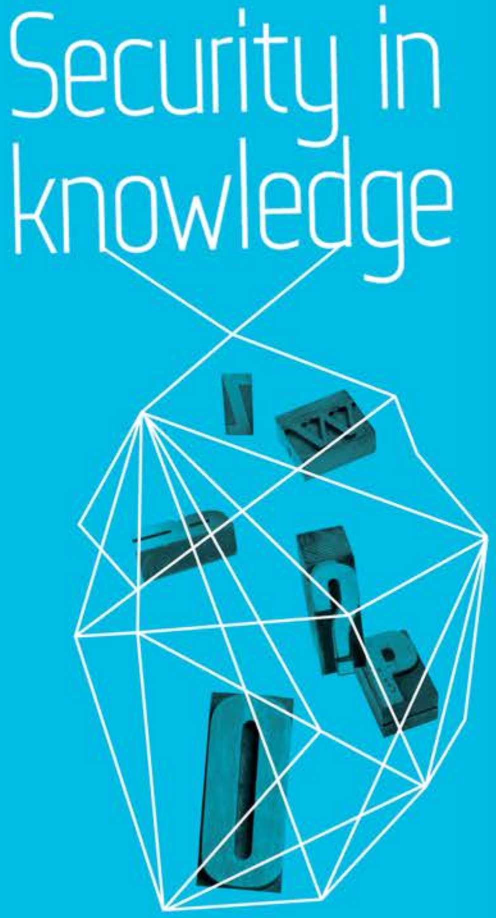
RSA CONFERENCE
ASIA PACIFIC 2013



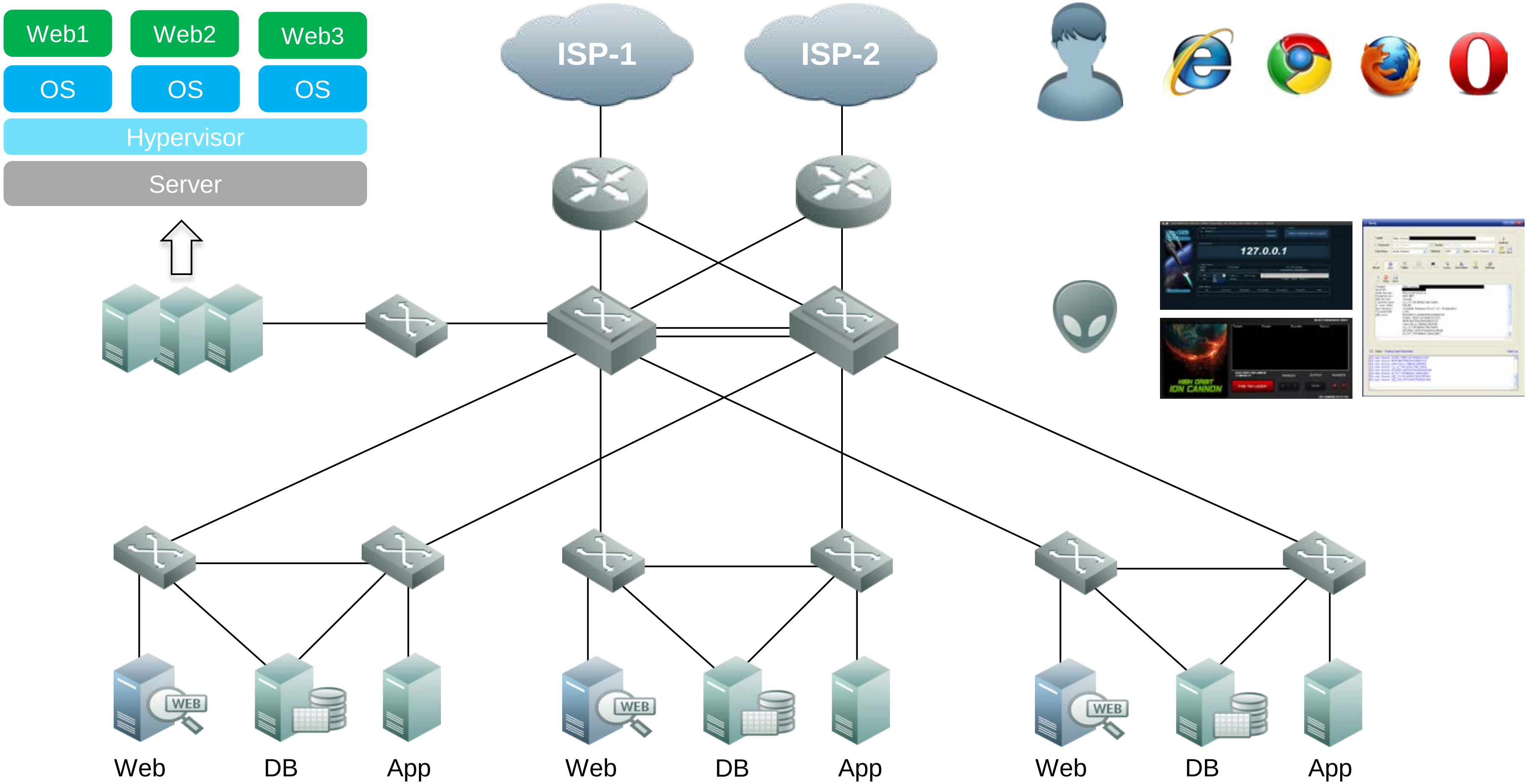
Architecture of a new DDoS and Web attack Mitigation System for Data Center

LIANG ZHAO
NSFOCUS Information Technology Co., Ltd.
CONGYU LI
NSFOCUS Information Technology Co., Ltd.

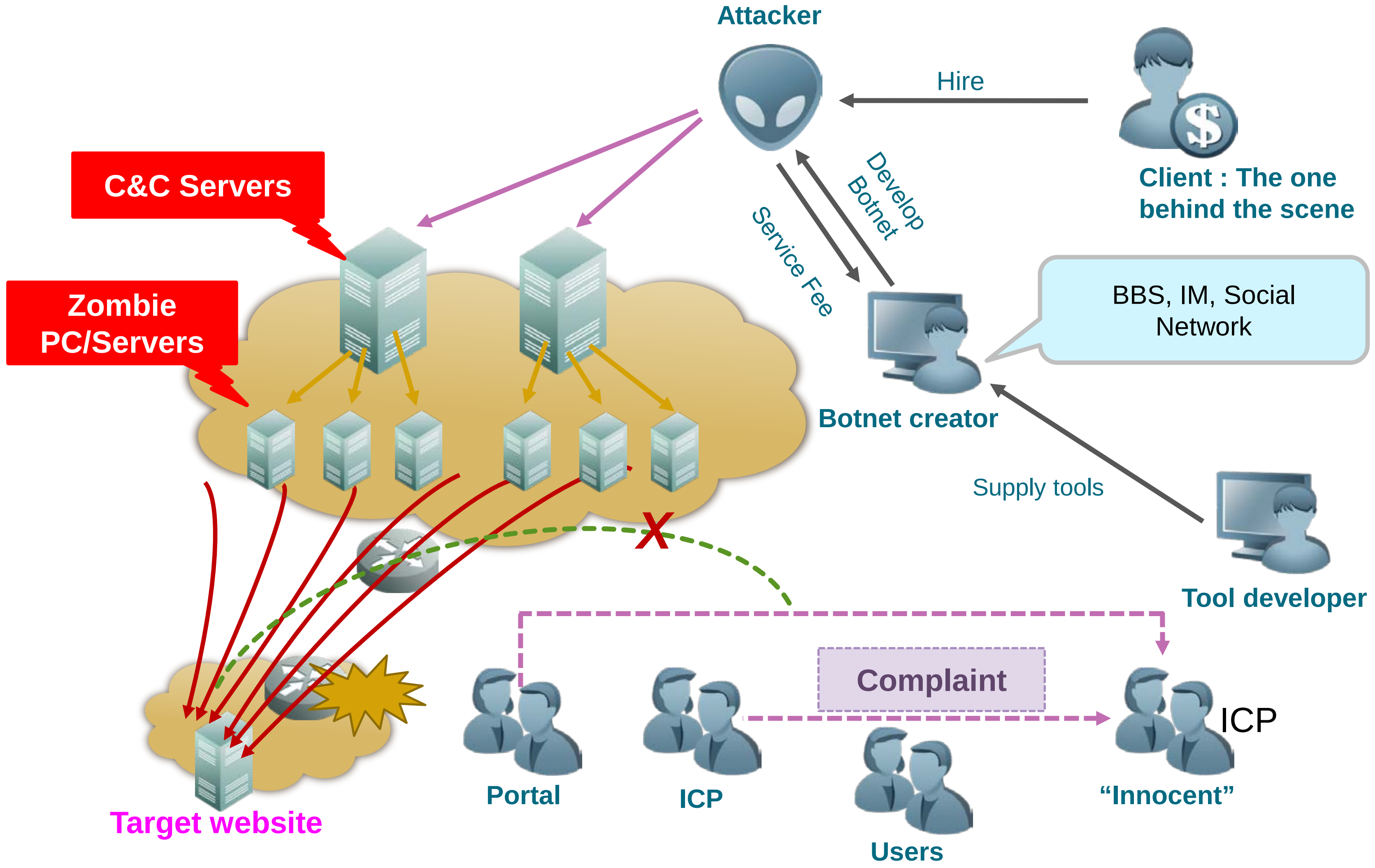
Session ID: DAS-T01

Session Classification: Intermediate

Data Center Web Hosting

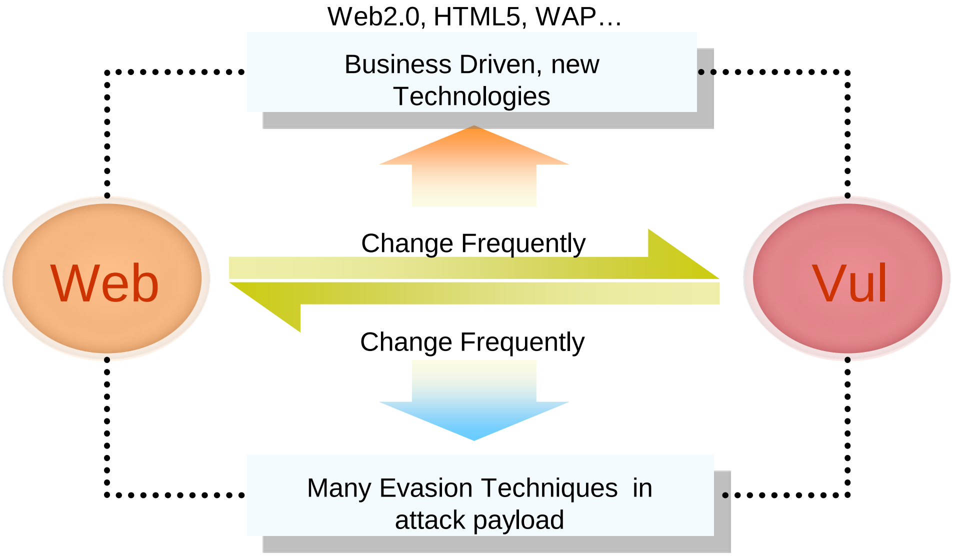


DDoS Attack


Attacker
Hire
Client : The one behind the scene
Develop Botnet
Service Fee
BBS, IM, Social Network
Botnet creator
Supply tools
Tool developer
C&C Servers
Zombie PC/Servers
X
Complaint
Portal
ICP
Users
ICP
"Innocent"
Target website

Web Attack

Technology	Examples
Protocol	HTTP, HTTPS
Application	HTML, CSS, XHTML, CGI, ASP, JSP, PHP…
Web Plug-in	Structs, Wordpress, ECShop…
Web Server	IIS, Apache, WebSphere, WebLogic…
OS	Windows, Linux, Unix
DB	SQL Server, MySQL, DB2, Sybase, Access…



Web2.0, HTML5, WAP…

Business Driven, new Technologies

Web

Change Frequently

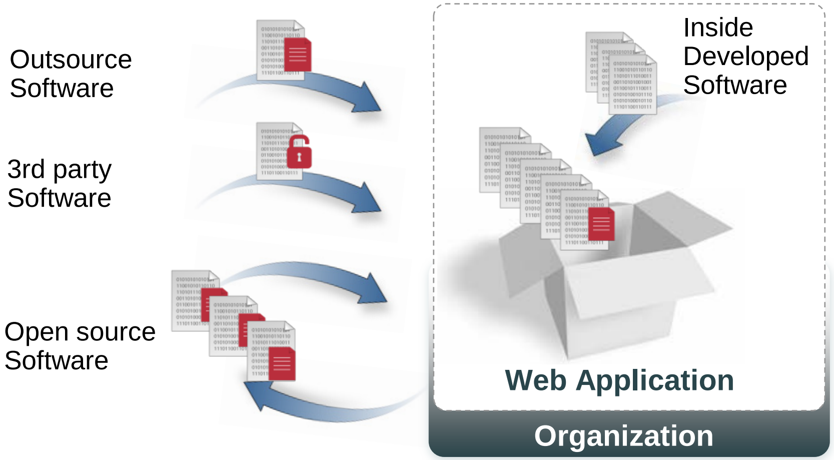
Change Frequently

Vul

Many Evasion Techniques in attack payload

Original: http://example/scripts/foo.cgi?page=menu.txt

Attack: http://example/scripts/foo.cgi?page=../scripts/foo.cgi%00txt



Outsource Software

3rd party Software

Open source Software

Inside Developed Software

Web Application

Organization

OWASP Top 10 2013

- Injection
- Broken Authentication and Session
- Cross Site Scripting (XSS)
- Insecure Direct Object References
- Security Misconfiguration
- Sensitive Data Exposure
- Missing Function Level Access Control
- Cross-Site Request Forgery (CSRF)
- Using Components with Known Vulnerabilities
- Unvalidated Redirects and Forwards

Attack Case 1

<Operation Ababil>

Background/Phase

Protest

2012.7
Disaster cased by a film clip

Attack

2012.9.18
Cyber Fighters set up DDoS attack to Banks of the U.S.
Named as “Operation Ababil”

2 Phases

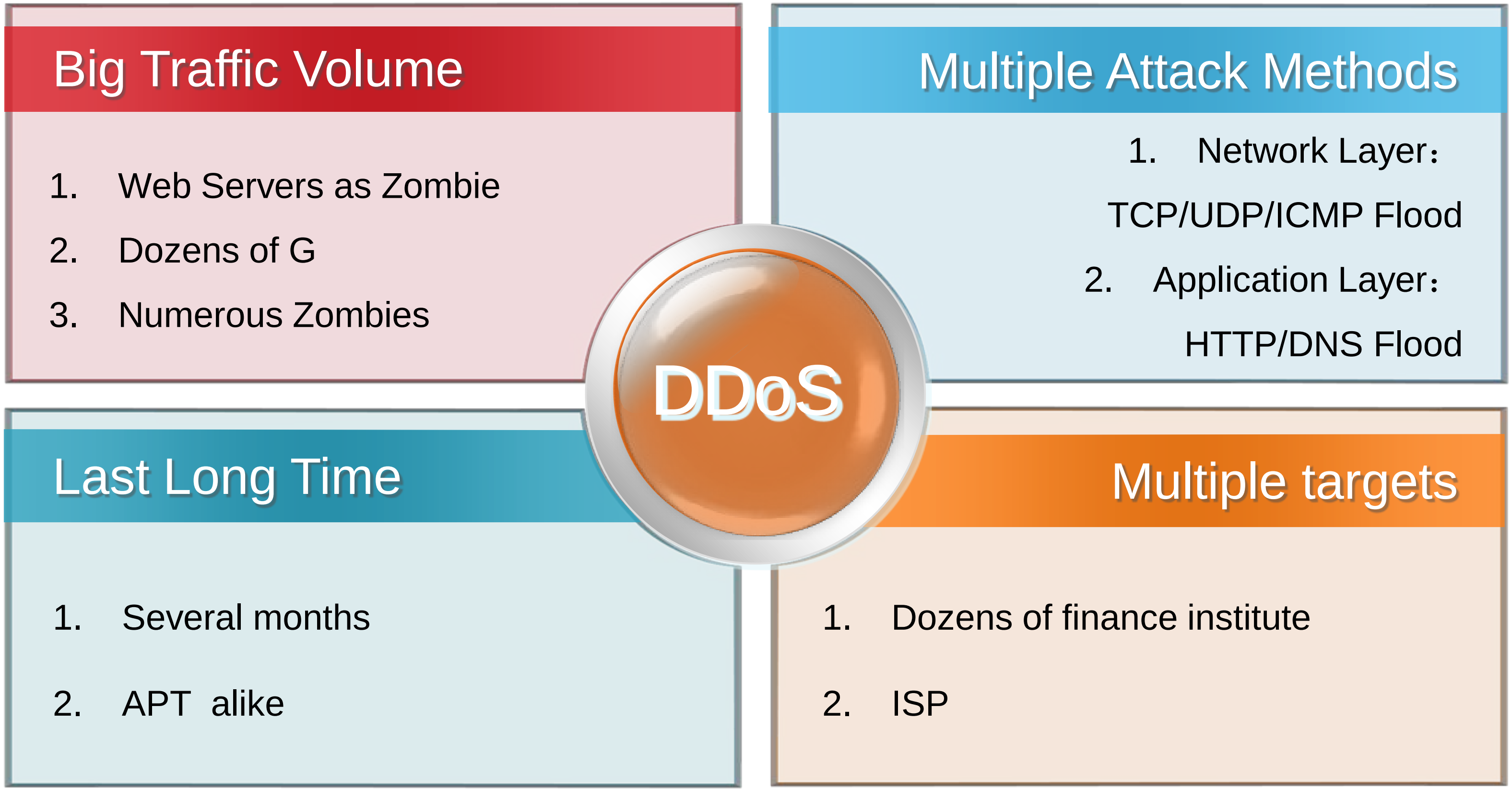
Phase 1, 5 weeks (9.18-10.23)
Phase 2, 7 weeks (12.10-1.28)

Pause/Continue

2013.1.29 attack pause
2013.3.5 attack continue

Bank of America
HSBC
citi
Capital One

Characteristics



DDoS

Big Traffic Volume

1. Web Servers as Zombie
2. Dozens of G
3. Numerous Zombies

Multiple Attack Methods

1. Network Layer：
   TCP/UDP/ICMP Flood
2. Application Layer：
   HTTP/DNS Flood

Last Long Time

1. Several months
2. APT alike

Multiple targets

1. Dozens of finance institute
2. ISP

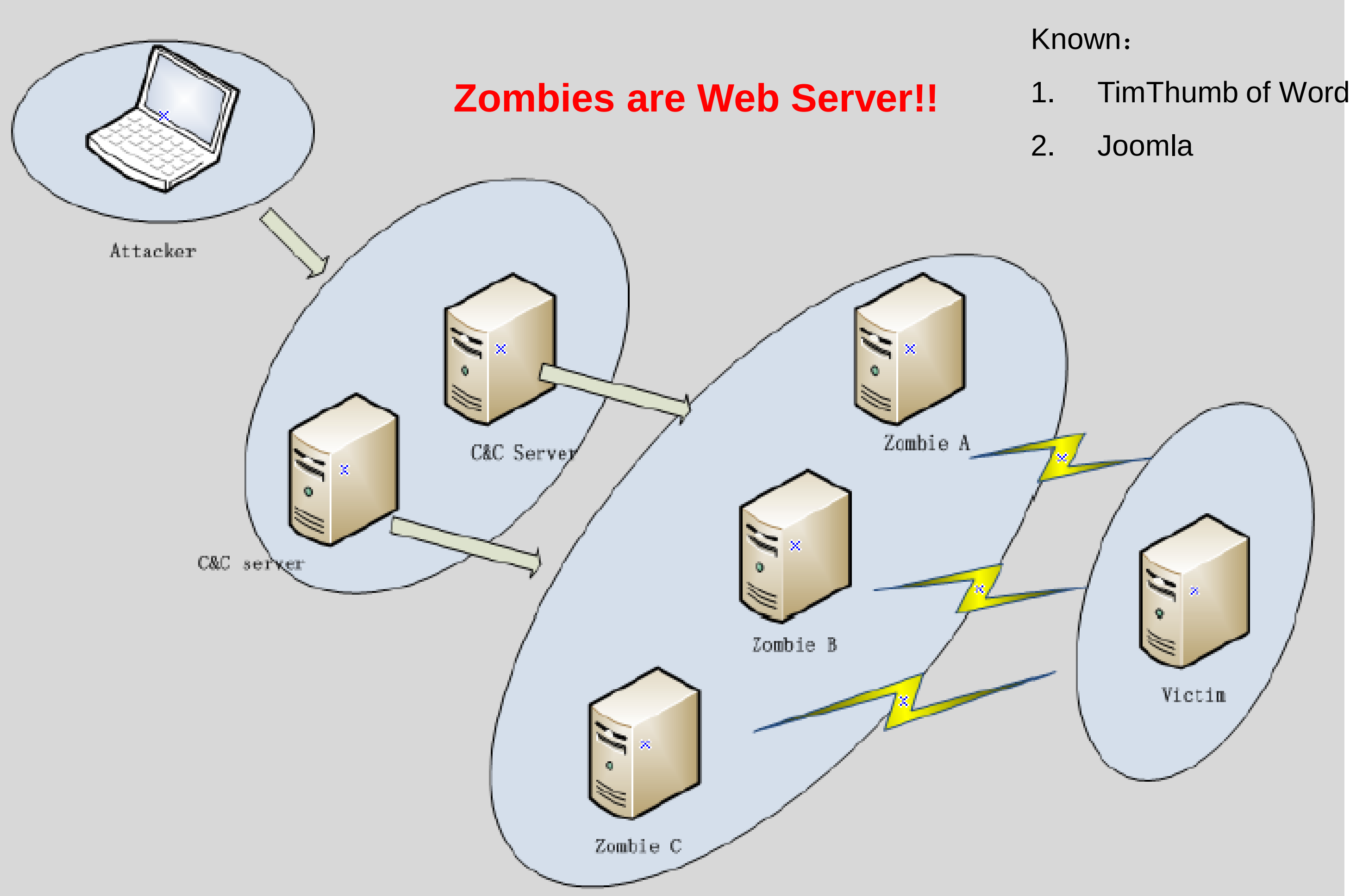
Operation Steps

- Vulnerable admin passwords
- Software Vulnerabilities

Known：

1. TimThumb of WordPress
2. Joomla

Zombies are Web Server!!



oS

DDoS

gets

Attack Tools

Name	Type
Itsoknoproblembro	TCP Flood
	UDP Flood
	HTTP Get Flood
	HTTP Post Flood
Kamikaze	HTTP Get Flood
Amos	HTTP Post Flood

Attack Case 2

<Spamhaus VS. Cyberbunker>

ICP VS DC, 2013.3.18

Cyberbunker has relationship with criminals from East Europe and Russia, is behind recent network attacks

SPAMHAUS

1

You send spam, Blacklist you!

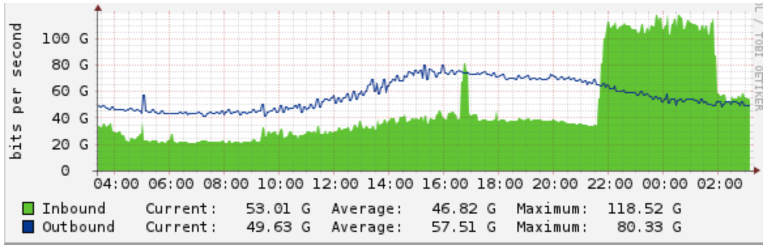
2

Why? You dare block me, I strike you!

Spamhaus abused its position, it has no right to decide what content can appear on the Internet and what cannot.

MSSP step out, VS DC

CLOUDFLARE



5

Just 75G,
got it done,
you can do some marketing

4

Help!
I got attacked
DDoS!!

SPAMHAUS

75G, day and night, strike to death

3

We have been attacked continuously for 1 week, but we kept standing, never down. You cannot imagine how much efforts our engineers made. Such attack can swallow everything.

MSSP became Target

CLOUDFLARE

6

You dare to help him!
I will strike you instead.

5

Just 75G,
got it done,
you can say something about it

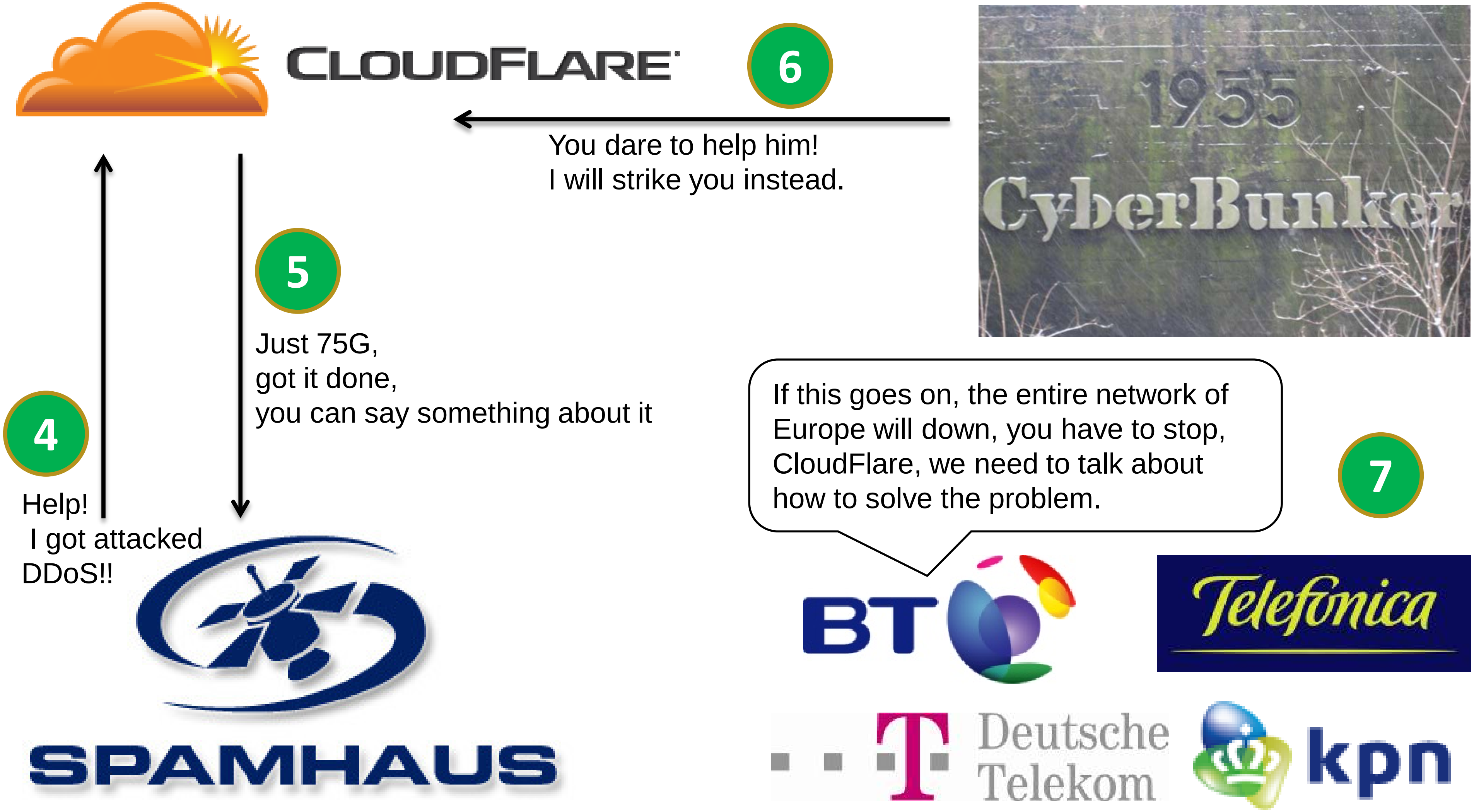
4

Help!
I got attacked
DDoS!!

SPAMHAUS

Attacked from Mar 23, 300-600G, targets are not ordinary equipments, but CloudFlare BGP direct peering and IX, attacks are totally out of control. Attacks to IX include London LINK, Amsterdam AMS-IX, HK-IX, Frankfurt DE-CIX, etc. Among them, London IX got influenced most significantly, caused direct effects to Internet Business within.

ISP got effected



4

Help!
I got attacked
DDoS!!

5

Just 75G,
got it done,
you can say something about it

6

You dare to help him!
I will strike you instead.

If this goes on, the entire network of Europe will down, you have to stop, CloudFlare, we need to talk about how to solve the problem.

7

Words after Event

SPAMHAUS

We will continue our righteous career, we will not be stroked down, we are the best!

1955 CyberBunker

There is no evidence saying that we are responsible of the action. We will persist in our belief, “Freedom Internet”!

CLOUDFLARE

We should keep low-profile, thanks for the collaboration of everyone, we need to improve.

BT Telefónica Deutsche Telekom kpn

You made so much trouble to us, and we did not earn any money from these work.

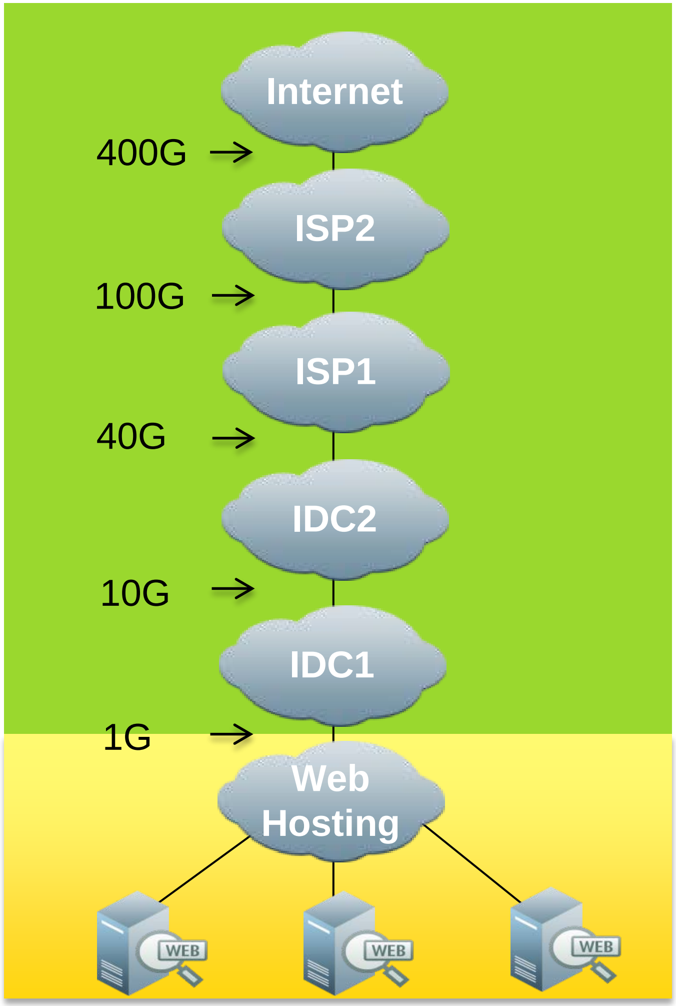
US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Last year, we have warned that we need to pay attention to the right configuration of DNS server, you see…

Thoughts

- DDoS and Web attack devastate Data Center Web Hosting business.
- Both of the 2 attacks are complicated, but in different ways.
- Data Centers need to mitigate DDoS and Web attack simultaneously, accurately and cost-effectively.
- How to transfer from DDoS attack mitigation to Web attack mitigation smoothly as the attack changes? For instance, DDoS attack from 1G to 10G to 40G to 100G to 400G, and change from DDoS attack to Web attack.

DDoS Attack Mitigation



1. IP address Verification
- Source/destination IP address check/verification

2. Access Control List
- Layer 4 ACL
- Conn-Exhaustion ACL
- URL ACL

3. Reputation List
- White/Black List
- Dynamic Prioritizing

4. Protocol Analysis
- Protocol Validation by RFC check

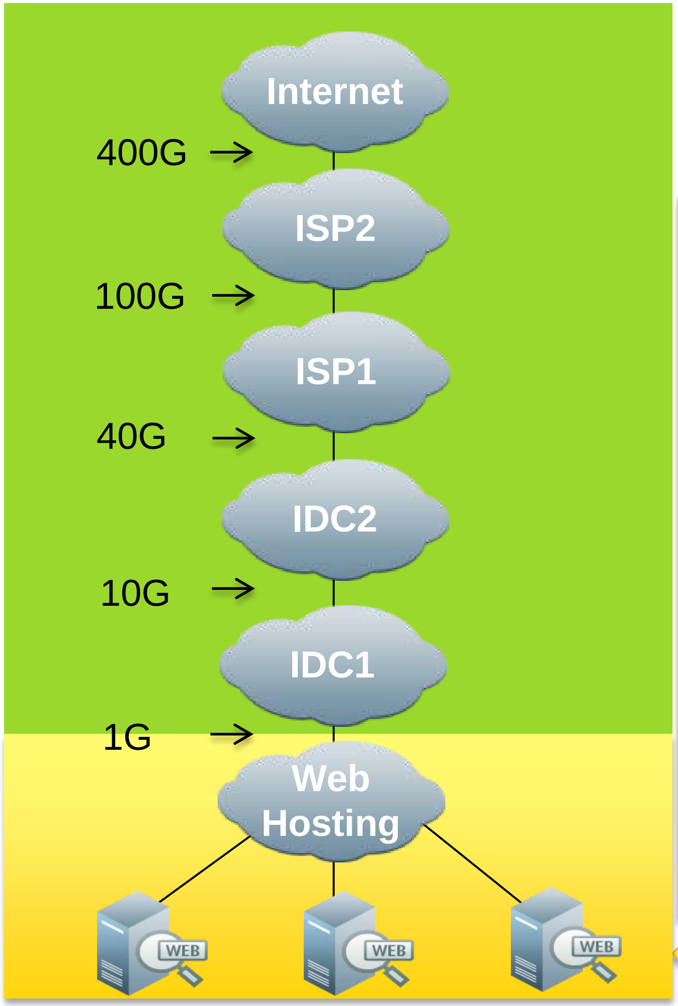
5. Layer 4 Flood Mitigation
- Source/destination IP address check/verification
- Various mitigation algorithms

6. Layer 7 Flood Mitigation
- Various mitigation algorithms
- Pattern Matching

7: Rate Limit
- Restricts traffic and ensures the critical business.

It has been consensus in Data Center industry that the best place to stop DDoS attack, e.g. SYN flood, is in backbone network, since the attack traffic volume can be large, e.g. 10Gbps. Data Center usually provides DDoS attack mitigation as a part of its infrastructure service.

Web Attack Mitigation



On the other hand, Web attack, e.g. SQL Injection, is not large in volume, but its payload goes up to data level. Data Center usually provides Web attack mitigation as a dedicated service to Web Hosting customer.

1. Network Access Control

2. TCP Flood Protection

3. HTTP Termination

4. SSL Decryption

5. Data Normalization

6. HTTP Flood Protection

7. HTTP Validation

8. HTTP Access Control

9. Web Server and Plug-in Protection

10. Rule-Based Protection

- •Crawler
- •XSS
- •SQL Injection
- •LDAP Injection
- •SSI Command Injection
- •XPath Injection
- •Command Line Injection
- •Path Traverse
- •Remote File Inclusion

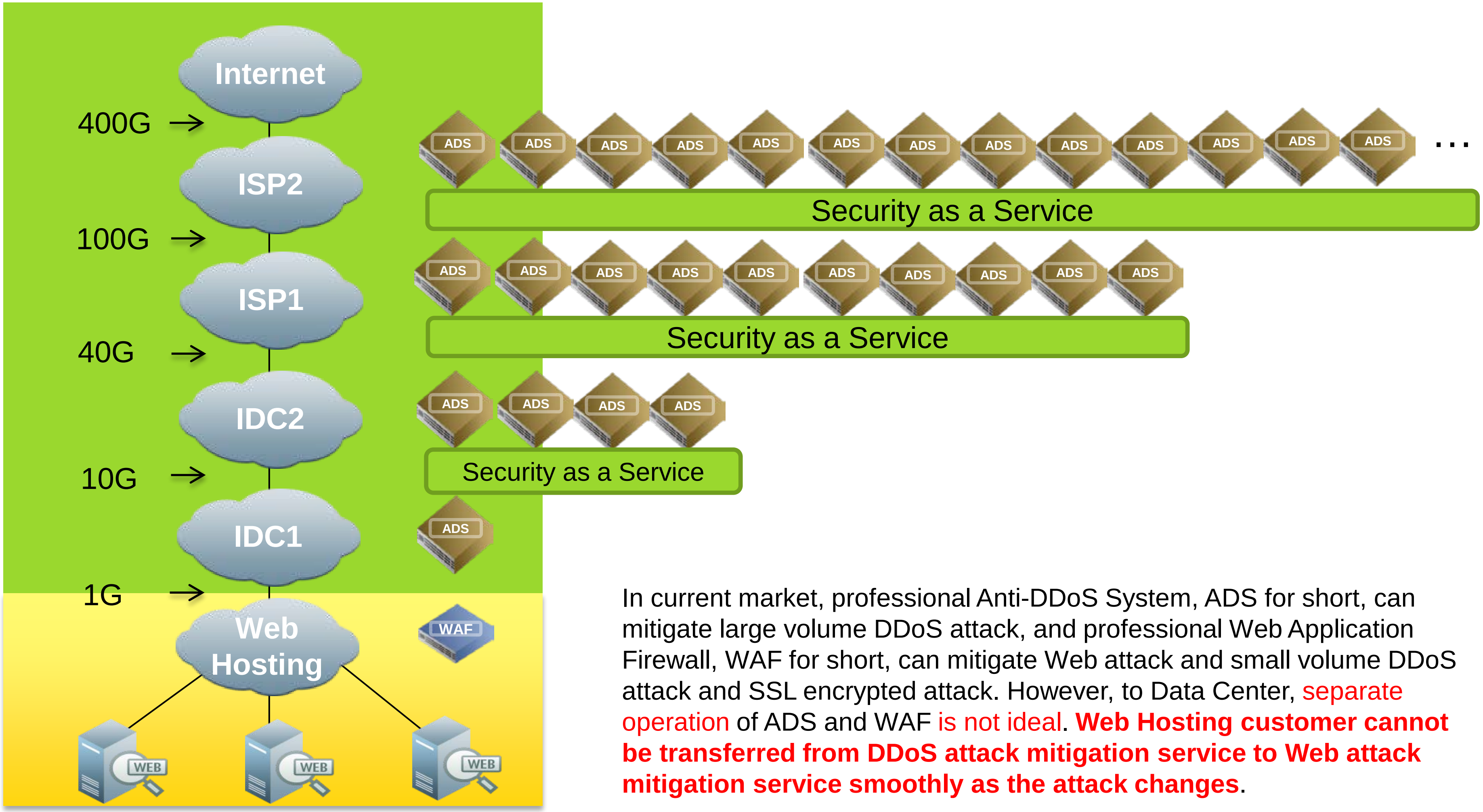
11. Behavior-Based Protection

- •Illegal File Upload
- •Illegal Download
- •Information Disclosure
- •Leech
- •CSRF
- •Scanning
- •Cookie Hijacking

12. Customized Protection Mechanism

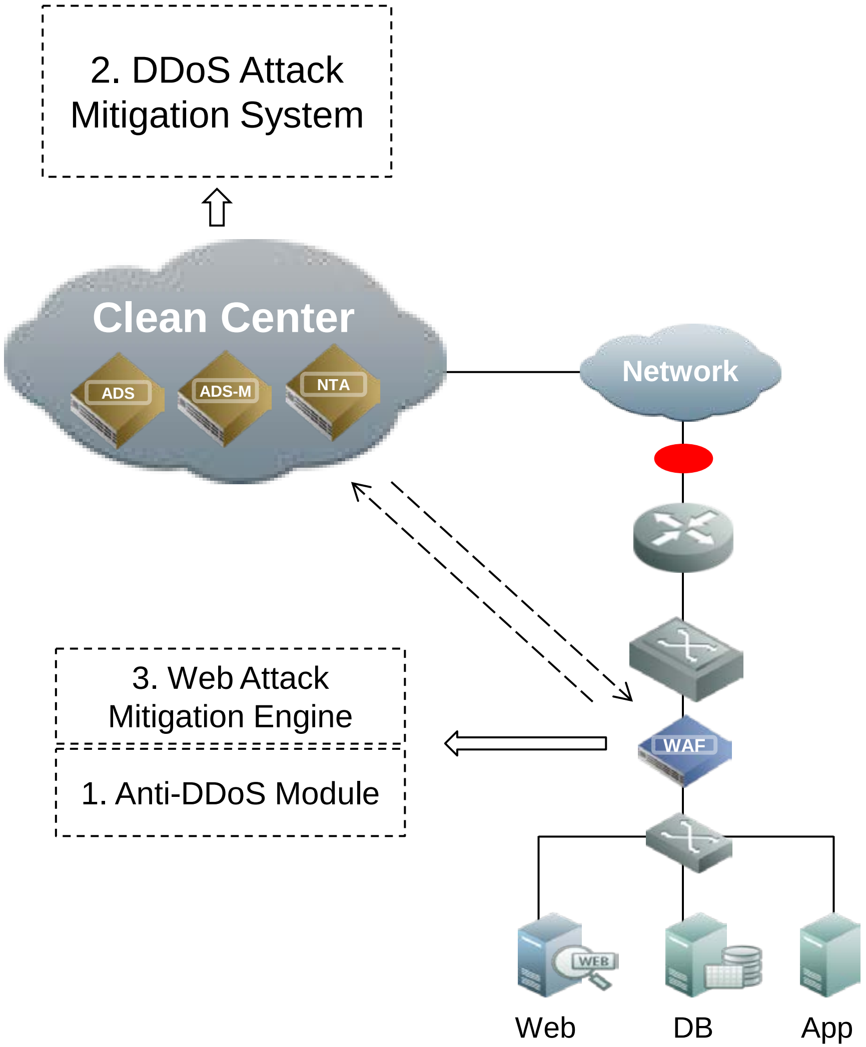
- •White List
- •Smart Patch
- •Custom Security
- •Exception Policy

Current Situation



In current market, professional Anti-DDoS System, ADS for short, can mitigate large volume DDoS attack, and professional Web Application Firewall, WAF for short, can mitigate Web attack and small volume DDoS attack and SSL encrypted attack. However, to Data Center, separate operation of ADS and WAF is not ideal. **Web Hosting customer cannot be transferred from DDoS attack mitigation service to Web attack mitigation service smoothly as the attack changes**.

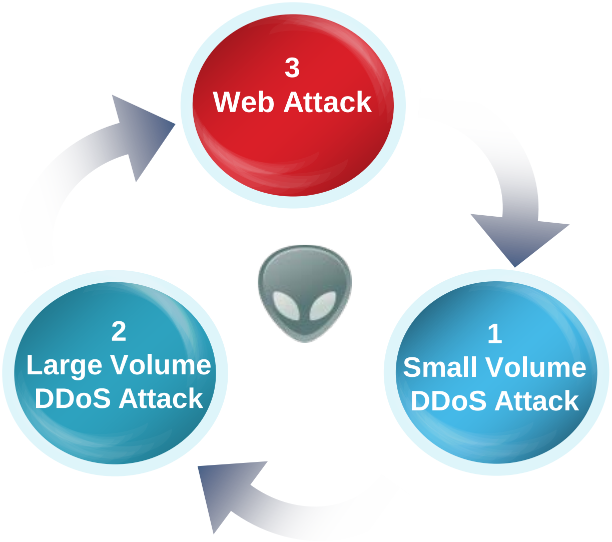
New System



2. DDoS Attack Mitigation System

3. Web Attack Mitigation Engine

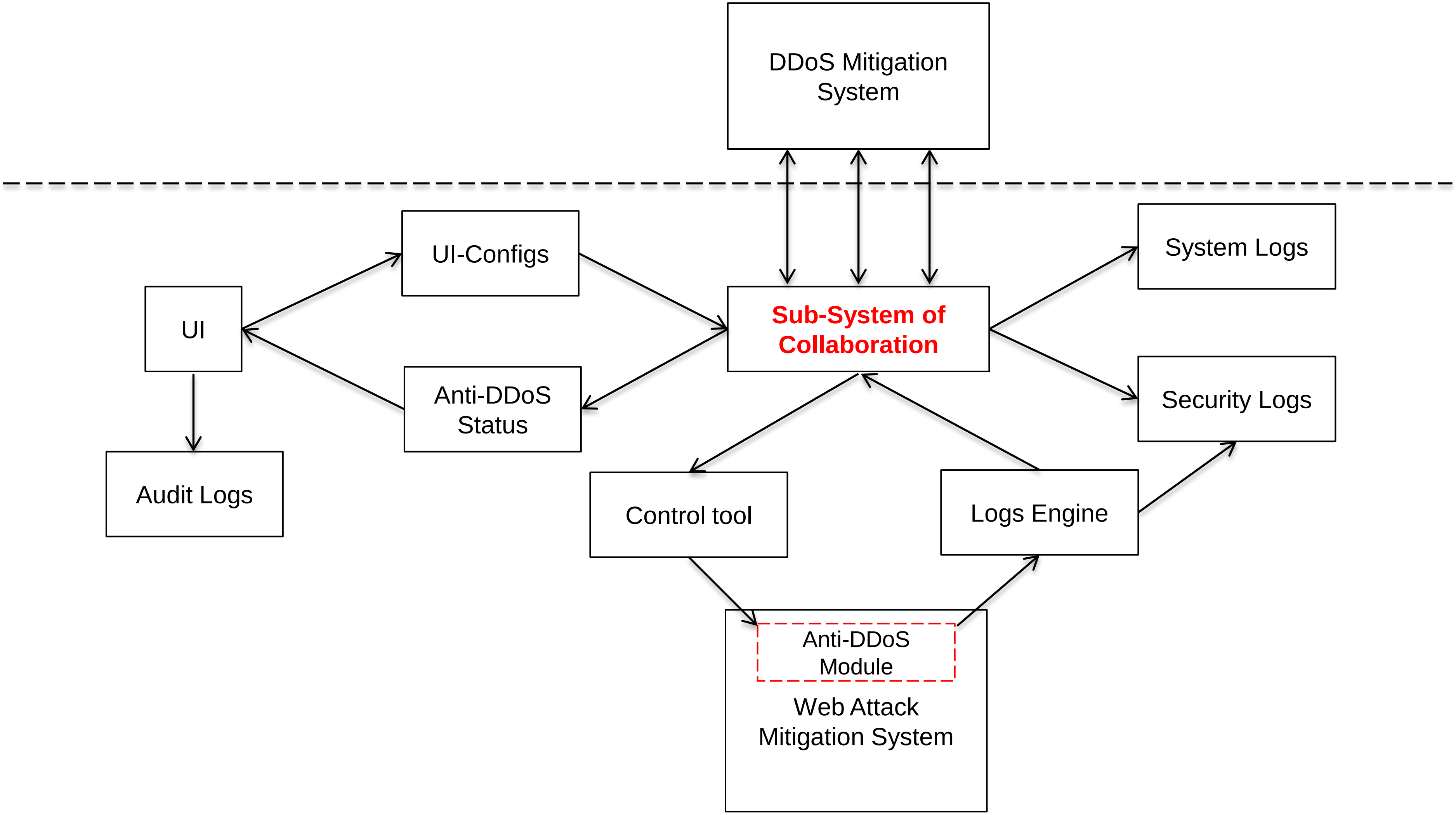
1. Anti-DDoS Module



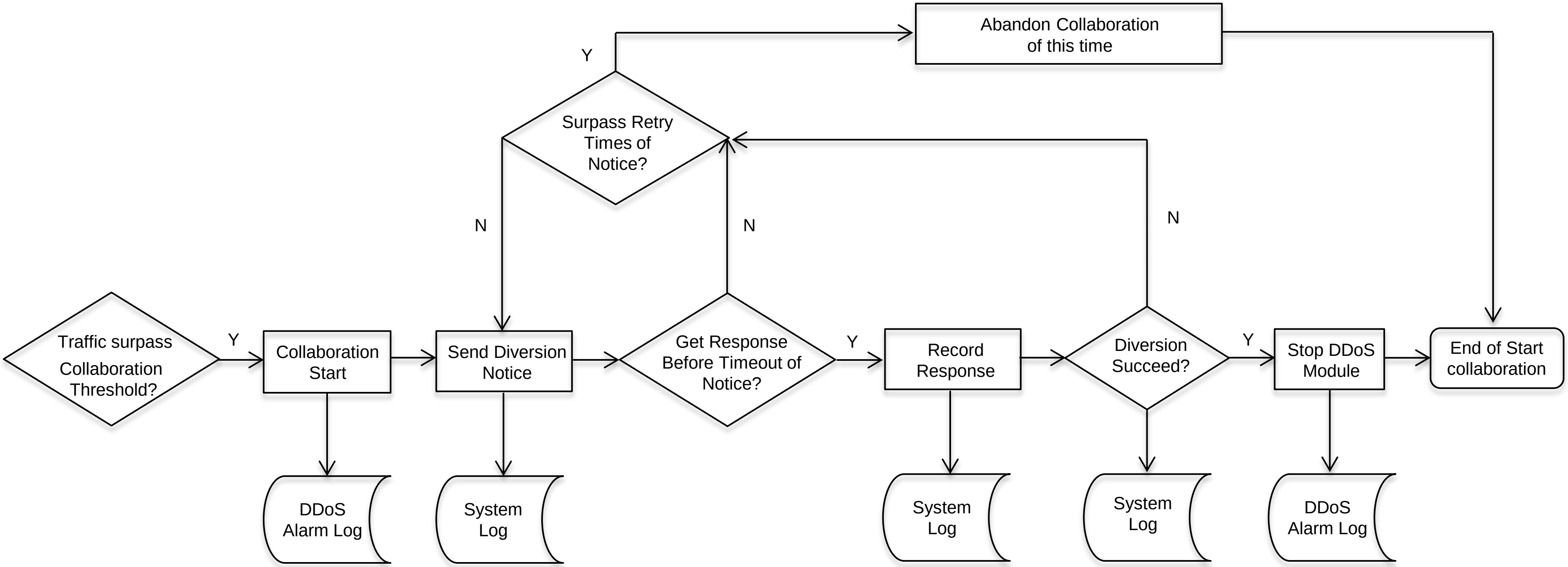
Benefits

1. Mitigate DDoS and Web Attack Simultaneously and accurately
2. Adaptability to Changes of attack
3. Cost-effectiveness

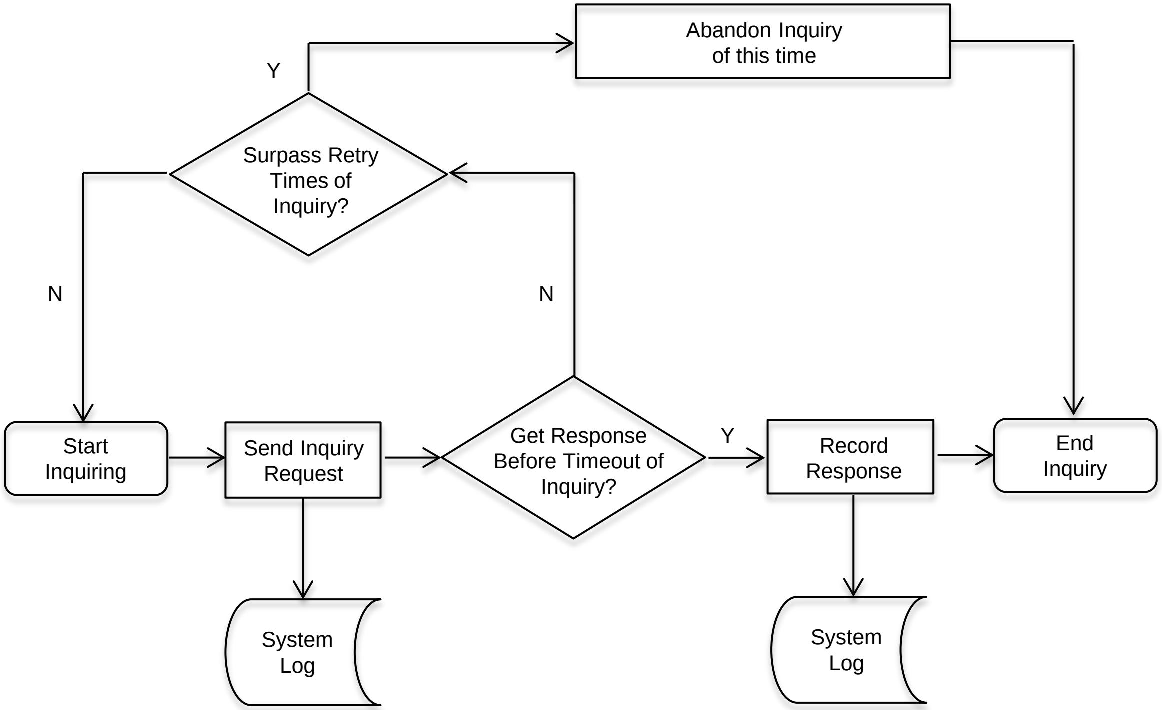
System Architecture



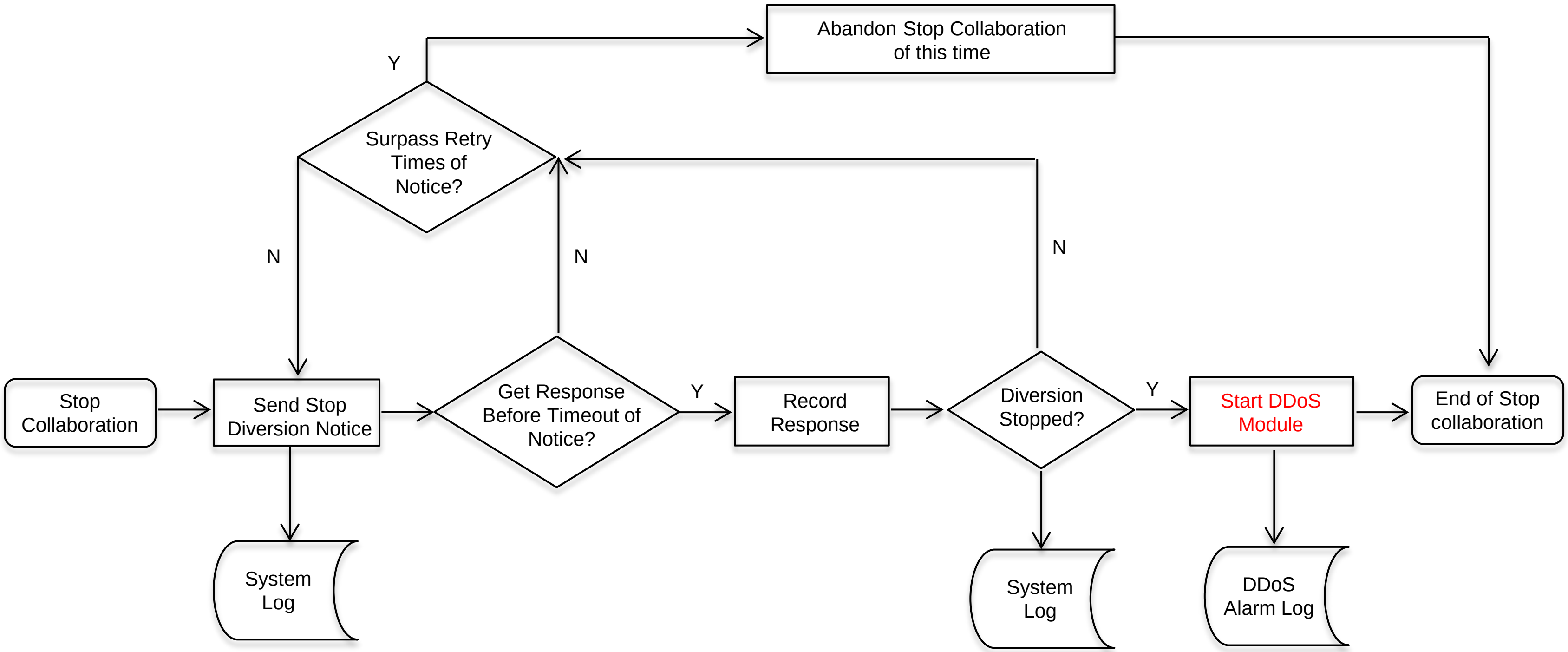
Process of Start Collaboration


Traffic surpass Collaboration Threshold?
Y
Collaboration Start
DDoS Alarm Log
Send Diversion Notice
System Log
Get Response Before Timeout of Notice?
N
Surpass Retry Times of Notice?
N
Y
Abandon Collaboration of this time
Y
Record Response
System Log
Diversion Succeed?
N
System Log
Y
Stop DDoS Module
DDoS Alarm Log
End of Start collaboration

Process of Traffic Inquiry


Abandon Inquiry of this time
Y
Surpass Retry Times of Inquiry?
N
N
Start Inquiring
Send Inquiry Request
Get Response Before Timeout of Inquiry?
Y
Record Response
End Inquiry
System Log
System Log

Process of Stop Collaboration



Abandon Stop Collaboration of this time

Y

Surpass Retry Times of Notice?

N

N

N

Stop Collaboration

Send Stop Diversion Notice

Get Response Before Timeout of Notice?

Y

Record Response

Diversion Stopped?

Y

Start DDoS Module

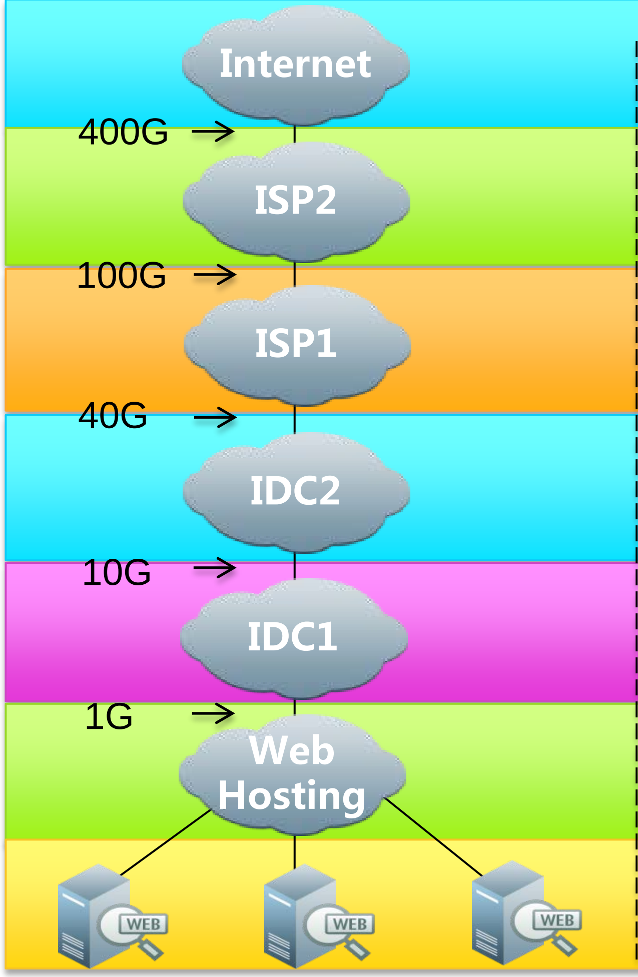
End of Stop collaboration

System Log

System Log

DDoS Alarm Log

Cost-effective? Probably…



	Web attack Mitigation	DDoS attack Mitigation	
		Equipment	Service
ISP2		16,000,000$ 400G ADS	40,000$ 400G/1 hour
ISP1		4,000,000$ 100G ADS	10,000$ 100G/1 hour
IDC2		1,600,000$ 40G ADS	4,000$ 40G/1 hour
IDC1		400,000$ 10G ADS	1,000$ 10G/1 hour
Web Hosting	60,000$ 1G WAF	40,000$ 1G Anti-DDoS Module	

- For instance, a customer meet consistent Web attack and 1, 10, 40, 100 and 400G DDoS Attack for 1 hour respectively.
- To completely defense, overall infrastructure investment is 22,100,000$.
- In new architecture, to the Web Hosting customer, it costs 155,000$ in total, and 55,000$ is service fee.

Summary

1. DDoS and Web Attacks are complicated and primary threats to Data Center.
2. Attackers will use both of these 2 attacks in one round of attack.
3. Current situation is separate operation of 2 kinds of attack mitigation system.
4. New System connects 2 existing attack mitigation systems together, and make security service can be transferred to different security service providers in network, as quick as attack changes.

Thank you!

Congyu Li