Cloud-Based dWAF

A Real World Deployment Case Study

Alexander Meisel
Riverbed Technology
alex AT meisel DOT cc

OWASP
5. April 2012

The OWASP Foundation
http://www.owasp.org

Alexander Meisel

- Director Engineering WAF @ Riverbed Technology
- Former founder and CTO of 'art of defence'
- OWASP Germany (Paper on Best Practices WAF)
- Likes Performance, Scalability and Security
- Email: alex **AT** meisel DOT cc
- Twitter: @one4many

Agenda

- The Cloud … Infinite Space in front of us
- WAF vs. dWAF vs. cloud based WAF
- Customer expectations / operations
- Step One: Datacenter (home ground)
- Step Two: Cloud deployment
- Q & A / Discussion

The Cloud … Infinite Space in front of us

"Space, the final frontier. These are the voyages of the starship Enterprise. Her five-year mission: to explore strange new worlds, to seek out new life and new civilizations, to boldly go where no man has gone before."

(Star Trek NG opening lines)

"Cloud, the current frontier. These are the voyages of the distributed web application firewall. The mission: to explore strange deployments, to seek out new deployment scenarios and (cloud) platforms, to boldly go where no web security software has gone before."

(Alex Meisel, OWASP DC 2012)

Cloud space

- Virtualization
  - OS: Full virtualization, partial virtualization, Paravirutalization
    - Enabling technology for Cloud
  - Storage:
    - Traditional Filesystem: Host-, Device-, Network-based
    - New: Object-based with HTTP interface
- IAAS, PAAS, SAAS
  - Boring, you heard all of this.
- Pricing, CapEx, etc.
  - Not my talk ;-)

Cloud space (Pro's and Con's)

- Con:
  - Most Apps are not developed for the cloud
  - Availability is an issue (SLAs don't solve this!)
  - Persistent performance of virtual infrastructure is not guaranteed
    - Latency
    - Bandwidth
    - CPU time
    - I/O local and remote
  - Shared infrastructure with complete strangers
  - No inter-cloud-vendor API standard

Cloud space (Pro's and Con's)

- Pro:
  - Money (paid incrementally)
  - Scalability (Reacting to business velocity)
    - Unlimited capacity (at a price ;-))
  - Agility (be closer to the customer)
    - Business expansion on a budget
  - Flexibility
    - But ONLY when App's are developed with cloud in mind
  - Highly Automated (using APIs)
    - The DevOps guys love this!

Cloud space (Applications)

- Traditional (local)
- Server based (Web and others)
  - Client Front-End
  - (potentially) multiple Back-Ends like DBs and Disks
- Cloud based
  - Multiple Client Front-Ends
    - SOAP, XMLRPC, WEB, REST
  - Distributed Architecture
    - Program blocks are split up and distributed over several systems communicating over APIs
  - Multiple Back-Ends via distributed program blocks
    - Different Object Storages, DBs or external Systems

Cloud Space (App Deployment)

- Apps get installed on (versioned) images of systems.
- The new image get deployed into the cloud in parallel to the current image
- Once deployment is complete, traffic gets moved (migrated) to the systems with the new image
- After some 'burn-in time' the systems with the old image get shutdown and deleted

Push and Kill vs. Patch and Nurse

WAF vs. dWAF vs. WAF in the cloud

- Traditional WAF
  - Box or monolithic Software
  - In front of the App (Load Balancer, Proxy, etc)
  - Near the App on the Web or Application-Server
- WAF in the cloud
  - Traffic is being redirected (via DNS for e.g.) to traffic scrubbing and protecting proxy farm of WAFs
- dWAF
  - WAF software divided into is parts made to scale over several systems (policy engine, client agents, distributed admin, database, log storage etc.)

Case Study: The Customer

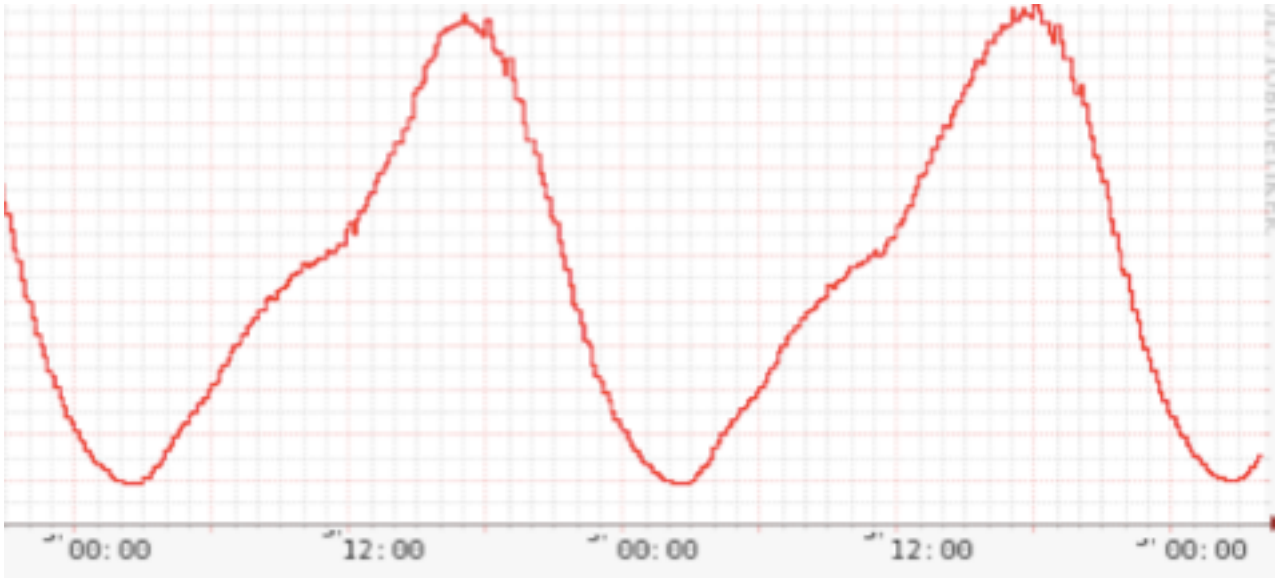
- Has highly agile development department
- They live DevOps because business is changing very fast and growth is exponentially
- They host apps in their own data center but the data center is limited in space
- They realized that the move to cloud in inevitable, but they want to do "the Right Way"

The Customer

- They realized that the application needs to be reengineered and made it cloud ready by re-writing it completely
- They wanted to automate as much as possible using APIs and services of the cloud provider(s)
- They wanted to be compliant, audible, scalable and reliant

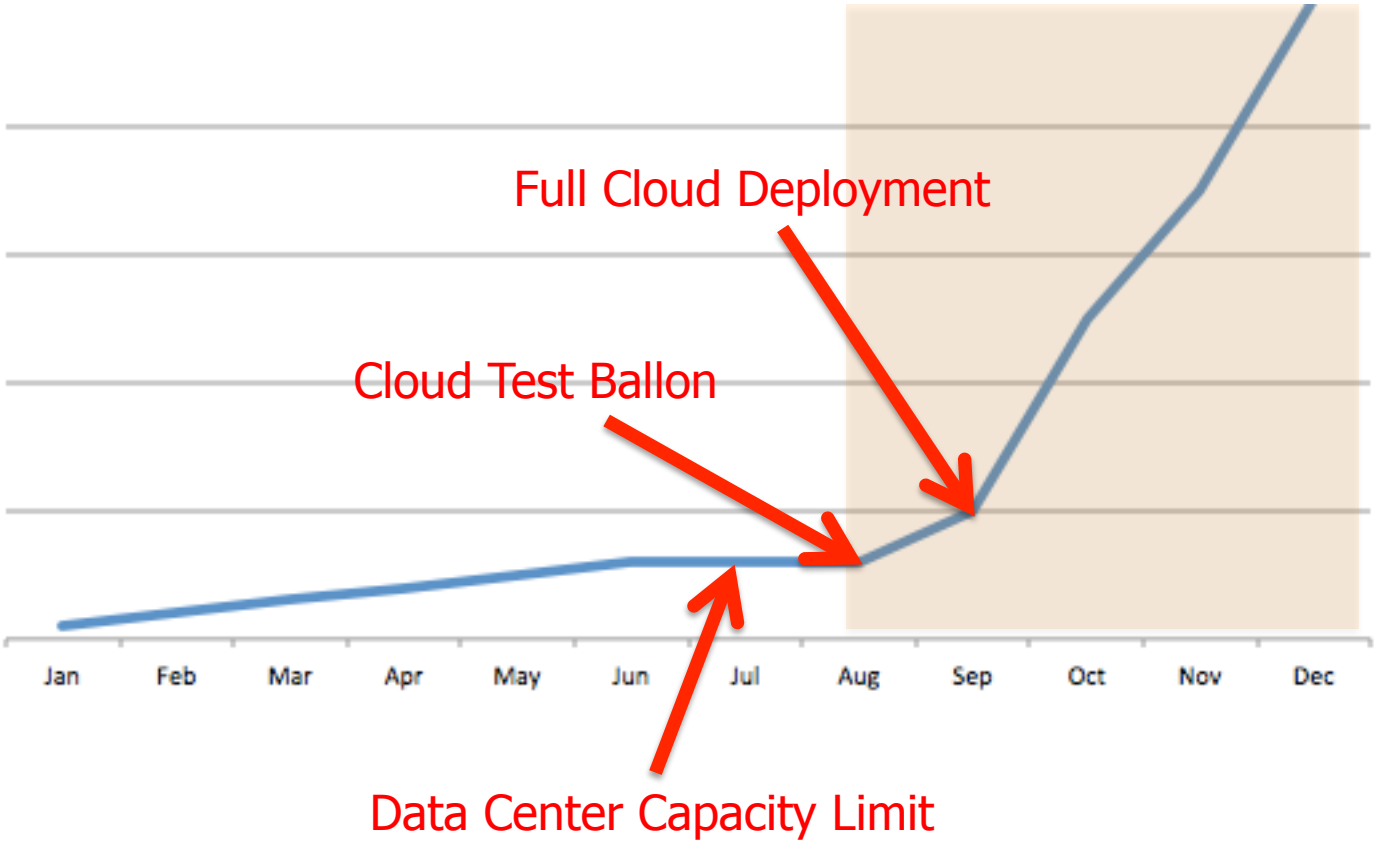
The Customer

- Their traffic looks like this:



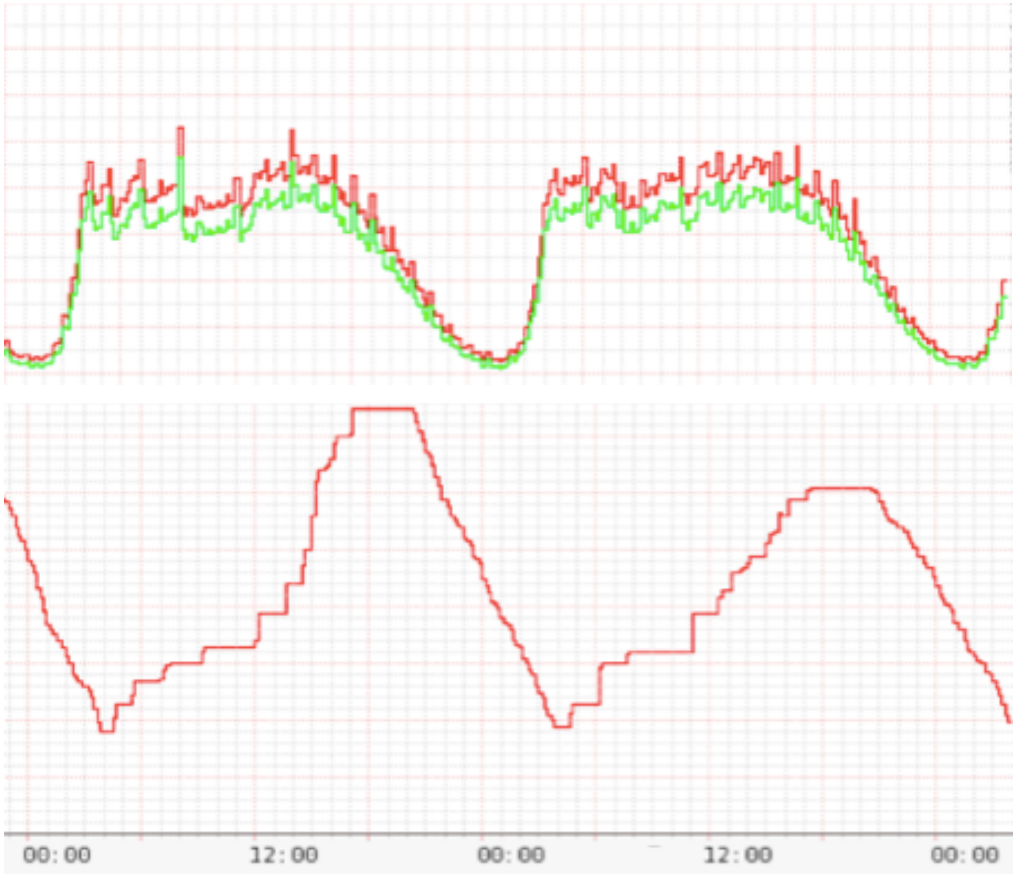
The Customer

- The traffic growth (last year) looks like this:



The customer

- Server Utilization and Auto-Scaling



Test Deployment in (own) Data Center

- Challenges
  - A dWAF deployment is very different from traditional a WAF. Engineers tried it on their own without reading the manual
  - Testing the system under load
- Solutions
  - Explain the architecture and help the engineers on their first install of the software

After all: It is just software and not magic! ;-)

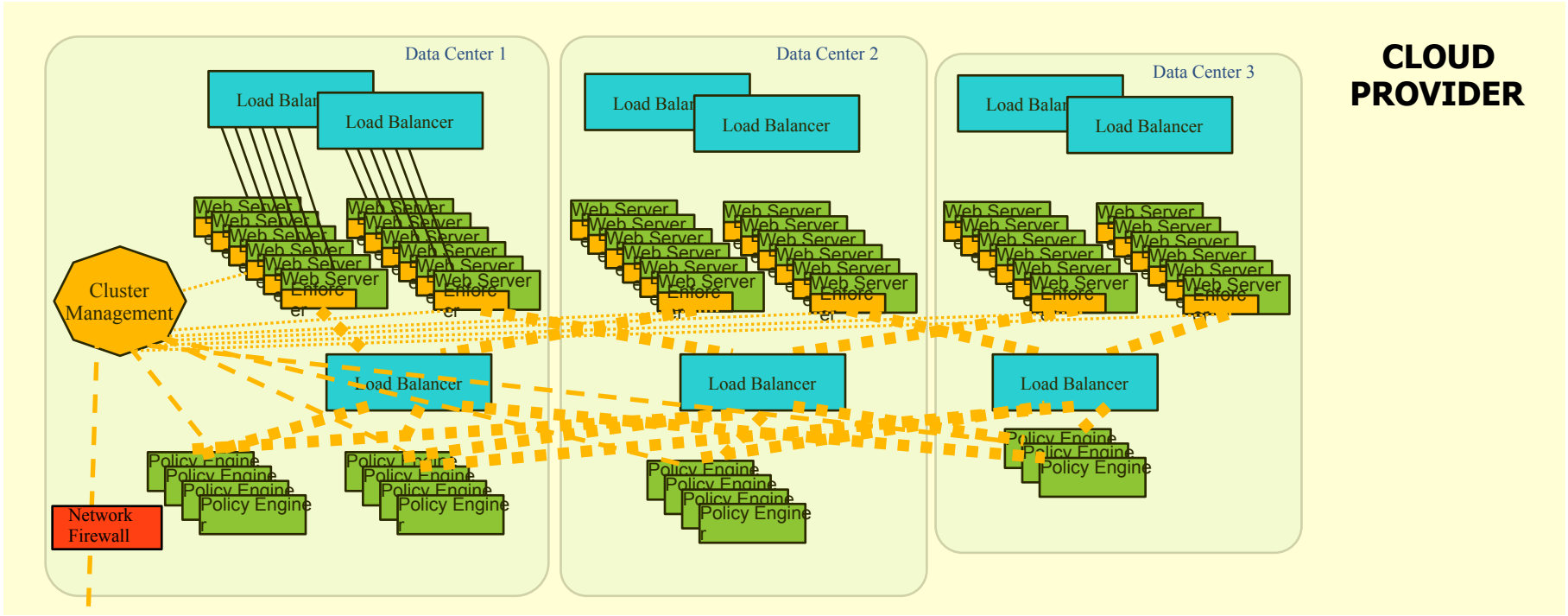
Cloud Deployment and Rollout

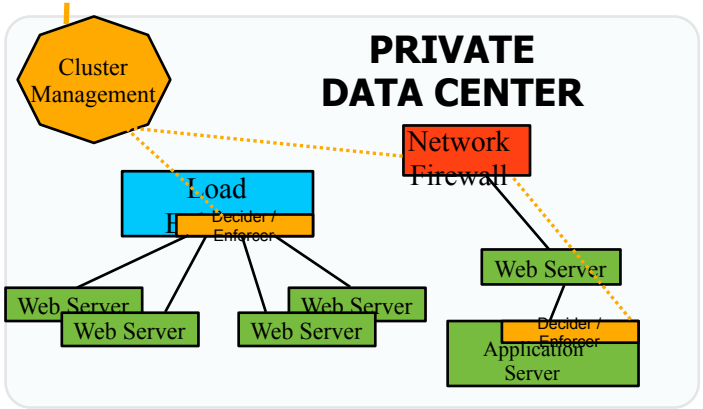
- Challenges
  - Networking between own Data Center and Cloud Provider and NAT
  - Cloud Provider inter Data Center networking
  - Cloud Provider IP address assignments
  - Reduced Load Balancer functionality in Cloud
  - Automated Scaling of Policy Nodes based on some key metrics acquired through dWAF and Cloud-Provider APIs
  - Licensing options with Vendors are limited and not Cloud-Aware/Friendly

Cloud Deployment and Rollout

- Solutions
  - Applications should never use IP addresses to tag sub parts of the system. In order to find new sub systems a service discovery service has been developed and deployed.
  - WAF sub-systems need to register with the service discovery system
  - Communication between WAF parts need to one way to get through NATed networks.
  - WAF components use a generic HTTP based LB-Service to distributed workload and make the overall system more fault-tolerant

Cloud Deployment





- So what does it look like?

Questions?