神州数码
Digital China

互联网电商DDoS防护

Imcloud

北区SE 赵应伟
2022/8/18

神州数码
Digital China

CONTENTS

技术背景调研&讨论

神州数码 Digital China

1.新同事的大学专业讨论-开放性话题

应用交付学习路线

神州数码 Digital China

第一年

技术能力
应用交付基础知识
F5虚拟机，虚拟环境搭建
F5组网
F5基础安装和部署
互联网出口安装部署（不含DNS）
F5 LTM高级配置
实验 (vLab)
101 – Application Delivery Fundamentals
Exam 101
Exam 201–TMOS Administration

第二年（提升）

技术能力
网络TCP/IP协议
DNS协议详解
HTTP / Web协议详解与抓包实战
Linux操作系统
F5 university 培训和考试
Nginx web服务器 / Http 协议详解
Docker的部署和使用
K8S部署和运维
Devops 原理
Python 培训
CCNP
F5 case流程
ELasticStack
神州数码-内部培训视频

三年及以上

解决方案
F5 7个基础解决方案之一 – DDOS防护解决方案
F5 7个基础解决方案之一 – 智能DNS
F5 7个基础解决方案之一 – 高可靠以及优化解决方案
F5 7个基础解决方案之一 – 互联网出口解决方案
F5 7个基础解决方案之一 – 应用交付解决方案
F5 7个基础解决方案之一 – Web安全防火墙解决方案
F5 7个基础解决方案之一 – 双活数据中心解决方案
F5大数据引擎解决方案
F5多云多活解决方案
F5 统一出口解决方案
F5 IPV6改造和迁移解决方案
F5 金融银行行业场景解决方案
F5 NGINX+ 解决方案
F5 与容器 K8S解决方案
神州云科解决方案（任意部分，参考F5模板）

解决方案分享
DDoS电商防护解决方案

DDoS攻击是混合多个层面的

神州数码 Digital China

Application

http flood、慢速交易、恶意秒杀…

SSL

SSL Renegotiation、SSL flood…

DNS

DNS flood、UDP flood、反射攻击…

Network

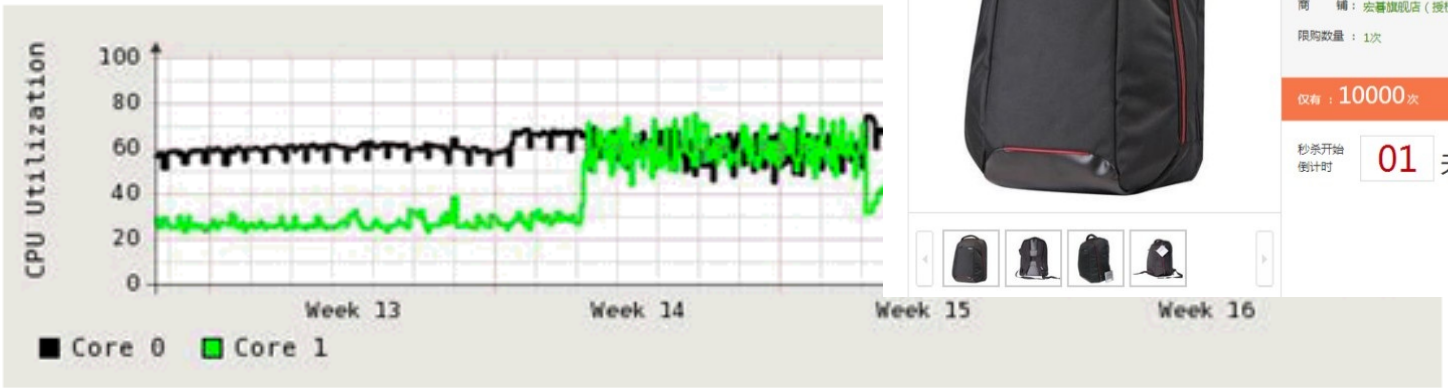
SYN flood、TCP flood、UDP flood、Ping of Death…

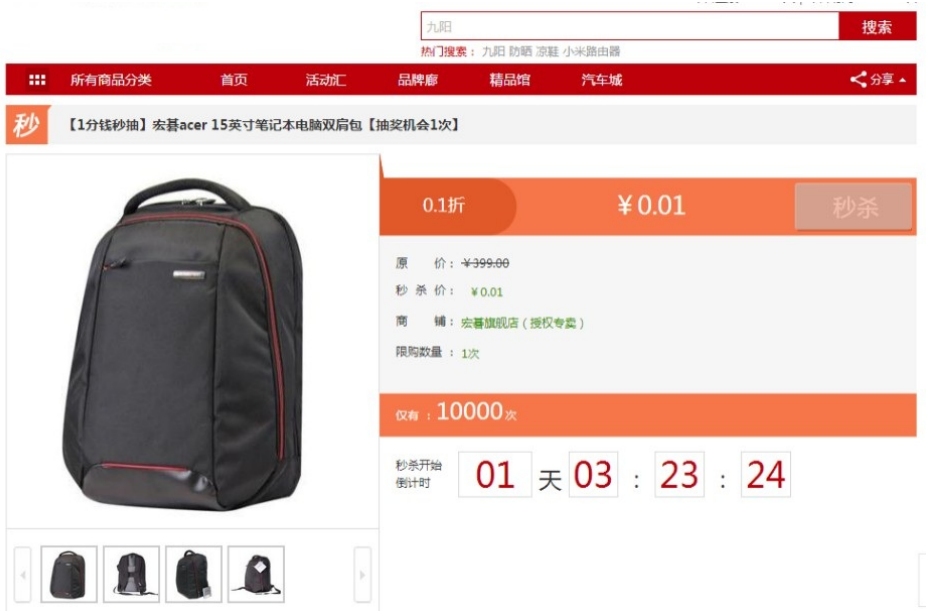
××电商前期实际发生的DDoS事件

神州数码 Digital China

- 4月份小规模DNS DDoS事件
  - 3月13日，LDNS 429K , PATH 1.3M
  - 4月7日，LDNS 554K，PATH 1.9M
  - 4月16日，PATH 1.5M

前期电商平台出现过1秒钟内完成下单交易的情况，突破了包括验证码在内的多重防护体系。





DDoS攻击 - 恶意秒杀的现状

神州数码 Digital China

- 利用秒杀工具抢拍的基本原理是通过机器人、代理、僵尸网络或者脚本并发多个进程向目标网站发起自动化的下单请求，此时大量秒杀商品被少数黄牛党垄断。该行为从业务逻辑难以探测，如何防范也是业界的一个难题，采用多种限制手段效果均不理想。
- 少量黄牛党通过较小的代价获取了大部分的秒杀商品，获取暴利，从而对其他用户造成不公平，也削弱了××银行电商平台希望通过秒杀活动聚集用户人气的初衷。
- 除此以外，“恶意爬站”、“恶意投票”、“恶意占座”、“恶意抢票”等利用电商平台漏洞进行符合业务流程的，大规模的程序请求也成为电商平台经常遇到的DDoS攻击。

采用哪种形式的DDoS防护技术?

神州数码 Digital China

CLOUD/托管类服务

- CDN（Content delivery network）
- 运营商提供的服务
- 基于云端的DDoS服务

内部部署防御

- 网络防火墙+SSL 检查
- Web应用防火墙（WAF）
- 内部部署的DDoS解决方案
- IDPS

采用哪种形式的DDoS防护技术?

神州数码 Digital China

CLOUD/托管类服务

CDN（Content delivery network）

运营商提供的服务

基于云端的DDoS服务

优点

- 完全的外部部署，DDoS攻击不会到达用户内部
- 跨多个用户的防御可以分摊成本
- 实现DNS Anycast在多数据中心提供保护

不足

- CDN无法对动态页面进行防护
- 不管用户是否受到攻击都需要付费
- 被服务条款限制
- 解决方案通常只关注在特定的层面（非所有层面）

采用哪种形式的DDoS防护技术?

神州数码 Digital China

优点

- 对基础架构可以直接控制
- 快速消除攻击，实时的相应和报告
- 解决方案可以设计为互相独立的架构

不足

- 市场中有涉及到很多点的解决方案，但是很少有全面综合的DDoS解决方案
- 现有解决方案瞄准合规性审查而不是实际攻防
- 通常在受到攻击时才有效益 (因此需要综合的解决方案，例如F5的ADN)

内部部署防御

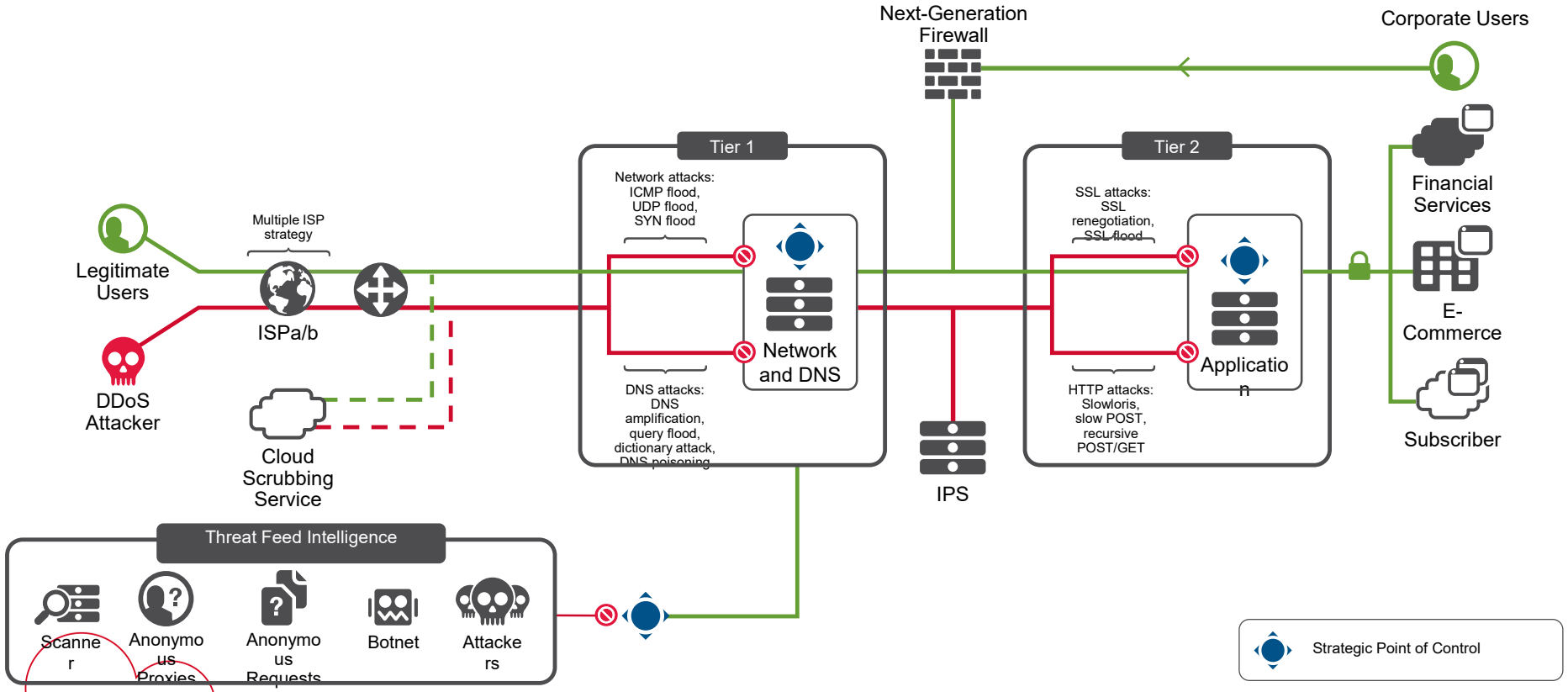
网络防火墙+SSL 检查

Web应用防火墙（WAF）

内部部署的DDoS解决方案

IDPS

DDoS 防护的参考架构



电商防秒杀项目建设目标

- 总体目标：确保针对大部分用户的公平性，从而提高用户的参与积极性，达到业务设计的目标效果。
- 平滑性：限制性措施不能对业务造成中断影响；
- 性能保证：采用限制性措施后不能大幅度降低系统性能；
- 易于实施：不能对原有架构进行大的调整，应用的修改降低到最小；
- 有效性：对恶意流量进行识别和阻截，保证正常用户的正常访问体验。

技术需求分析

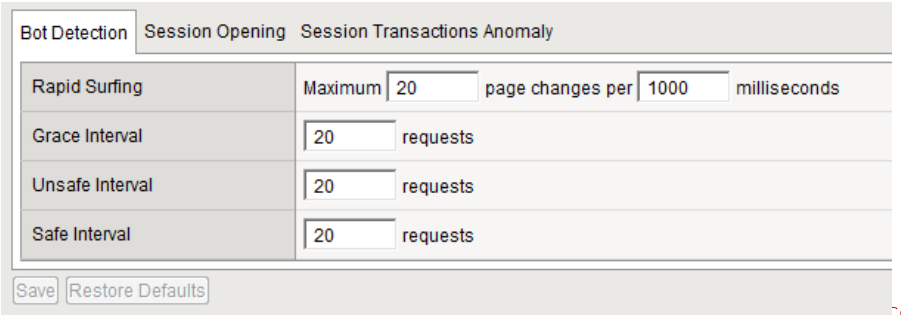
- 为了达到对恶意秒杀行为的防范，需要限制单个用户在规定单位时间内的秒杀商品提交次数；
- 由于F5部署的位置最贴近于应用，且在后台有几十台服务器的情况下，从单个服务器上的应用上入手进行限制并不是针对应用整体的，此时需要有一个全局的统计和控制限制手段，F5的位置最有利于实现基于应用整体的控制。
- 通过F5的irules可以自定义用户的交易行为控制逻辑，通过ASM的Bot防范机制可以判断用户端是否为人的行为。

建设方案 – 防恶意秒杀

- 主要措施：可通过F5 iRules来实现限制单一session在单位时间段内的交易次数。

- 辅助措施：F5 ASM设备周期性的发起挑战信息尝试检测区分正常用户浏览器访问行为和通过秒杀工具发起的访问行为，对于可疑的请求启动防护。

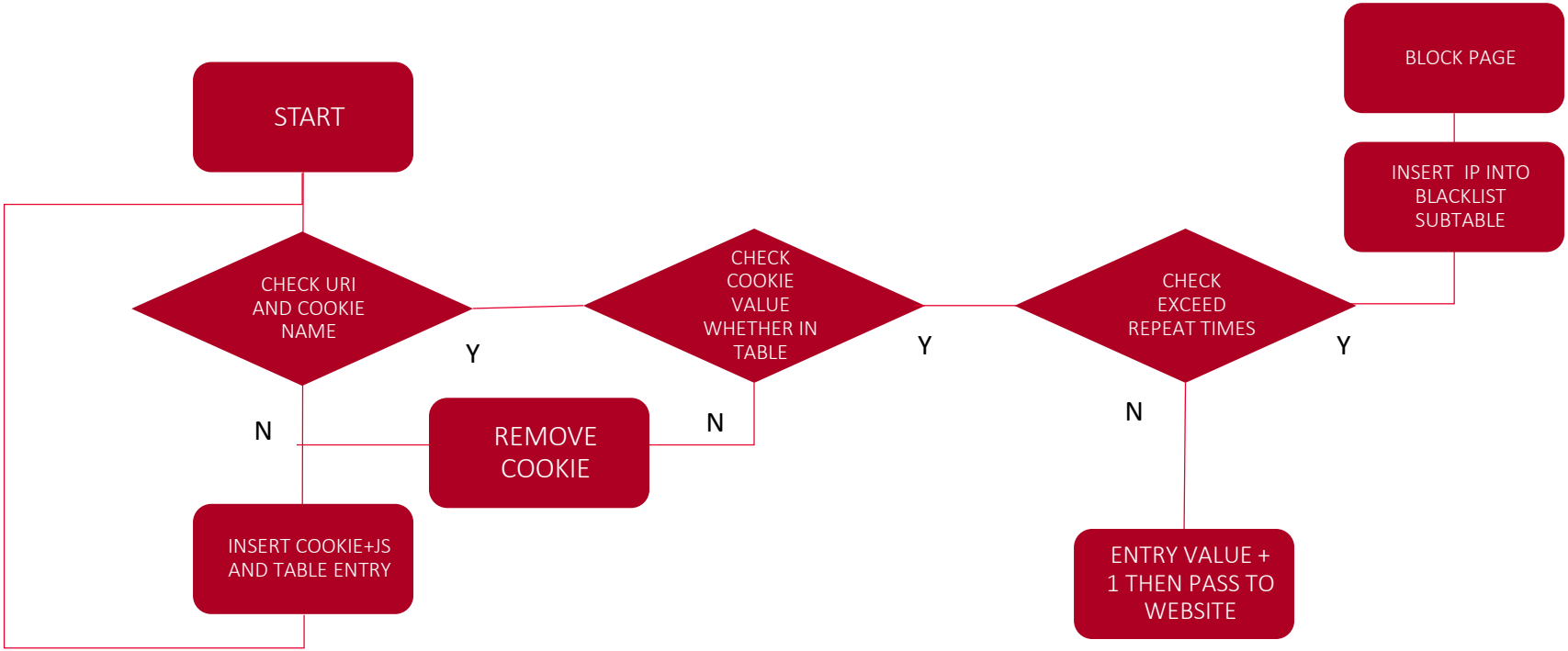
```
when HTTP_REQUEST {
if {[HTTP::method] eq "POST"} {
if { [HTTP::uri] contains "/security/shoppingcart/commit.jhtml" or [HTTP::uri] contains "/shopSe
ckill/confirmIdentifyCodes.jhtml" or [HTTP::uri] contains "/order/createNormalOrder.jhtml" or [H
TTP::uri] contains "/order/createSeckillOrder.jhtml" or [HTTP::uri] contains "/order/createPromo
tionOrder.jhtml" or [HTTP::uri] contains "/order/createFinanceOrder.jhtml" or [HTTP::uri] contai
ns "/safeConnection/reg/subRegisterInfo.jhtml" or [HTTP::uri] contains "/member/memberOrderCance
l.jhtml"} {
  if { $static::control_by_Session == 1} {
    set  SessionId [HTTP::cookie JSessionID]
  }
  else {
    set  SessionId [IP::client_addr]
  }

  #tracking表满，drop请求，这个可以根据需求进行调整
  if { $static::tracking_memlimit == 1 } {
    set total [table keys -subtable "tracking" -count]
    if { $total > $static::tracking_maxentry } {
        #drop
        return
    }
  }

  #update子表中该sessionid的值加1
  table incr -subtable "tracking" $SessionId
  # 设定该key的存活时间为180秒
  table lifetime -subtable "tracking" $SessionId 180
```



扩展思考

- 在实际攻防中，黑客会猜解服务端的防护方式，这就要求服务端的防护手段多样化，并且可以随时变化
- 可以利用ASM或iRules采用插入Javascript和Cookie的方式检验客户端是否为浏览器
- 通过和F5其他功能结合，如Session，HASH，Table等，将客户端的Cookie内容动态化
- 再根据用户实际业务要求进行流程控制

举例：实际攻击防护思路


START
CHECK URI AND COOKIE NAME
Y
N
CHECK COOKIE VALUE WHETHER IN TABLE
Y
N
REMOVE COOKIE
CHECK EXCEED REPEAT TIMES
Y
N
BLOCK PAGE
INSERT IP INTO BLACKLIST SUBTABLE
INSERT COOKIE+JS AND TABLE ENTRY
ENTRY VALUE + 1 THEN PASS TO WEBSITE

竞争分析

- 与应用开发修改的方案对比
  - 无法从应用全局的角度进行控制，只能每一台服务器单独计数控制频率；
  - 修改复杂，工作量大；
  - 无法适应攻击特征及频度的动态变化；

- 与其他网络设备的竞争对比
  - 无法进行应用逻辑层面的统计和控制；

技术优势

- 可从战略控制点（SPC）的全局角度，对用户的交易行为进行统计和控制，贴合用户需求；
- 高级防火墙、DDoS和WAF的统一结合，涵盖L4-L7的整体安全；
- iRules简单易实施，平滑变更；
- iRules可随时根据攻击特征及频度进行灵活的调整；
- 能够与用户session相结合，深入控制七层特性；
- VIPRION性能突出，且可根据需要随时插板进行扩容；

XX电商项目建设需求

相比于集群化程度低，集约化水平高，应用架构耦合度紧密，牵一发而动全身传统企业IT架构，互联网业务对IT架构提出了哪些要求呢？主要有以下三个方面：

1. 时效性

   互联网产品生命周期具有很强的时效性，要求后台IT架构具有较强的敏捷性。

2. 扩展性

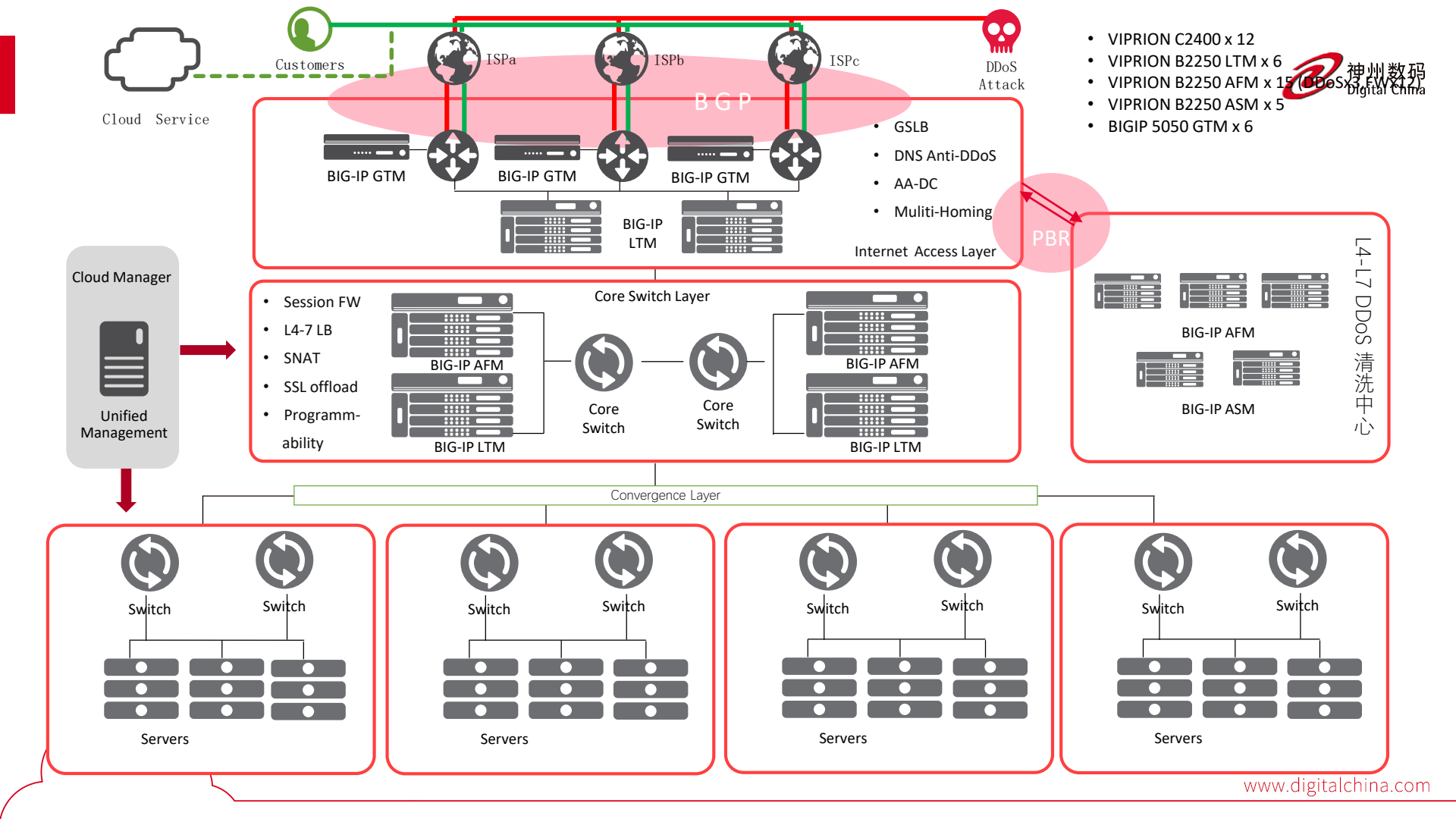
   互联网产品不同时期客户数量具有较大的变化，甚至同一天不同时段客户数量千差万别。这要求后台IT架构具有较强的弹性与伸缩性。

3. 可管理性

   传统IT架构采用烟囱式业务模式，各业务相互隔离，管理模式相对单一。而互联网的时效性与扩展性要求IT架构具有高度管理性与安全性作为支撑。

方案设计基于以下XX电商的特点

- 互联网思维，勇于创新
- 引入分布式架构，商业产品和开源软件并行
- 基于不同场景，不同业务的需求分析及开发部署
- 云化思维，资源池化，功能服务化，架构平台化 (SDAS)
- 安全隔离在应用层解决，安全架构扁平化
- L4-L7层DDoS是安全的重点
- 自动化部署和运维


Customers
ISPa
ISPb
ISPc
DDoS Attack
Cloud Service
BGP
BIG-IP GTM
BIG-IP GTM
BIG-IP GTM
BIG-IP LTM
GSLB
DNS Anti-DDoS
AA-DC
Muliti-Homing
Internet Access Layer
PBR
VIPRION C2400 x 12
VIPRION B2250 LTM x 6
VIPRION B2250 AFM x 15 (DDoSx3 FWx12)
VIPRION B2250 ASM x 5
BIGIP 5050 GTM x 6
神州数码 Digital China
L4-L7 DDoS 清洗中心
BIG-IP AFM
BIG-IP ASM
Cloud Manager
Unified Management
Session FW
L4-7 LB
SNAT
SSL offload
Programm-ability
Core Switch Layer
BIG-IP AFM
BIG-IP LTM
Core Switch
Core Switch
BIG-IP AFM
BIG-IP LTM
Convergence Layer
Switch
Switch
Servers
Switch
Switch
Servers
Switch
Switch
Servers
Switch
Switch
Servers

DDoS清洗中心可防护攻击种类

OSI 层级	攻击内容	LTM AFM	LTM+ iRule	DNS	ASM
Network Based (2-4层)	IP Fragment				
	Tear Drop				
	SYN Flood (Dirt Jumper)				
	TCP (connection) Flood e.g. SYN-ACK, ACK & PUSH-ACK, RST or FIN and Fragmented ACK				
	Christmas Tree				
	Fake Session				
	LAND				
	Redirect Traffic Attack				
	ICMP Flood, Ping Floods and SMURF Attacks				
	Ping of Death ICMP				
DNS based (4层)	UDP Flood				
	UDP Fragment				
	DNS Flood (Distributed and DNS Blacklisting) e.g. DNS UDP Flood, DNS Query Flood and DNS NXDOMAIN Flood		IP Blacklist (Datagrp)	DNS Express + DNS iRule	
SSL/TLS based (5–6层)	SSL Floods, Malformed SSL (e.g. empty SSL HELLO)				
	SSL THC attack (Extending from SSL Renegotiation vulnerability)				
Application based (6–7层)	Slowloris (Nuclear DDoSer, Slowhttptest)				
	Keep-Dead				
	Slow POST (R-U-Dead-Yet, Tor Hammer, Nuclear DDoSer, Slowhttptest)				
	HashDoS				
	Apache Killer (Slowhttptest)				
	HTTP GET Flood, Recursive GET Flood (Web Scraping), Dirt Jumper (HTTP Flood)				
	#RefRef (exploit SQLi - OWASP Top 10 vulnerability as entry)				
	XML “Bomb” (DTD attack), XML External Entity DoS				

客户收益

- 保障电商业务的7*24的高可用性，保障用户最佳体验。
- DDoS清洗中心，抵御大规模攻击，保证业务在遭受DDoS攻击时高可用。
- 72M Session的高并发级别防火墙，240G吞吐并且支持无缝扩展升级。
- 硬件设备的虚拟化降低了用户采购设备和后期运维的成本，提升了系统的处理能力和可扩展性。
- 快速部署复杂应用，并自动实现应用的优化，通过可编程脚本根据业务需求及时更新应用服务，有效减轻了应用系统的压力。
- 未来双活数据中心无缝升级，无需对当前数据中心进行复杂改建，节约成本。

综合讨论-总结

神州数码
Digital China

神州数码
Digital China

神州数码集团股份有限公司
股票代码：000034.SZ

谢 谢 大 家

欢迎关注
神州数码集团微信