RSA CONFERENCE 2014
ASIA PACIFIC & JAPAN

Share.
Learn.
Secure.

Capitalizing on
Collective Intelligence

Revenge of the Full Proxy

SESSION ID: SPO-W05

Edwin Seo

Security Architect, APJ
F5 Networks
@F5NetworksAPJ

(C) 20th Century Fox, 2005

"In the time of greatest despair, a child shall be born
who will destroy the Sith and bring balance to the Force…"

History of the Full Proxy

Too many Protocols
to support:
IP, SNA, IPX, Appletalk
…

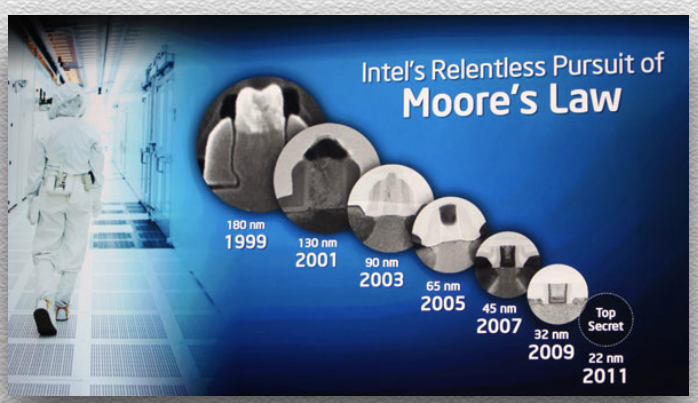
CPUs were Slow…
Not able to keep up.

FireWall ToolKit
1st Oct 1993

Most secure, but
change in
protocol not trivial…

Fast FPGAs
Not as smart, but could
process packets faster

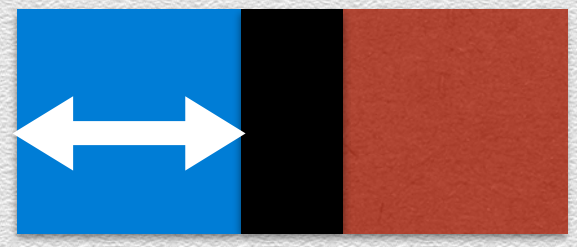
Come the New Millennium and beyond…



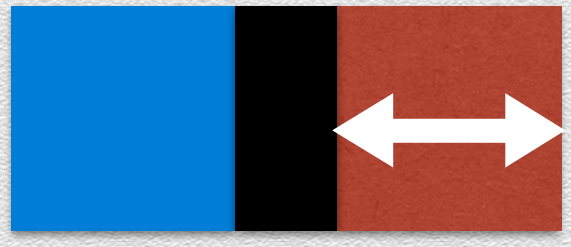
Moore's Law
CPUs are getting faster,
smaller, with higher performance

Major Protocol Convergence
TCP, DNS, HTTP, SSL

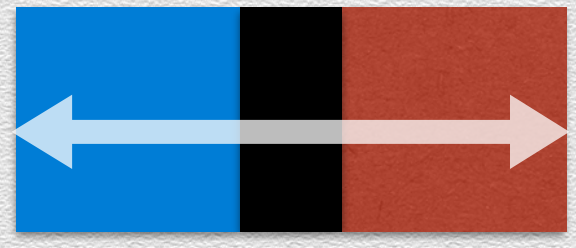
Many Technologies Out There…



1. Reverse Proxy



2. Forward Proxy



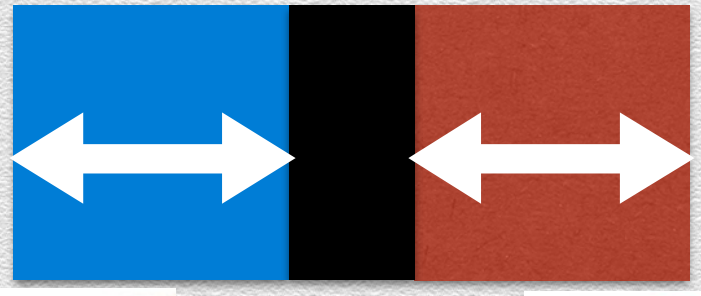
3. Transparent Bridge

4. Offline / Port Span

The Full Proxy

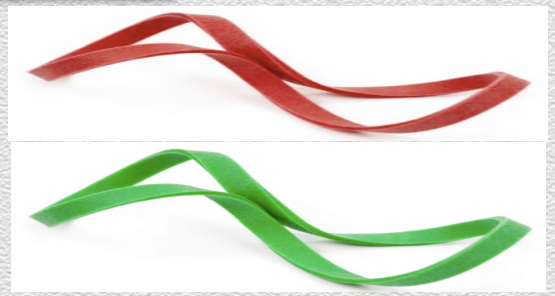
Outside
"Untrusted"

Inside
"Trusted"



Multiple
Individual
Connections

Translation
Distribution
Manipulation
Optimisation



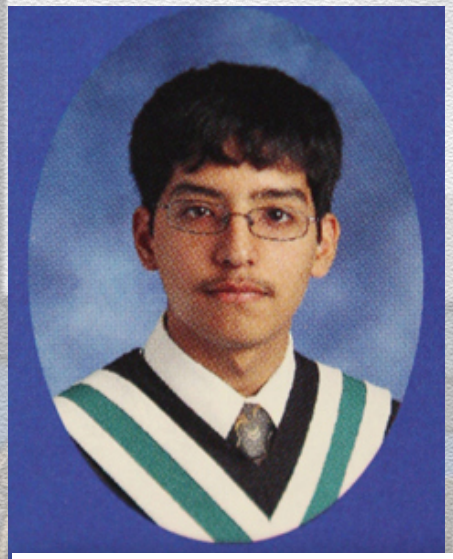
Reusable
Fewer
Connections

Security Air Gap

So how does this "Air Gap" Help?

HeartBleed


7 April 2014
U.S. CYBER COMMAND
NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE



Mail Online

First Heartbleed hack arrest: 19-year-old Canadian student charged with stealing taxpayer data

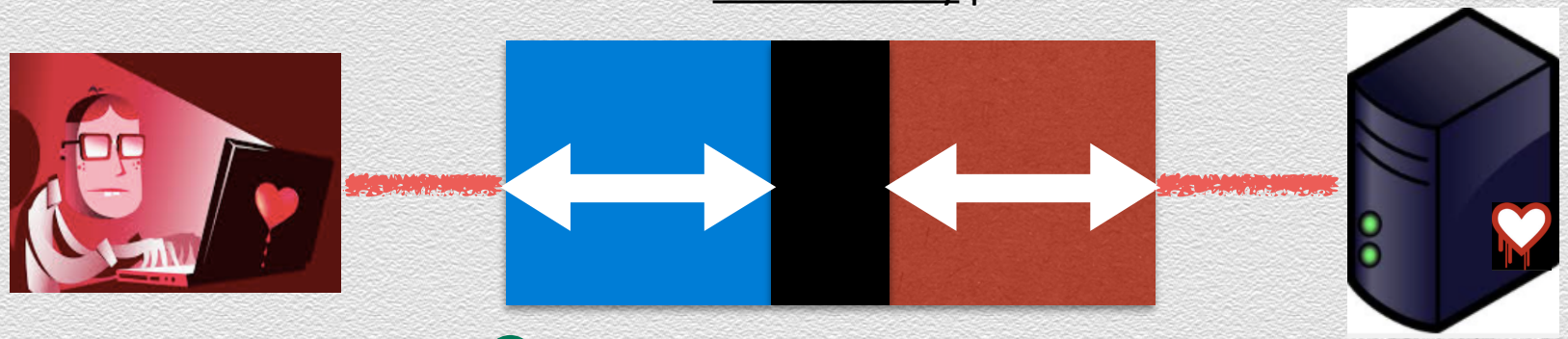
- Suspect is student Stephen Arthuro Solis-Reyes from London, Ontario
- He is accused of lifting 900 social security numbers from government site
- Police seized his computer and a court appearance will take place July 17
- Mumsnet is also thought to have been targeted by Heartbleed hackers
- Other affected sites include Google, Facebook, Yahoo and Netflix
- Problem was found last week in the widely-used OpenSSL software
- Security firms are urging users to only change passwords on sites that have confirmed they are safe

By ELLIE ZOLFAGHARIFARD and VICTORIA WOOLLASTON

PUBLISHED: 11:11 GMT, 17 April 2014 | **UPDATED:** 15:52 GMT, 17 April 2014

Mitigating Heartbleed

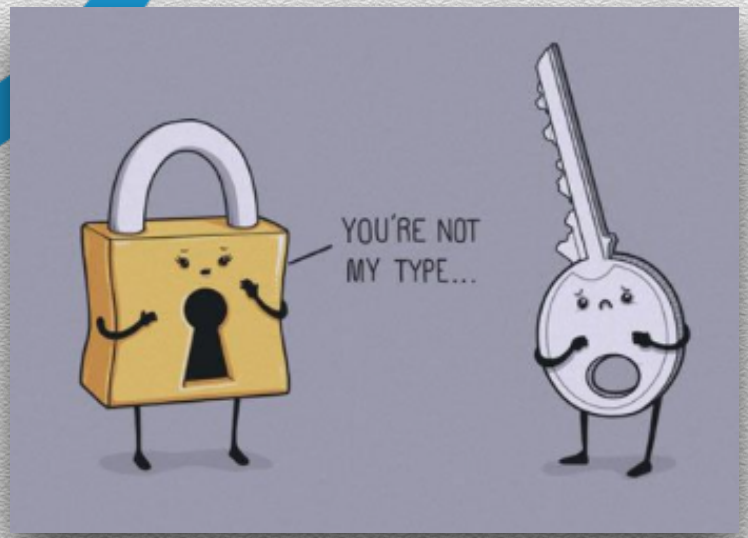
1. If Full Proxy is terminating SSL on behalf of server, and if the Full Proxy is not vulnerable, servers are automatically protected.



2. If Full Proxy is not terminating SSL on behalf of server, then:

A. Check for Heartbeat request from client and terminate.

B. Check for unusually long Heartbeat response by server and terminate.

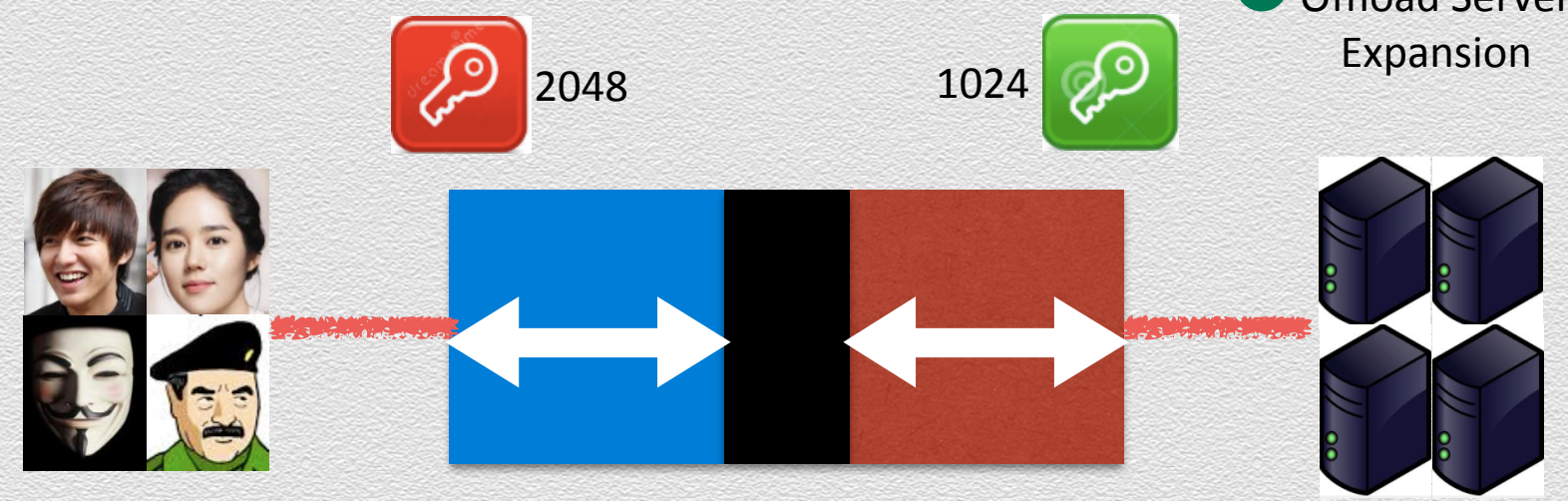


SSL

SSL Protection

1 More secure key lengths on “Untrusted” networks

2 Offload Server Expansion



5 Mitigate SSL / TLS Encrypted attacks

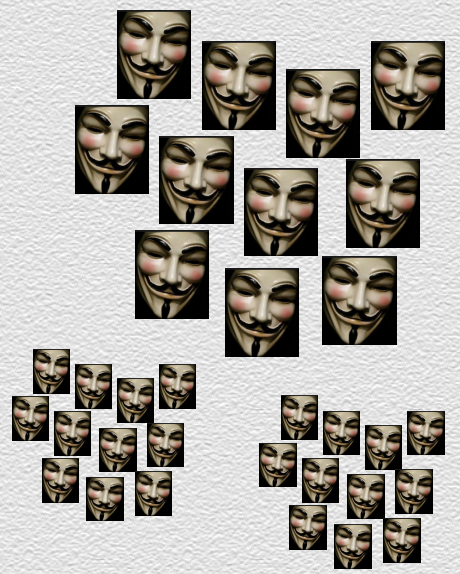
4 Mitigate SSL Protocol attacks
- Handshaking
- Re-negotiation
- RFC compliance

3 Centralised Secure Key Management

Layer 3/4 DDoS

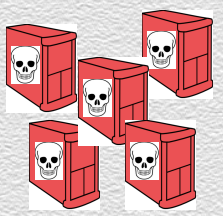
The Flooders

Anonymous & Friends



L3/4 Floods
TCP/UDP/ICMP

L7 Floods
HTTP GETS /
DNS Queries



Compromised
Servers

Open DNS /
Unpatched NTP Servers

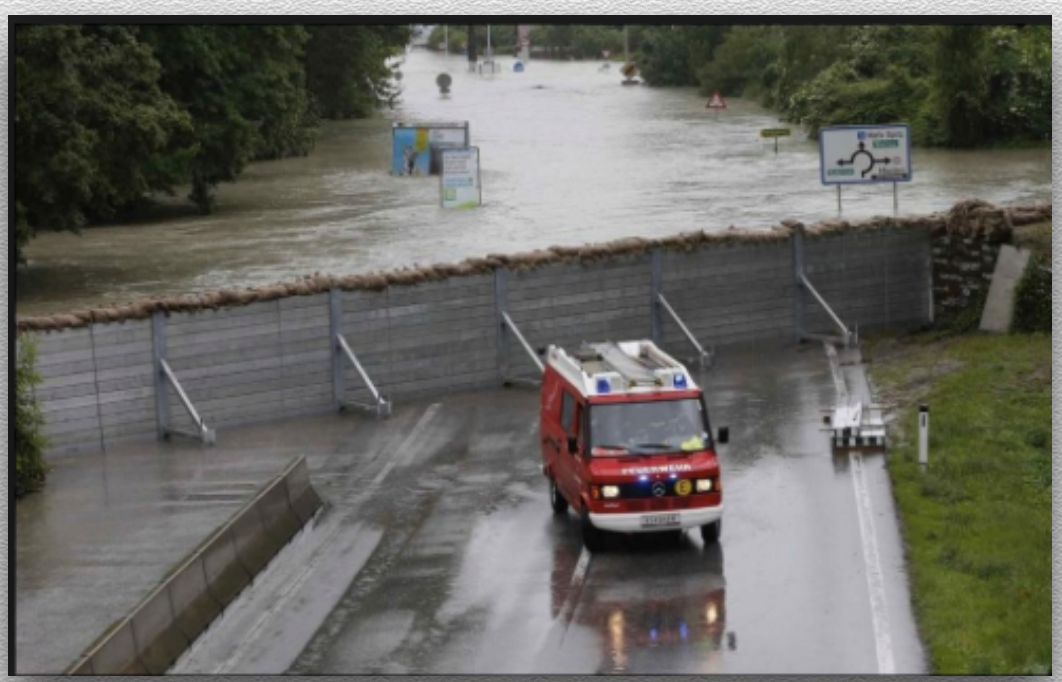
Reflective
Amplifiers
DNS/NTP

Flood Protection - Many different methods

H/W SYN Cookies
for Anti-Spoofing

Huge Connection Tables /
High CPS

L3/4 DOS vector threshold
Baselining / Learning



DNS Attack
Absorption

Connection
Rate Limiting

Default
Deny policies

HTTP / DNS / SIP
Protocol
Conformance

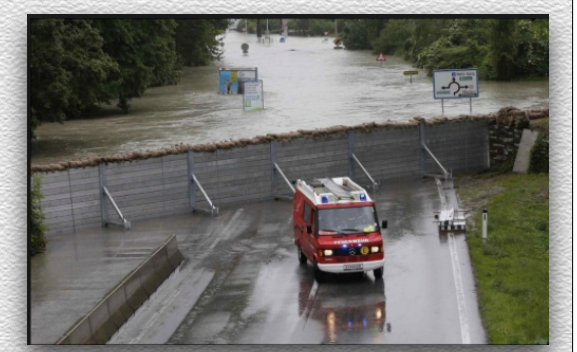
Brute Force
Login /
Dictionary attacks

HTTP / DNS / SIP
Method Whitelisting

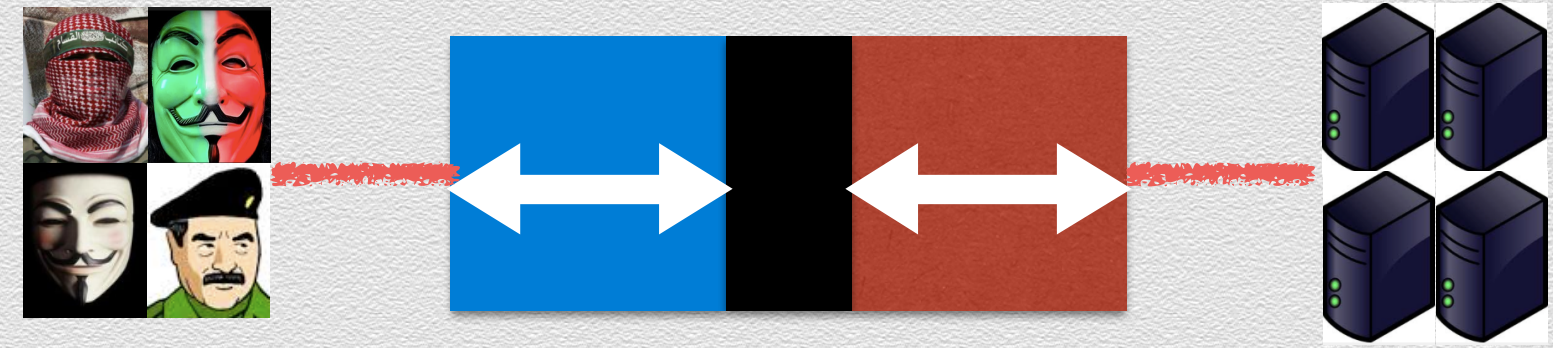
DNS Truncate
Challenge

HTTP URI TPS
Baselining / Learning

Flood Protection
Full Proxy perspective…



1 Server Response <-> Perform Rate Limiting / Blocking



4 Buffering or Absorption : Connection / DNS Query / HTTP

3 Protocol Compliance Checks

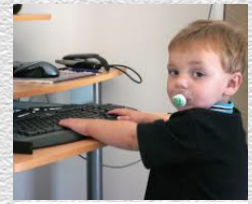
2 Server Health Checks <-> Activate countermeasures (e.g. SYN Cookies, DNS Truncate)

Layer 7 DDoS

The Exploiters

Asymmetric
Heavy URL Requests

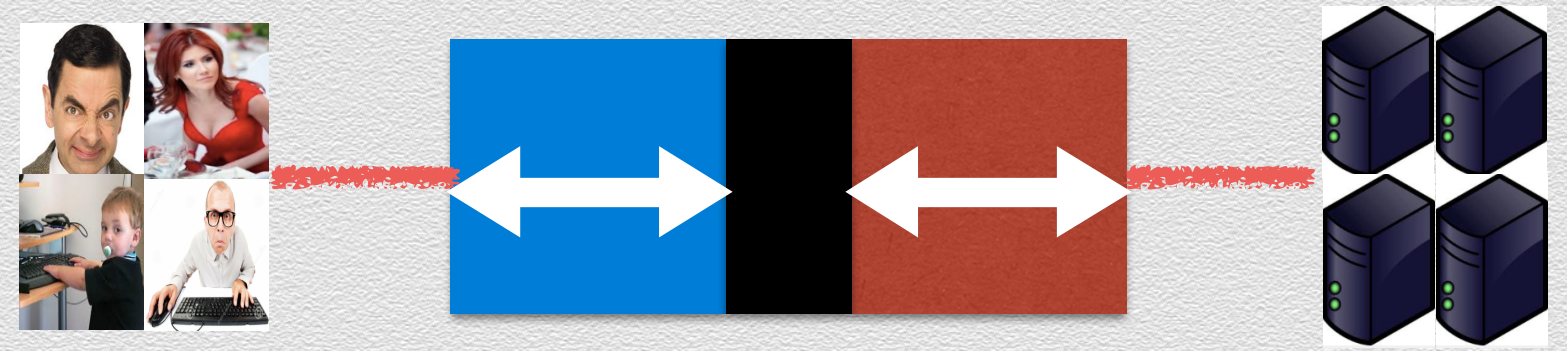
Server Workload Exploits
Expensive Searches /
DB Queries /
HashDoS



SSL Exploits
Handshaking /
Renegotiation

Defending against the Exploiters

1. Server-Side / DB Health Checks
2. Tracking HTTP Response Size



5. Baselining URL requests/sec
4. "Non-Human" Botnet Checks
3. Step-Up Authentication protection

RSA CONFERENCE 2014
ASIA PACIFIC & JAPAN

Web Applications

The Ninjas

Middlemen
MITM / MITB

Injection
SQL / OS / RFI / LFI

Poisoning & Tampering
Cookie / DNS

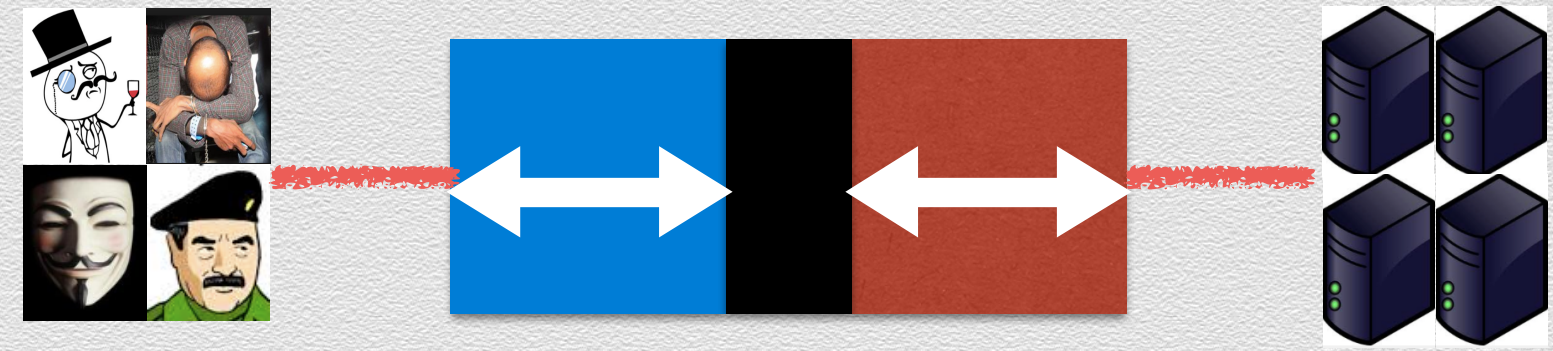
Lulzsec &
Friends

Web Vulnerabilities Exploits
XSS / CSRF / Workflow /
Traversals

Defending against the Shurikens

1. Tightening
   - Parameter
   - Workflow

2. Web Application-Specific Signatures



5. Cookie / Token / JavaScript Injections
   E.g. CSRF protection

4. DAST scanner
   Cyclic-Integration,
   Virtual Patching
   "Buying time"

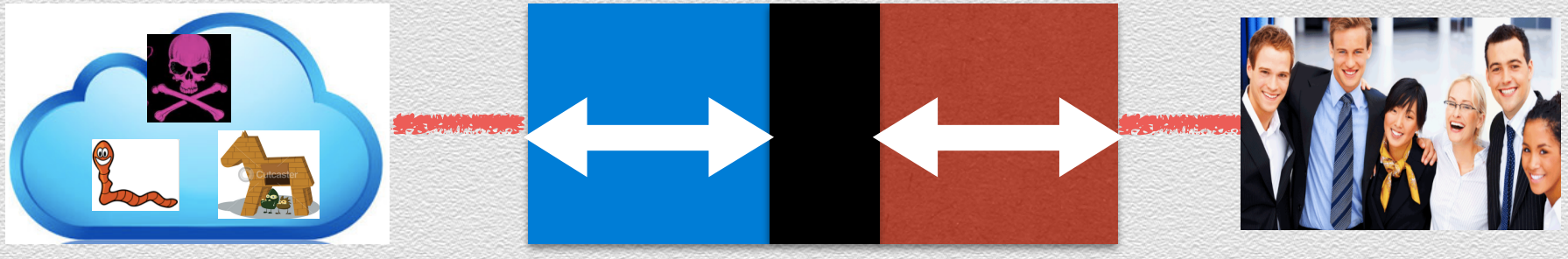
3. Masking Sensitive Response Data

RSA CONFERENCE 2014
ASIA PACIFIC & JAPAN

Secure Web GateWays

Secure Web Gateways

1. Malicious Website Visit prevention
2. PCI-Compliance for CDEs



5. Embedded Content Scanning e.g. Images / Files
4. SSL Forward Proxy / Inspection
3. URL Filtering for Corporate AUP

Enumeration

Know your enemy and know yourself
and you can fight a hundred battles without disaster.
- Sun Tzu
知彼知己，百戰不殆
－孙子

Dealing with Enumeration

Nmap

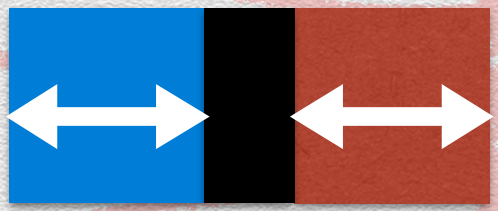
Metaspoilt
F/W

Recon-NG
F/W

Netcraft

O/S Versions

Web Server Type
& Versions



Response
Headers

Error
Responses

Known SQLi &
XSS Vulnerabilities

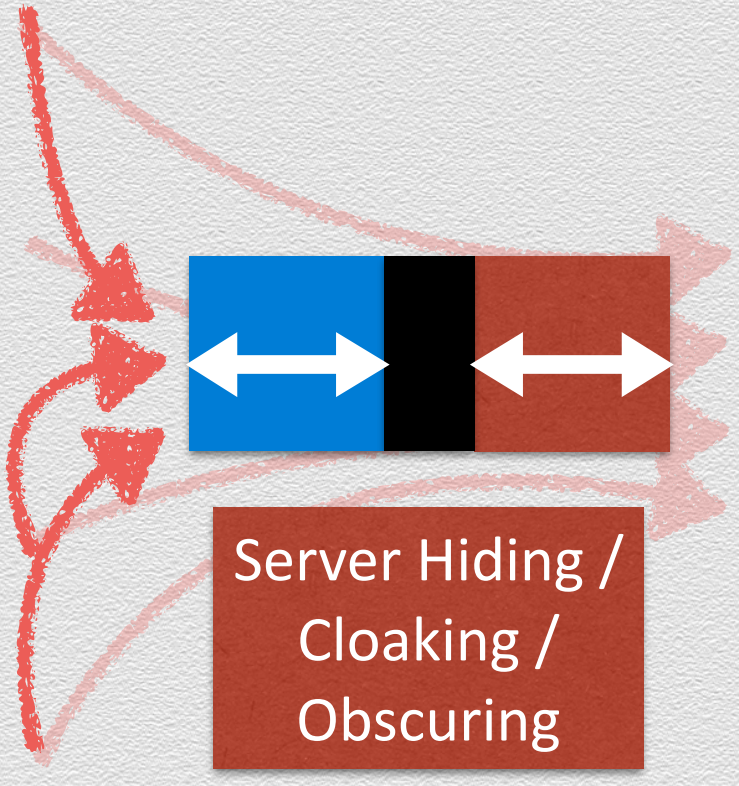
Dealing with Enumeration

Nmap

Metaspoilt F/W

Recon-NG F/W

Netcraft



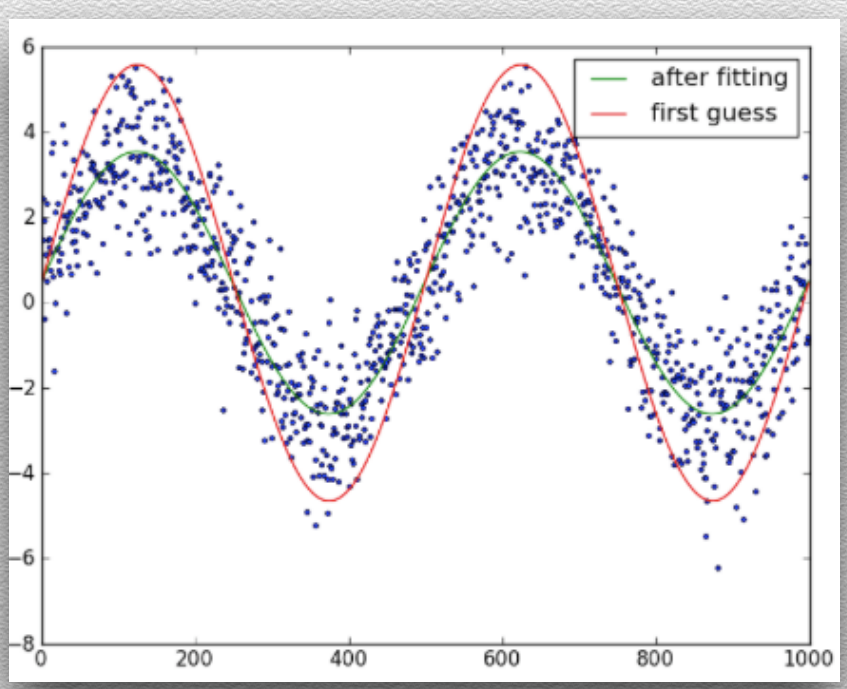
Optimization

"The Internet is a terribly
Un-optimized environment…"

Normalising the Not-so-Normal

TCP Protocol
is Lossy!

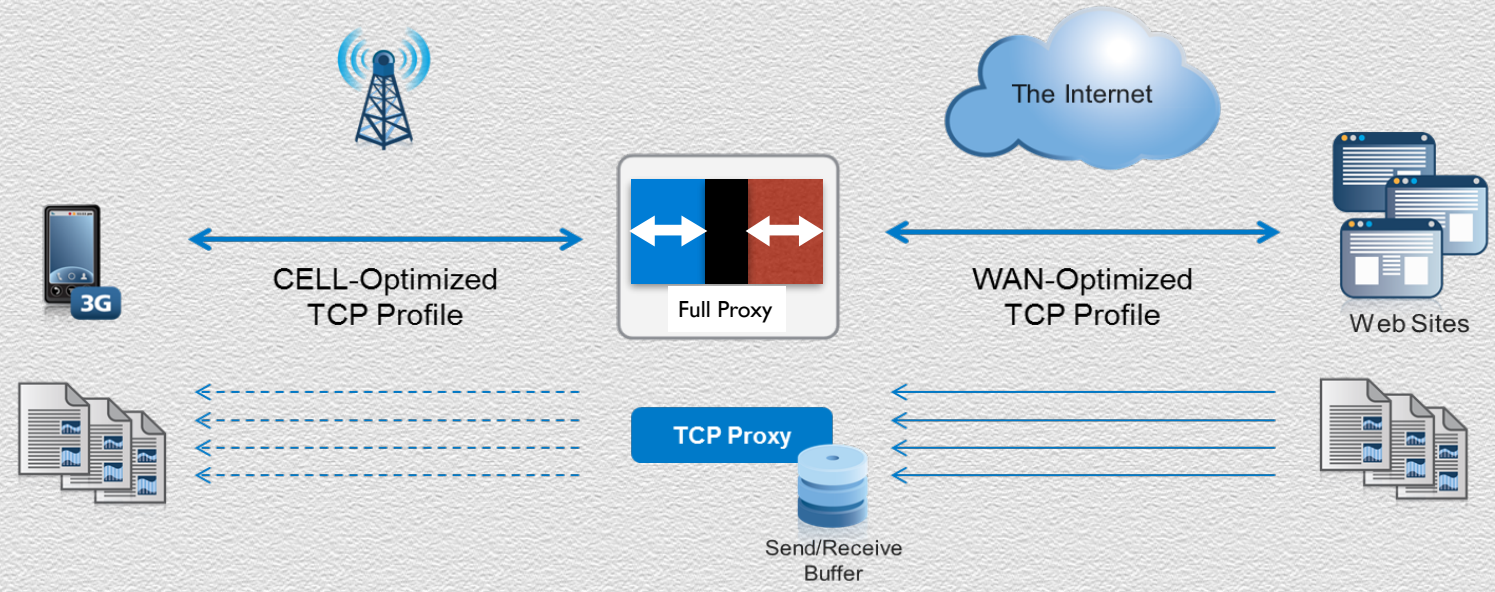
Mobile Networks
vs.
Fixed Networks

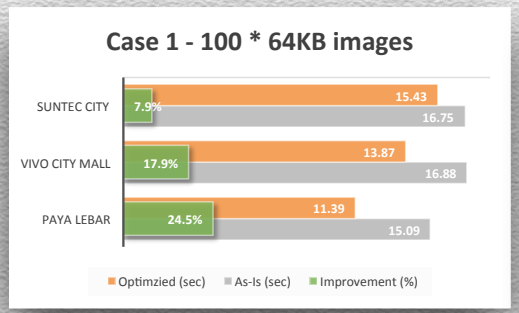


Protocol
RFC Compliance
HTTP / DNS / SIP

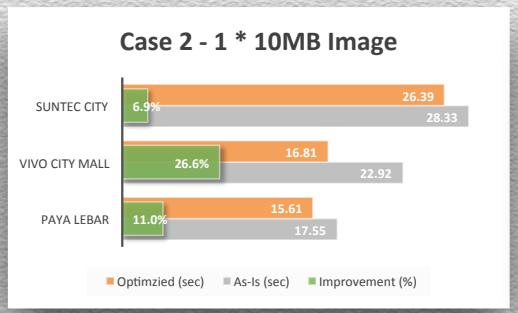
SSL Handshaking /
Cipher Support /
Compliance

How a Full Proxy helps

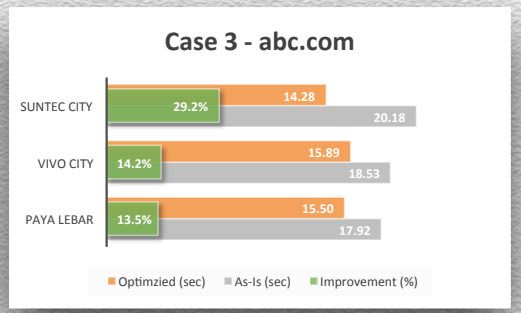




7.9% - 24.5% ▲



6.9% - 26.6% ▲



13.5% - 29.2% ▲

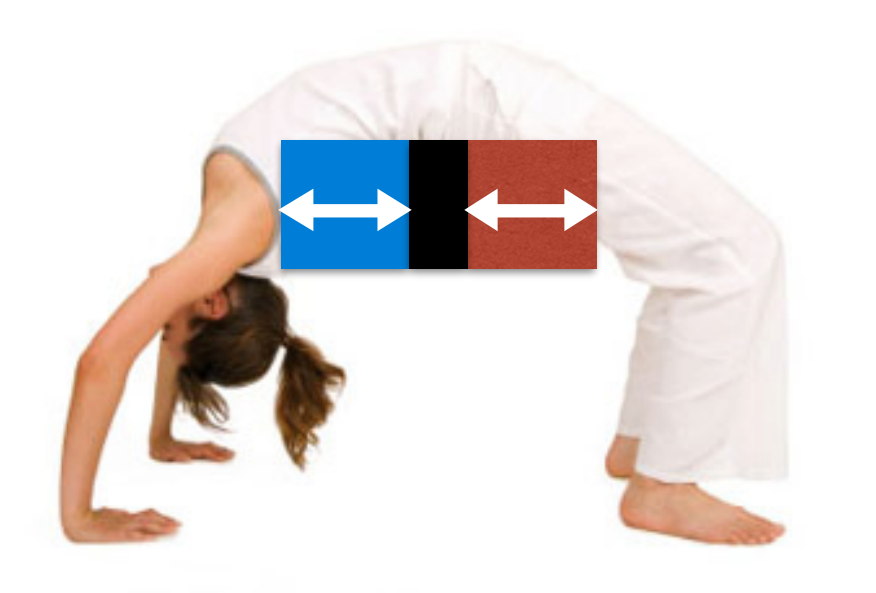
Traffic Manipulation

CAPTCHA Injection

HTTP Cookie Injection

Deliberate Delay Injection

JavaScript Injection



Selective Redirects

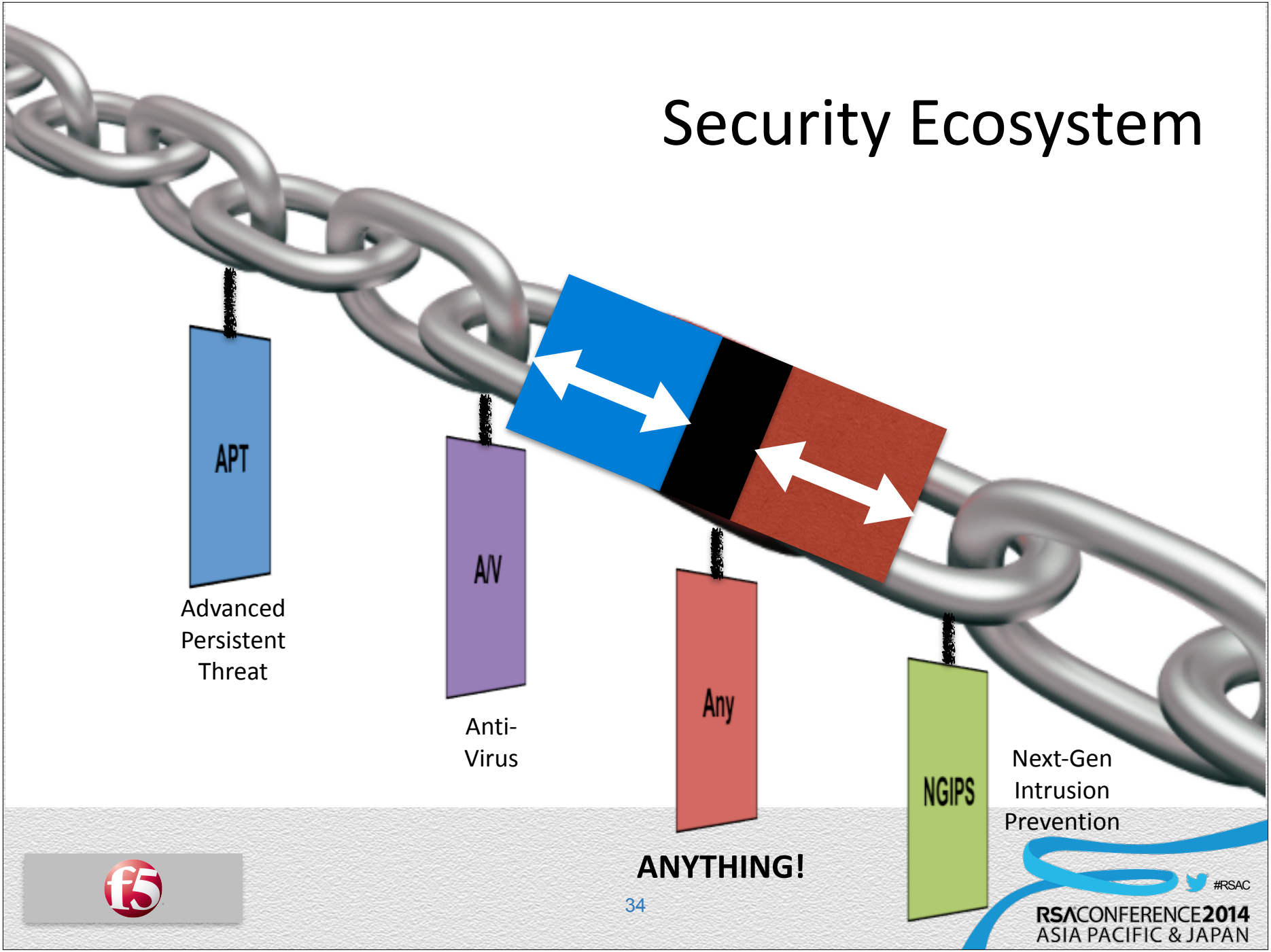
Token Injection

Browser Fingerprinting

Ability to programatically modify
***Any parameter in data path**
based on certain conditions

Service Chaining

Security Ecosystem



Advanced Persistent Threat

Anti-Virus

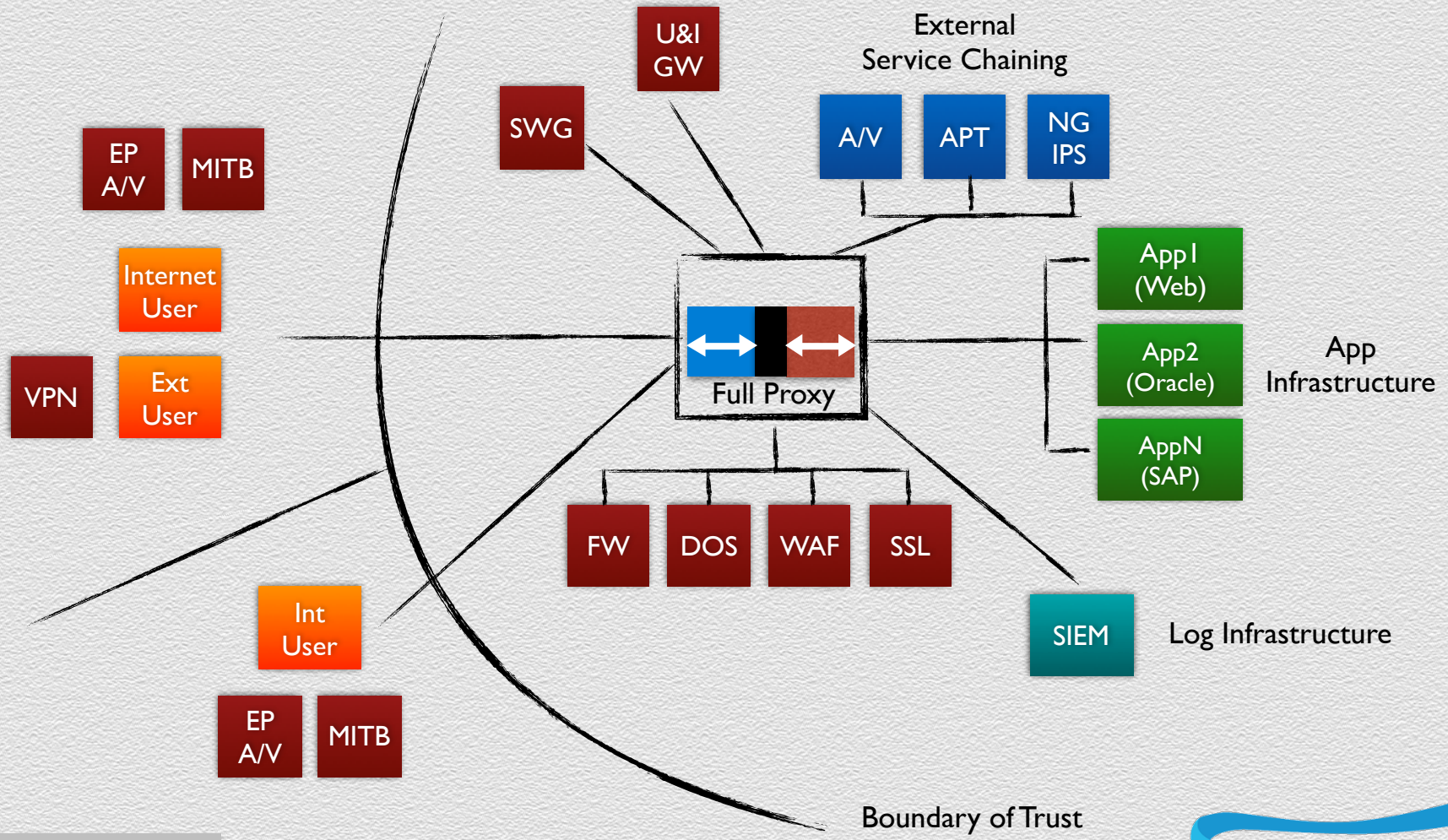
ANYTHING!

Next-Gen Intrusion Prevention

RSA CONFERENCE 2014
ASIA PACIFIC & JAPAN

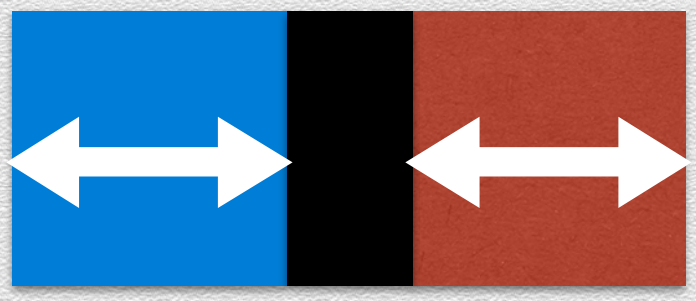
NG DataCenter Architecture

Bird's Eye View



Will Vader be the one who will bring balance back to the Force?

Will the Full Proxy be the Solution to ALL Security threats?



Absolutely NOT!

Web Application Protection

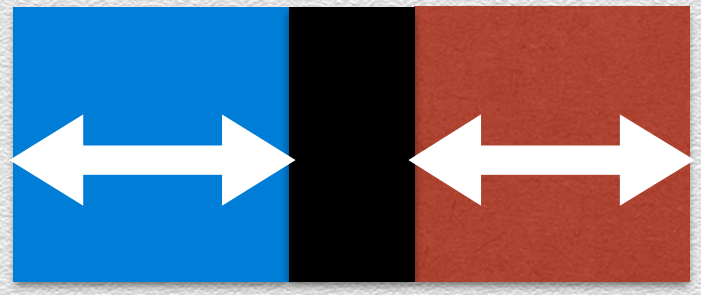
Layer 7 DDoS

Layer 3/4 DDoS

SSL

HeartBleed

Secure Web Gateway



Enumeration

Optimization

Traffic Manipulation

Service Chaining

It can Absolutely Help Enhance Security in the Modern Data-Center with the Air Gap!

Booth G8

Exciting Demos

(L3-L7 Threat Protection & Anti-Fraud Prevention)

Great Prizes

RSA CONFERENCE 2014
ASIA PACIFIC & JAPAN

Share.
Learn.
Secure.

Capitalizing on
Collective Intelligence

Thank You

Edwin Seo
Regional Security Architect, APJ
e.seo@f5.com