Security in knowledge

DEFENDING AGAINST LOW-BANDWIDTH, ASYMMETRIC DENIAL-OF-SERVICE ATTACKS

David W. Holmes (@dholmesf5)

F5 Networks

RSA CONFERENCE EUROPE 2013

Session ID: HT-R02

Session Classification: Intermediate

AGENDA

- Introduction
  - Why does this matter?
  - General Methods
- Asymmetric Taxonomy
  - Network
  - Session
  - Application
- Countermeasures
  - Strategic Defenses
  - Mitigation Architecture
- Conclusion

"In the last 18 months, 100% of customer DDoS engagements I've been involved with have had an asymmetric component." – Security Solution Architect, F5 Networks

Take advantage of the enemy's un-readiness, make your way by unexpected routes, and attack unguarded spots.

--Sun Tzu

Security in knowledge

#RSAC

RSA CONFERENCE EUROPE 2013

Why is it Asymmetric?

- Asymmetry in Resources

Attacker

Defender

Why is this Important?

- Famed US Patriot Hacker @Th3J35t3r (The Jester)
- Selling the laptop that he used to bring down WikiLeaks and many targets with asymmetric Attacks
- A single agent, with a single laptop…

- See paper written about the Jester – "The Jester Dynamic: A Lesson in Asymmetric Unmanaged Cyber Warfare"

Why is this Important?

- Case Study: Commander X

- Attacked Santa Cruz County webservers
- From a Starbucks just a few blocks away
- Arrested when he returned to same Starbucks
- Jumped bail, tried to hike to Canada
- Woken up by bear eating his laptop
- Eventually made it across border, where he now resides as a fugitive

- Source: Ars Technica – full story links.f5.com/14YnY11

Asymmetric Attacks vs. Hacking

DENY SERVICE

- Make site unavailable

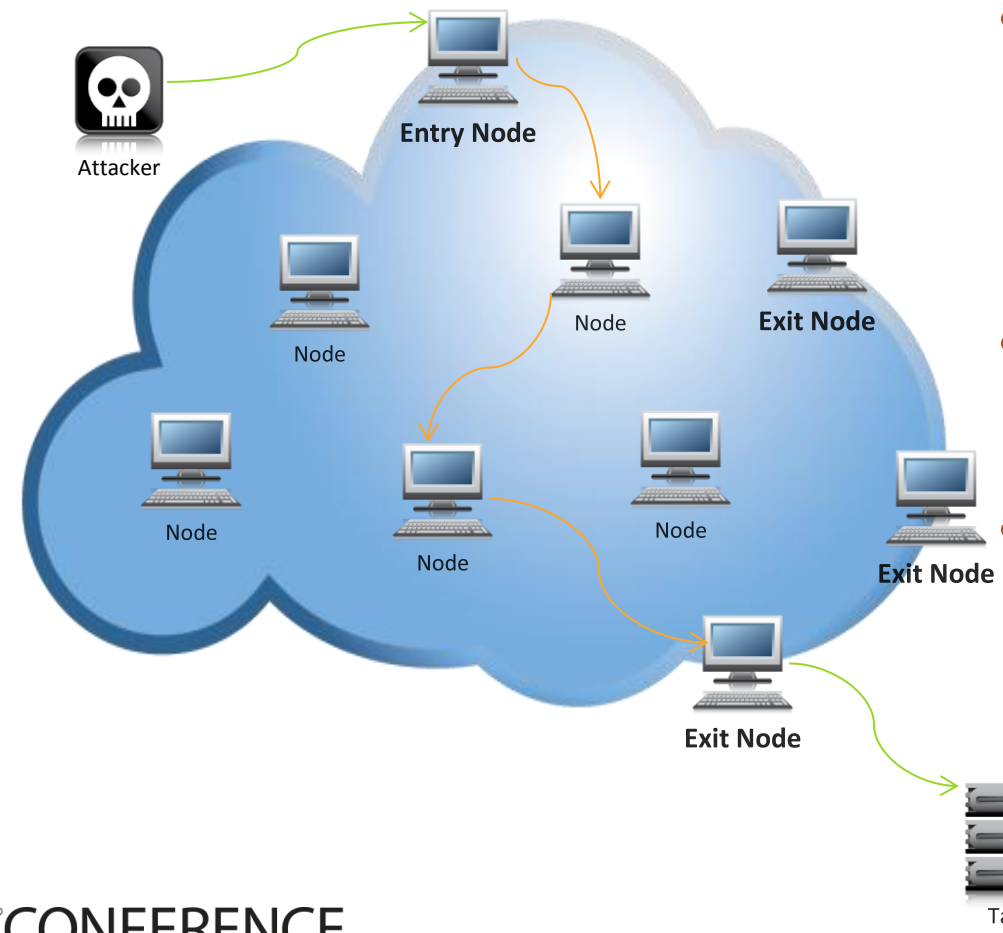
ACTION IN REAL-TIME

- Hacking may go on for months

STEALTH

- Asymmetric attacks avoid auto-detection

Masking Source IP



- Low-bandwidth attacks can go through TOR network.
- Can proxy via malware infection
- New: Rent cloud resources using stolen credit card numbers

Asymmetric Taxonomy

Security in knowledge

#RSAC

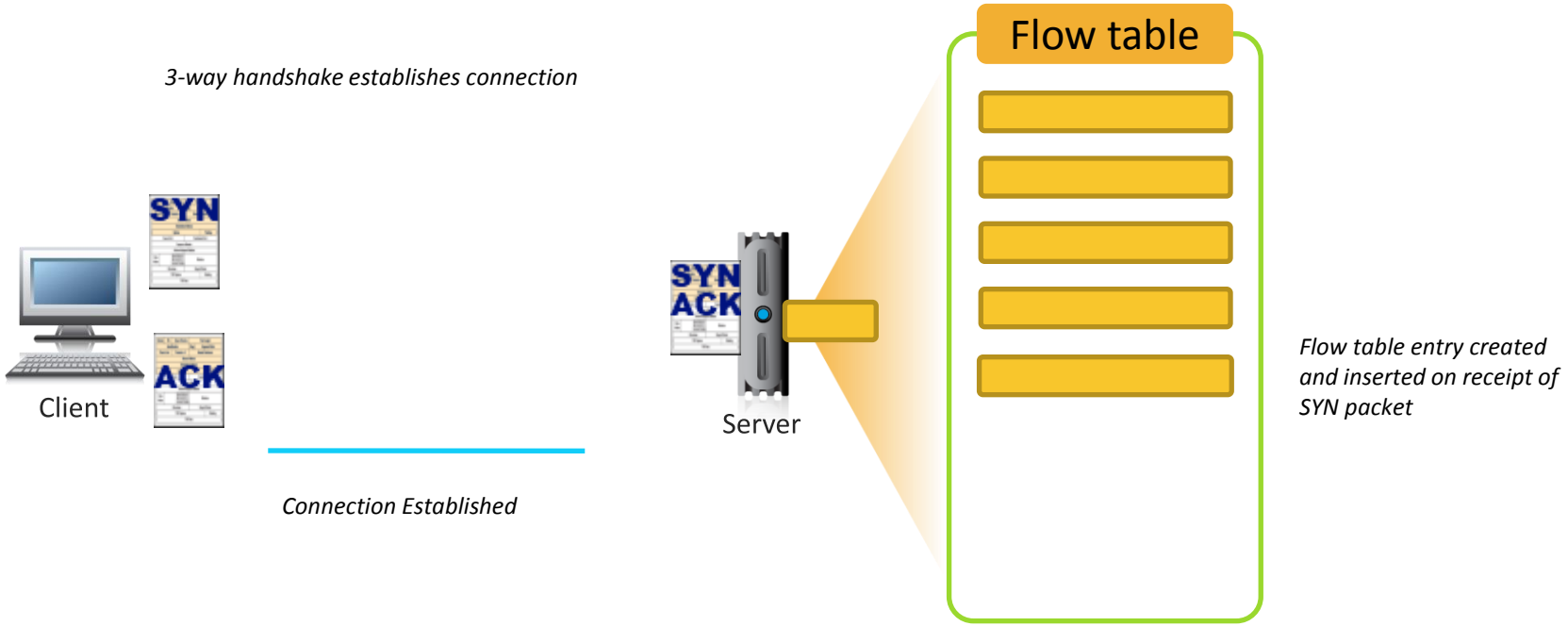
RSA CONFERENCE EUROPE 2013

Layer 4 –Asymmetric Network Attacks

Goal: Consume Connection Table

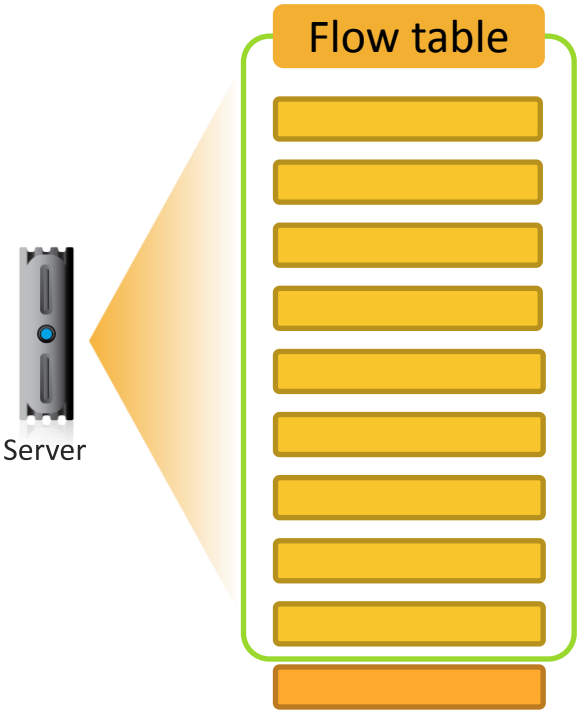
TCP SYN Flood	TCP Zero Window

Normal TCP Setup



SYN-Flood – Consume Session Table

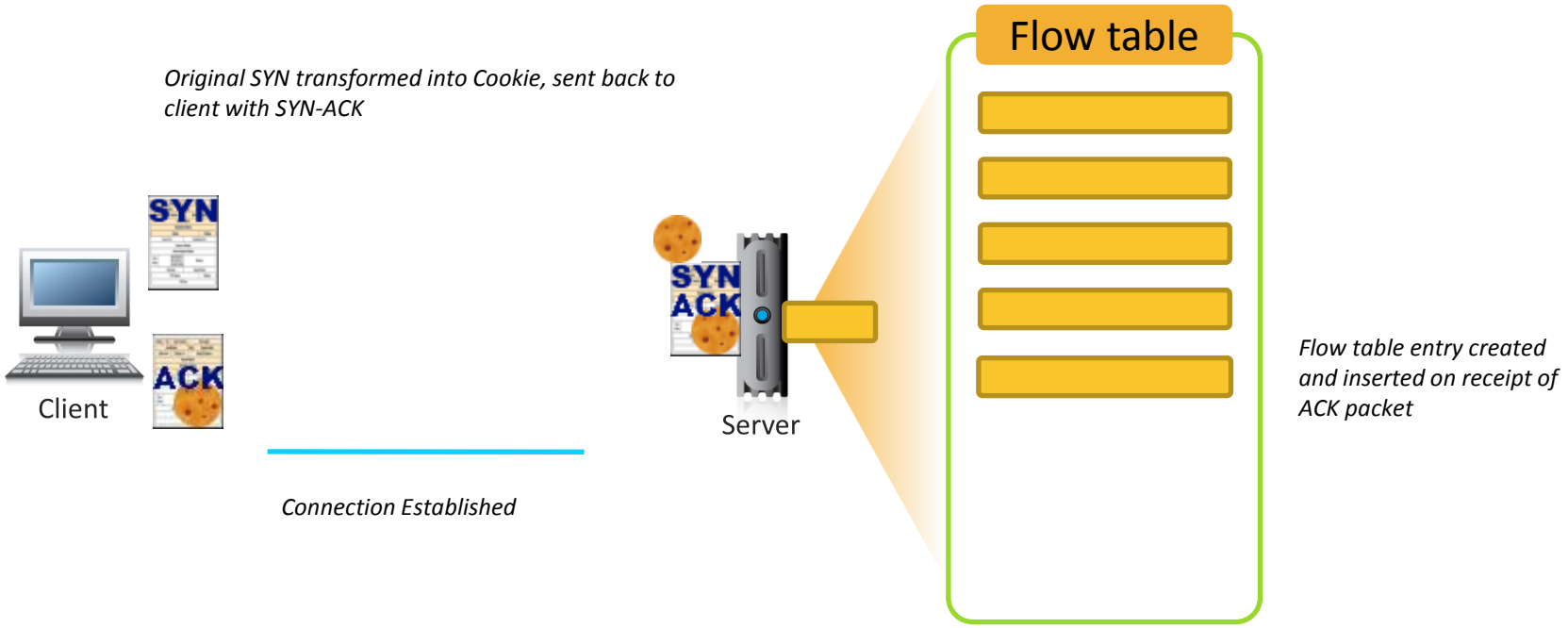
SYNs overflow flow table on server



Flow table entry created and inserted on receipt of SYN packet

Overflow! Denial of Service

Countermeasure – SYN-Cookies



Layer 4 –Asymmetric Network Attacks

Countermeasures

TCP SYN Flood	TCP Zero Window
SYN-Cookies (Not Syn-Cache)	Zero-Window Timeouts

Session Table Attacks

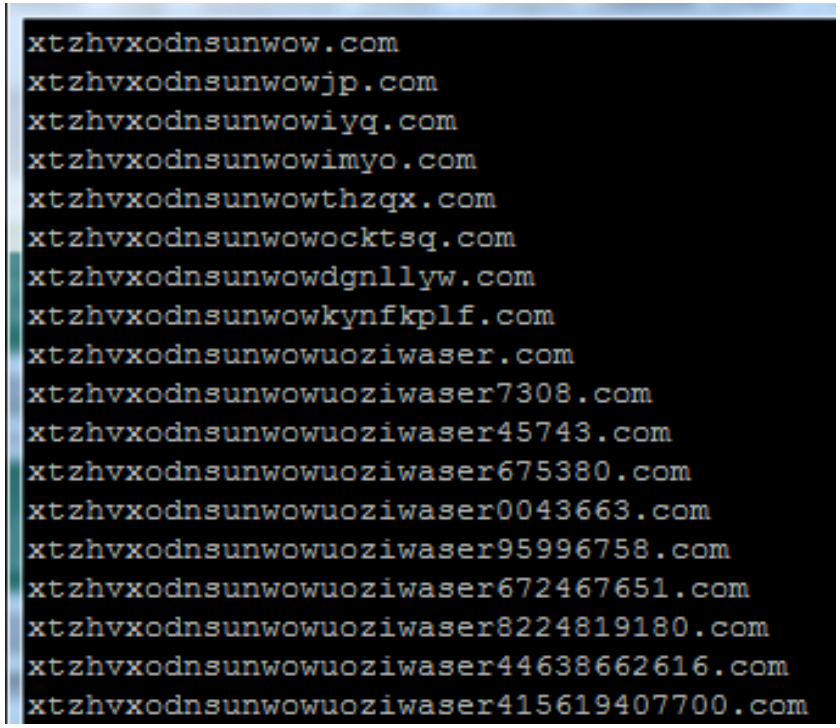
Goal: Consume Session Table

DNS NXDOMAIN Flood

SSL Renegotiation

DNS NXDOMAIN Attack

Querying Random Hostnames



Querying for randomly-generated non-existent hostnames

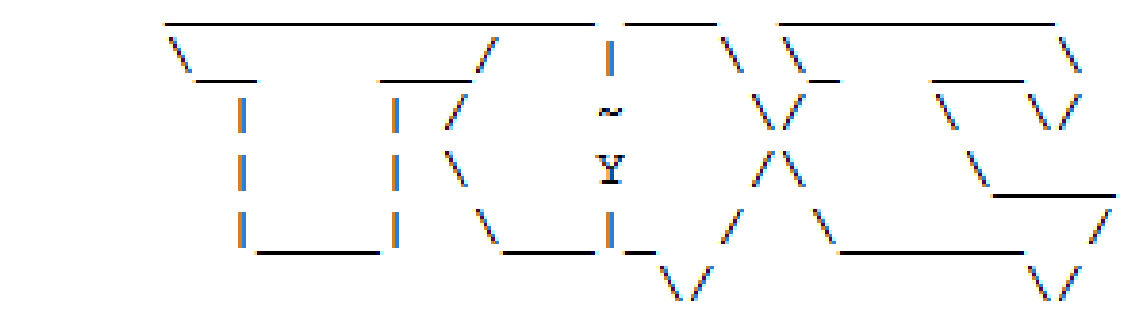
- Causes enormous work on DNS resolver
- Blows out DNS caches
- Easy to generate – single packets
- Easy to spoof source address – UDP

- Asymmetric
- Low-Bandwidth

SSL Renegotiation DoS

RSA public encrypt = 1/10 cost of decrypt

```
% ./src/thc-ssl-dos 30.1.1.134 443;
```



```
http://www.thc.org
           Twitter @hackerschoice
Greetingz: the french underground
Handshakes 0 [0.00 h/s], 1 Conn, 0 Err
Handshakes 417 [455.74 h/s], 37 Conn, 0 Err
Handshakes 924 [515.36 h/s], 52 Conn, 0 Err
Handshakes 1410 [486.44 h/s], 62 Conn, 0 Err
Handshakes 1916 [504.41 h/s], 71 Conn, 0 Err
...
```

Session Table Attacks

SOLUTIONS

DNS NXDOMAIN Flood

Overprovision

SSL Renegotiation

Easy Way: Disable this!

Layer 7+ Application Attacks

Goal: Attack Application Tier

SlowPOST

HTTP GET Flood

Web Application Firewall

Application Reconnaissance

Goal of the asymmetric warrior

- Obtain list of site URIs
- Sort by time-to-complete (CPU cost)
- Sort list by megabytes (Bandwidth)

Spiders for rent on Internet that will do this

- Though they are often known by security community
- Can be done with simple wget script

```
# wget –r –wait=1 -nv https://the.target.com
```

Network Reconn + HTTP Pipelining

GET /download/doc.pdf?121234234fgsefasdfl11 HTTP/1.1\r\n
Host: www.xxxxyyyyzzzz.com\r\n
User-Agent: Mozilla/4.0\r\n
Connection: keep-alive\r\n
GET /download/doc.pdf? qXs5udkLDd7DNG9ub HTTP/1.1\r\n
Host: www.xxxxyyyyzzzz.com\r\n
User-Agent: Mozilla/4.0\r\n
Connection: keep-alive\r\n
GET /download/doc.pdf?DLGgun1nEmfm5eid76 HTTP/1.1\r\n
Host: www.xxxxyyyyzzzz.com\r\n
User-Agent: Mozilla/4.0\r\n
Connection: keep-alive\r\n
GET /download/doc.pdf? 6ndfTygZPImXsNW22a HTTP/1.1\r\n
Host: www.xxxxyyyyzzzz.com\r\n
User-Agent: Mozilla/4.0\r\n
Connection: keep-alive\r\n

Randomized Query Parameters
Avoid Cache Defenses

Countermeasures

Security in knowledge

#RSAC

RSA CONFERENCE EUROPE 2013

What Doesn't Work?

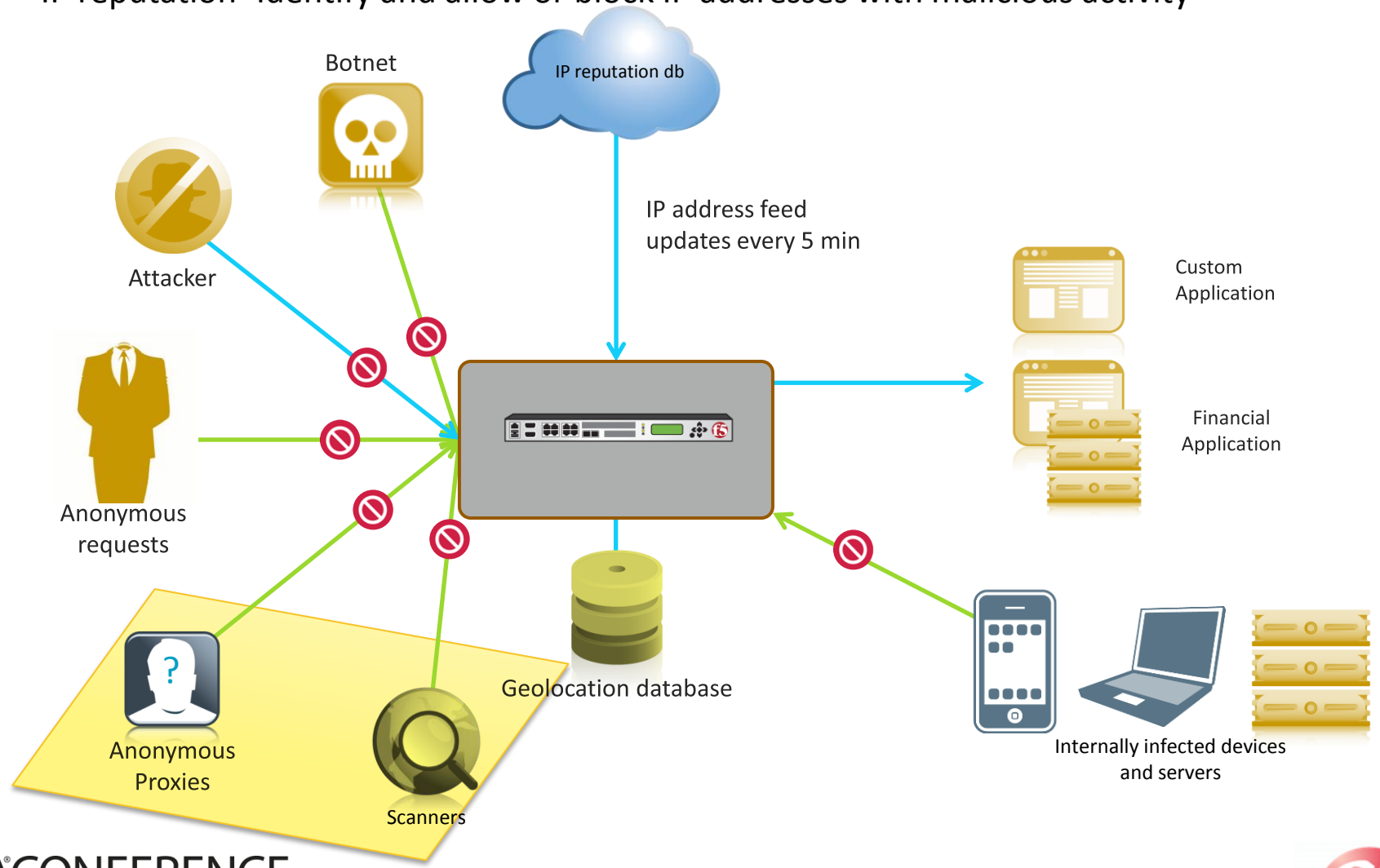
Defensive Technology	Protection Profile	Notes
Conventional Firewall	Weak	At least you can block IPs
Content Delivery Network	Moderate	Asymmetric attackers know to evade. No SSL. Not right use case.
Anti-DDoS Scrubbers	Weak	
Service Provider Anti-DDoS	Weak	
IDS/IPS	Moderate	A good asymmetric attack will not set off IDS.

Countermeasure Table

Attack	Countermeasure	Locate Defense
SYN-Flood	SYN-Cookies	Firewall
Zero-Length TCP Window	Signature or Full Proxy	Firewall
DNS NXDOMAIN	Authoritative Resolver	DMZ
SSL Renegotiation	Cryptographic Offload	ADC
HashDos	Signature or Patch	ADC or Server
Slowloris / Slow POST	Full Proxy	ADC, WAF
Pipelining	Disallow pipelining	
Apache Killer	Signature or Patch	ADC or Server
ReDos	?	?

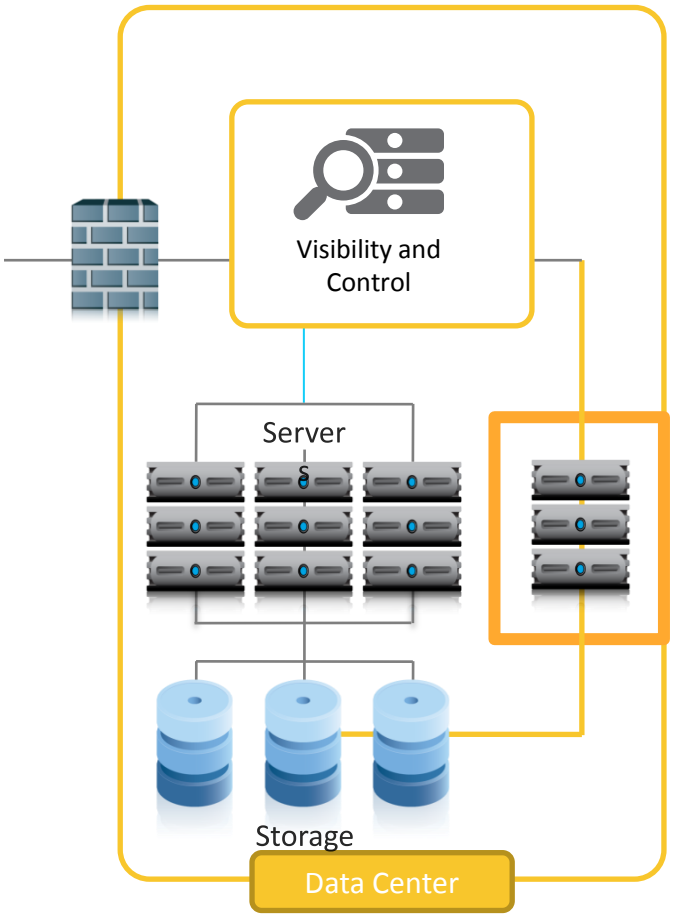
Use Case - Mitigate Network Recon

IP reputation- Identify and allow or block IP addresses with malicious activity



Hardened Hot-Site with Login-Wall

Temporarily reduce Layer 7 attack surface



Activated during DDoS Attack

- No **Unauthenticated** Requests
- No HTTP – Only HTTPS
- No Search Feature
- No Store Locator
- Real users maintain most of the normal site functionality during attack

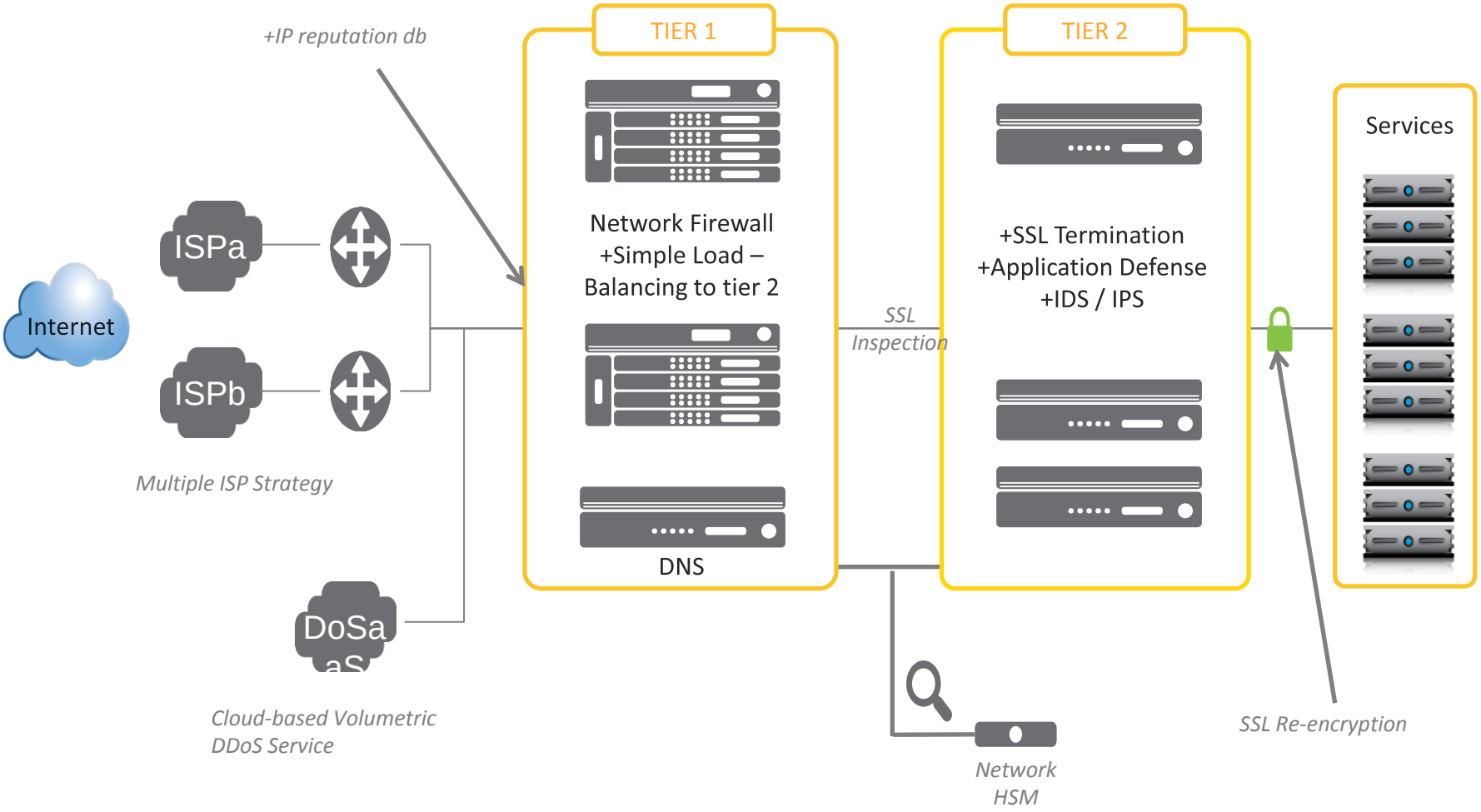
Other L7 Options

If you can't extend your perimeter to only known users…

- CAPTCHA
- JavaScript Redirect

But what about these guys?

Multi-tier DDoS Mitigation Architecture



On Your Own with Asymmetric DDoS

Plan

- Determine your risk profile
  - Talk to your marketing people, they know site metrics!
  - Spider your own site
  - You can start with wget, use a script to parse the data.
- Think Asymmetric!

Execute

- Develop a Asymmetric Attack DoS Playbook
  - Practice it!
- Need a set of TURING tests that you can enable
  - CAPTCHA
  - Authentication
  - Javascript Redirects

Security in knowledge

Thank you!

David Holmes

F5 Networks

@dholmesf5

d.holmes@f5.com

http://links.f5.com/1aojbrH