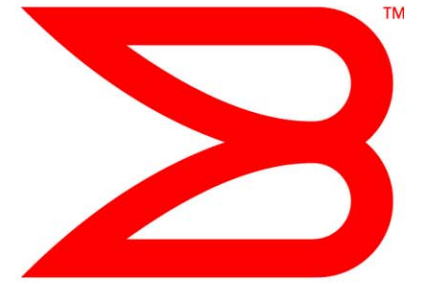
- With 10/100 enet connected Servers an ADC with 5G of throughput could handle 50-100 Servers
- With Gig connected Servers an ADC with 10G of throughput can handle 10-20 Servers
- Highest throughput ADC 's today provide 30-70G of bandwidth. How will they handle 10Gig capable application servers?
- Radical new ADC architectures will need to be developed that significantly lower cost per Gig of throughput and very low cost per transaction
- Trend towards inline deployment for ADCs to handle packet inspection
- Repurposing a PC to provide ADC functionality will no longer be possible
- Dedicated, lower cost ADC's with high-speed switch fabrics will be required (ie the bandwidth problem is going to come back)

Two Tier ADC Solutions



- One tier solution today
- ADC provides all L4-7 functionality, security, app acceleration
- In virtualized world, two tier architectures may be more scalable
- High end ADC provides L4 SLB, security, SSL, and Compression services
- Virtual ADC (software) provides L7 services for virtual servers

BROCADE



Thank You

