Anonymous: Tools of the Trade and Lessons Learned

Bill Church
Systems Engineer – Federal
bill@f5.com

IT agility. Your way.

Agenda

- Anonymous Background
- Evolution of Denial of Service
- DDoS Examples and Strategies for Mitigation
- Practical Strategy for Datacenter Security

Anonymous Background

Evolution of DDoS

3 Classes of DDoS Attack

3DOS

Request Flooding

- Each attack session issues requests at an increased rate as compared to a non-attacking session

Asymmetric Workload

- Attacker sends requests that are more taxing for the application than the client.
- Traffic volume remains low; detection is difficult

Repeated One-Shot

- Attacker sends single Asymmetric workload request, then closes. Attack is highly distributed to generate required power.
- Most challenging type of attack to detect and mitigate.

DoS Attacks Overview (known)

Simple

- HTTP, HTTPS, ICMP, SYN Floods, UDP Floods, DNS Request Floods, etc
- Lower layer DoS attacks target ISP connections / bandwidth
- **Defendable by proxies and SYN Cookies feature of TMOS**

Complex

- Layer-7 DDoS attacks targets HTTP, HTTPS, SOAP, XML and DNS services
- Typically targets server resources
- Not easily detectable, more efficient, less resources and harder to trace
- Defendable by features found in Application Security Manager (ASM)

DDoS Attacks Evolution

Current

- Reflection and amplification (including DNS recursion)
- Larger botnets & autonomous propagation
- Botnet markets which are increasingly sophisticated in nature
- Peer-to-peer botnets
- Botnets using encrypted communications
- Attacks against government infrastructure for political purposes
- Use of DoS by organized crime
- Increasing sophistication of malware and malware packaging

DDoS Attacks Evolution

Future

- Attacks on emerging technologies
- Application layer DoS
- Realistic behavior of DoS traffic (further difficulty in detection)
- Attacks against anti-DoS infrastructure
- Attacks against SCADA systems
- Attacks against shared infrastructure and the ‘cloud’
- Cloud to Cloud

Attacks are Moving “Up the Stack”

Network Threats

90% of security investment focused here

Application Threats

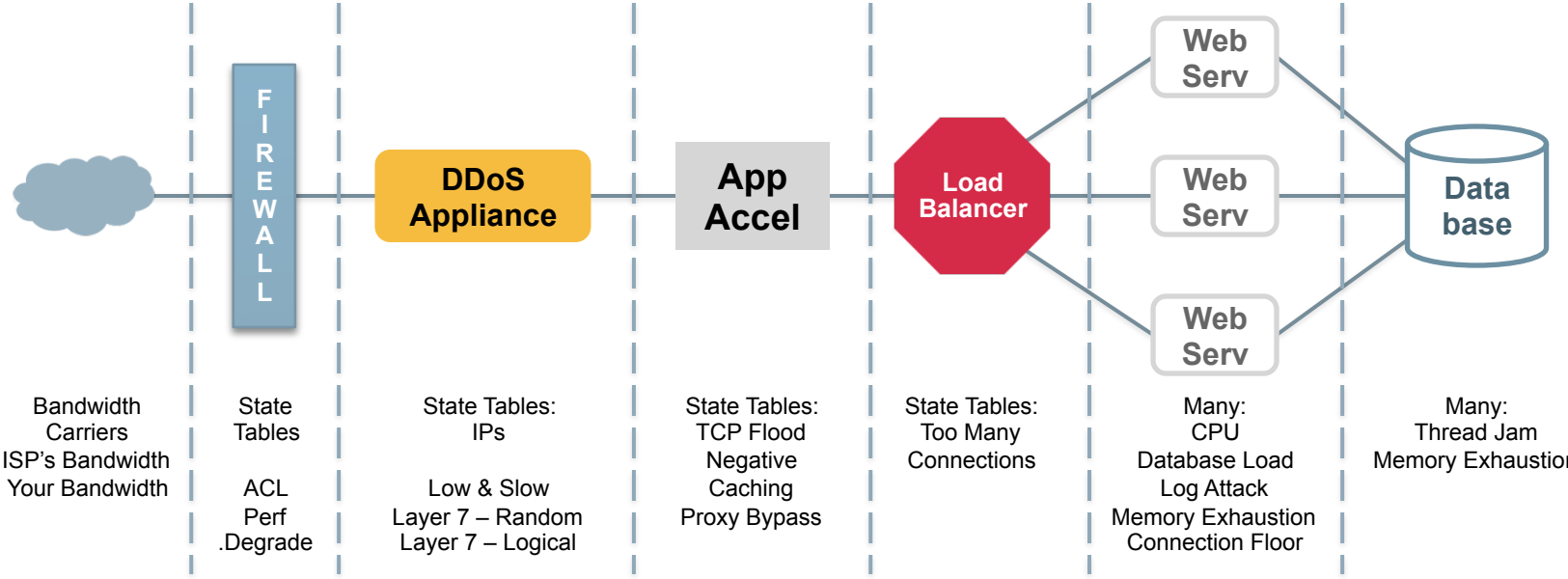
75% of attacks focused here

3DoS

Why The New Acronym?

- Diverse, Distributed Denial of Service
- “Attacks” are becoming increasingly a focussed period of many types of security events.
- Attacking groups are loosely collective, with a variety of methods, tools, resources and skills.
- Attacks start and stop, change in nature, and hit every aspect of a target infrastructure.
- Defensive controls must be broad and deep

Layer-7 Attacks



BANDWIDTH >> PACKET >> CONNECTION >> OS >>HTTP(S) >> APP >> DB

Mitigation controls which are failing…

- Network Firewalls
- Any Technology which blocks IP addresses
- Basic Rate Limiting
  - Connections per second
  - Per service, per client IP, etc
- Signature Scanning / IPS
  - SSL blinding
  - Out-of-band devices

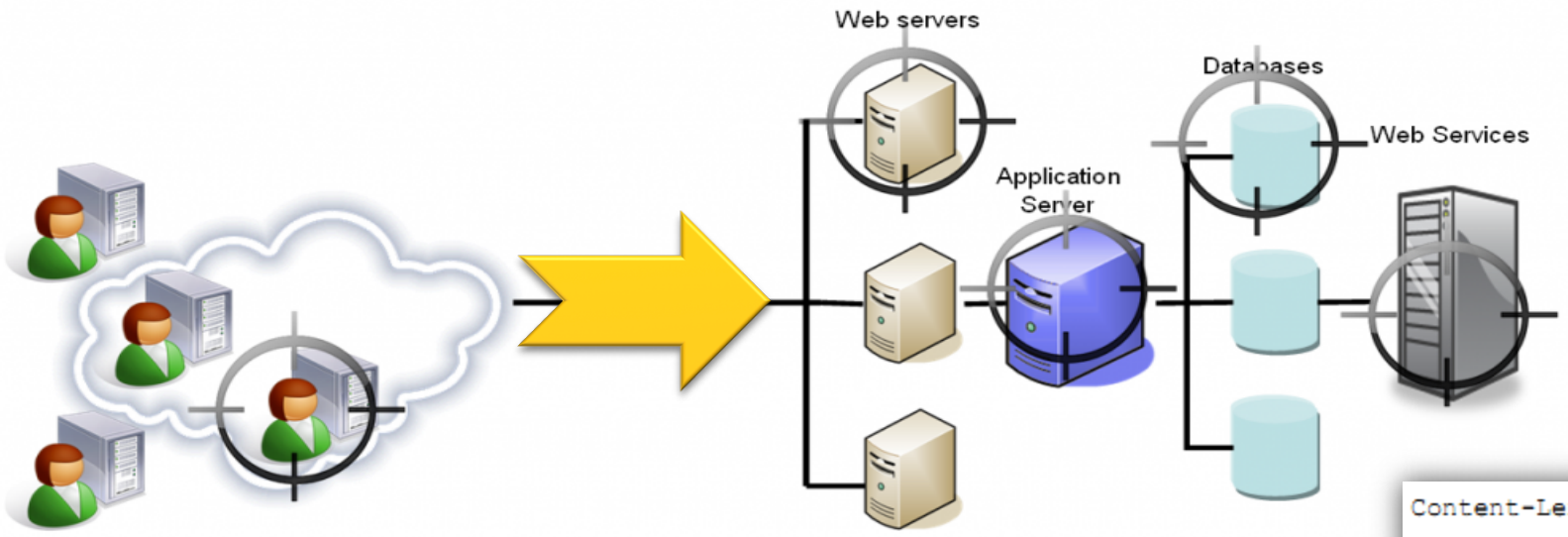
Mitigating controls must sit in path, know the application, and enforce behaviors - not IP addresses, or known bad strings

“It would appear that the security experts are not expertly secured

Anonymous

DDoS Eamples / Mitigation

SlowLoris



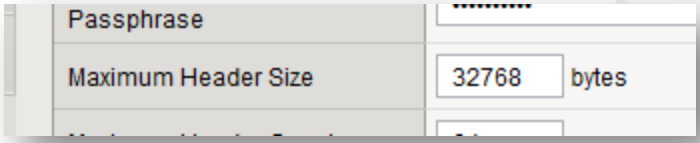

```
GET / HTTP/1.1
Host: 172.17.1.75
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; Trident/4.0; .NET CLR
1.1.4322; .NET CLR 2.0.50313; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729; MSOffice 12)
```

```
Content-Length: 42
...
X-a: b
...
X-a: b
...
X-a: b
...
X-a: b
...
X-a: b
...
```

Handling SlowLoris…

Resolution

Detect and drop slow requests to complete transmitting headers, and limits the Header size

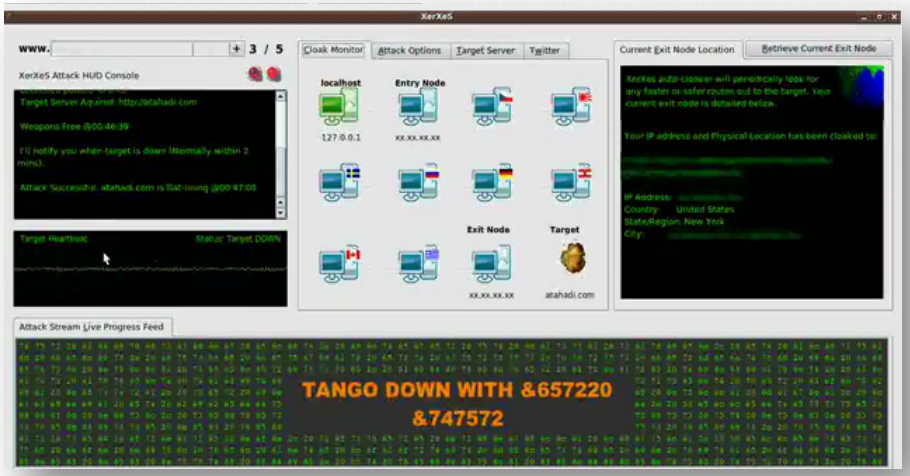



```
when CLIENT_ACCEPTED {
      set rtimer 0
      after 1000 {
            if { not $rtimer } {
                  drop
            }
}

 when HTTP_REQUEST {
       set rtimer 1
}
```

XerXes (2)…

Jester Unveils XerXeS Automated DoS Attack

Wednesday, February 10, 2010



Countermeasures (similar to Slowloris)

a) Lower TCP Connection Reaper percent from low 85/high 95 to low 75/high 90

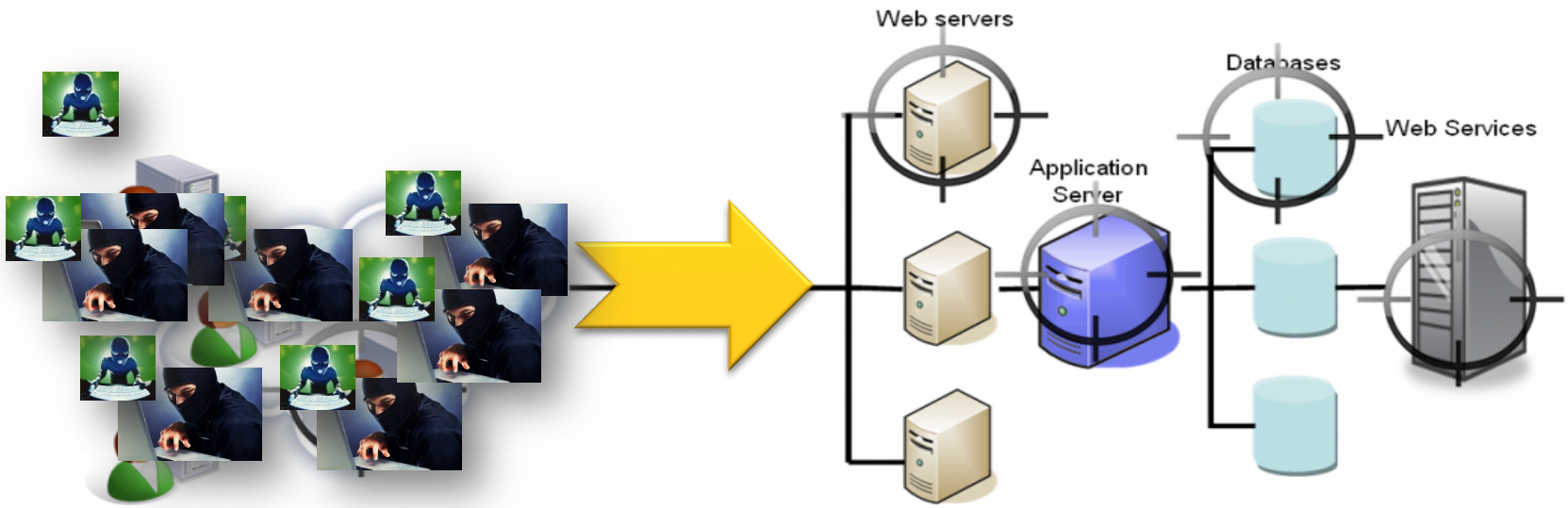
b) Lower TCP timeouts

LOIC (exploited in “Wikileak” saga)

Countermeasures (similar to Slowloris)

a) Lower TCP Connection Reaper percent from low 85/high 95 to low 75/high 90, Lower TCP timeouts

Slow Post Attacks



What The Vendors Say About Slow Post

Microsoft

"While we recognize this is an issue, the issue does not meet our bar for the release of a security update. We will continue to track this issue and the changes I mentioned above for release in a future service pack."

Apache

"What you described is a known attribute (read: flaw) of the HTTP protocol over TCP/IP. The Apache HTTP project declines to treat this expected use-case as a vulnerability in the software."

Handling Slow POST attack …

iRules

- Check on length and the client payload sent e.g. < 2048 bytes (def)
- Check on duration of connection with client e.g. < 2 seconds (def)
- If exceed custom duration or length, response to client retry

ASM

- ASM counts the number of slow post connections, connection above *Y* seconds are considered a slow connection.
- ASM will then prevent more than *X* slow connections to happen at the same time.

Handling Slow POST attack (iRule)

```
when RULE_INIT {
    # Default amount of request payload to collect (in bytes)
    set static::collect_length 2048

    # Default timeout for POST requests to send $collect_length bytes (in seconds)
    set static::timeout 2
}
```

```
when HTTP_REQUEST {
    # Only check POST requests
    if { [HTTP::method] equals "POST"} {
        # Create a local variable copy of the static timeout
        set timeout $static::timeout

# If the POST Content-Length isn't 0, collect (a portion of) the payload
if {[info exists collect_length]}{
    # If the entire request hasn't been received within X seconds, send a 408, and close the connection
    set id [after $timeout {
        HTTP::respond 408 content "Your POST request is not being received quickly enough. Please retry."
        TCP::close
    }]
```

#RefRef

- Use the target site's own processing power against itself. Its effectiveness is due to the fact that it exploits a vulnerability in a widespread SQL service
- Live fire exercises from the creator(s) took down "Pastebin" for 42 minutes after a 17 second attack
- Attackers combine with previous techniques like Slowloris and Slow POST to extend the impact

> I send two packets from my iphone, and everything else happens on the server. Basically eats itself apart, because since both are on the server, its all a local connection.

Anonymous

#RefRef Mitigation

- Block SQL commands from being inserted into HTTP requests (attack signatures for SQLi)
- Mitigation of Slowloris and Slow POST combo attacks

Handling “Apache Killer”

> The attack can be done remotely and with a modest number of requests can cause very significant memory and CPU usage on the server. The default Apache HTTPD installation is vulnerable. There is currently no patch/new version of Apache HTTPD which fixes this vulnerability.
>
> -- Apache mailing list archives

HEAD / HTTP/1.1 Host:xxxx Range:bytes=0-, 5-1,5-2,5-3,…

SSL/TLS Vulnerability BEAST (7)…

Hackers break SSL encryption used by millions of sites

Beware of BEAST decrypting secret PayPal cookies

By **Dan Goodin in San Francisco** • **Get more from this author**

Posted in ID, 19th September 2011 21:10 GMT

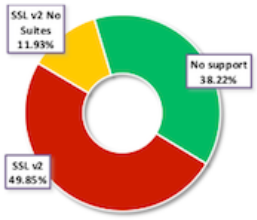
Free whitepaper – VMready

Researchers have discovered a serious weakness in virtually all websites protected by
secure sockets layer protocol that allows attackers to silently decrypt data that's passir
between a webserver and an end-user browser.

Half of all trusted servers support the insecure SSL v2 protocol

- Modern browsers won't use it, but wide support for SSL v2 demonstrates how we neglect to give any attention to SSL configuration
- Virtually all servers support SSLv3 and TLS v1.0
- Virtually no support for TLS v1.1 (released in 2006) or TLS v1.2 (released in 2008)
- At least 10,462 servers will accept SSLv2 but only deliver a user-friendly error message over HTTP

BLACK HAT USA 2010 QUALYS



Protocol	Support	Best protocol
SSL v2.0	302,886	-
SSL v3.0	607,249	3,249
TLS v1.0	604,242	603,404
TLS v1.1	838	827
TLS v1.2	11	11

November 05, 2009

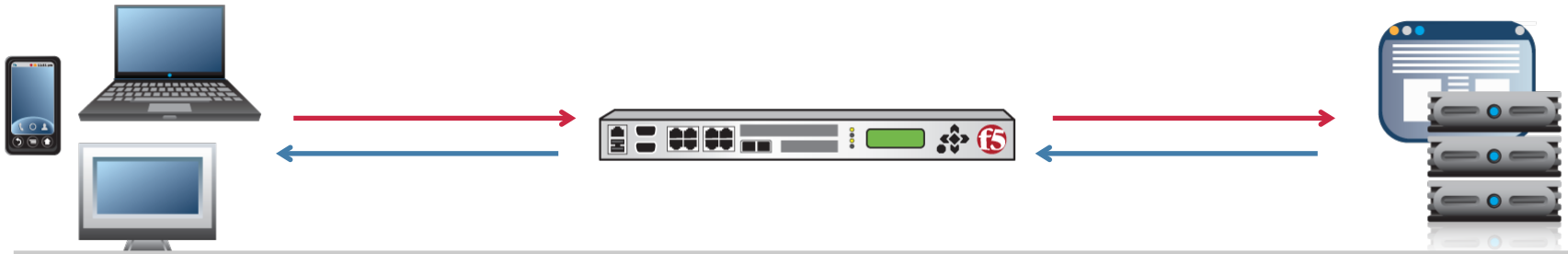
SSL and TLS Authentication Gap vulnerability discovered

A serious vulnerability has been discovered in the way web servers utilise SSL (and TLS, up to the most
recent versio
content int
vulnerable.

SOL10737: SSL Renegotiation vulnerability - CVE-2009-3555 / VU#120541
http://support.f5.com/kb/en-us/solutions/public/10000/700/sol10737.html

BIG-IP 10.1.0, BIG-IP 10.2.0
Introduce a clientssl / serverssl profile option to control whether midstream SSL renegotiation is allowed. For versions which include this CR, the default setting for the clientssl profile is disabled, and the default setting for the serverssl profile is enabled.

Addressing SSL/TLS vulnerability seamlessly



Client

- Different browser that would not support SSL/ TLS 1.2 yet e.g. Firefox, Chrome, Safari
- Pre-configured application policies

Enforcer

SSL Client Profile – enforce TLS 1.2

- **SSL Server Profile** – Automated compatibility (need not be TLS1.2)

Server

- Negotiable with its supported crypto algorithm

SSL DoS Tool

Hackers have released a program they say will allow a single computer to take down a Web server using a secure connection.

The THC-SSL-DOS tool, which was released Monday, purportedly exploits a flaw in Secure Sockets Layer (SSL) renegotiation protocol by overwhelming the system with multiple requests for secure connections. SSL renegotiation allows We sites to create a new security key over an already established SSL connection.

THC SSL DOS Tool Can Take Down a Server from a Single Laptop

SHARE: +1 0 Like 1 Send Tweet Adjust text size:

ENLARGE

A German hacker group released a hacking tool that by making use of a flaw in SSL Renegotiation can easily take down a website with minimal resources.

The group known as The Hacker's Choice (THC) released a proof of concept that will further force vendors to patch up the issues that revolve around the use of SSL.

"We decided to make the official release after realizing that this tool leaked to the public a couple of months ago," revealed a member of THC.

Unlike the traditional DDoS which requires a large number of bots, the new TCH SSL DOS utility needs only a handful of bots to take down a website and a single laptop to quickly exhaust the resources of a server.

"We are hoping that the fishy security in SSL does not go unnoticed. The industry should step in to fix the problem so that citizens are safe and secure again. SSL is using an aging method of protecting private data which is complex, unnecessary and not fit for the 21st century," said one of the group's members.

Even though SSL Renegotiation is rarely used in practice, the research shows that these days most serves have the feature enabled by default, leaving them vulnerable in front of an attack.

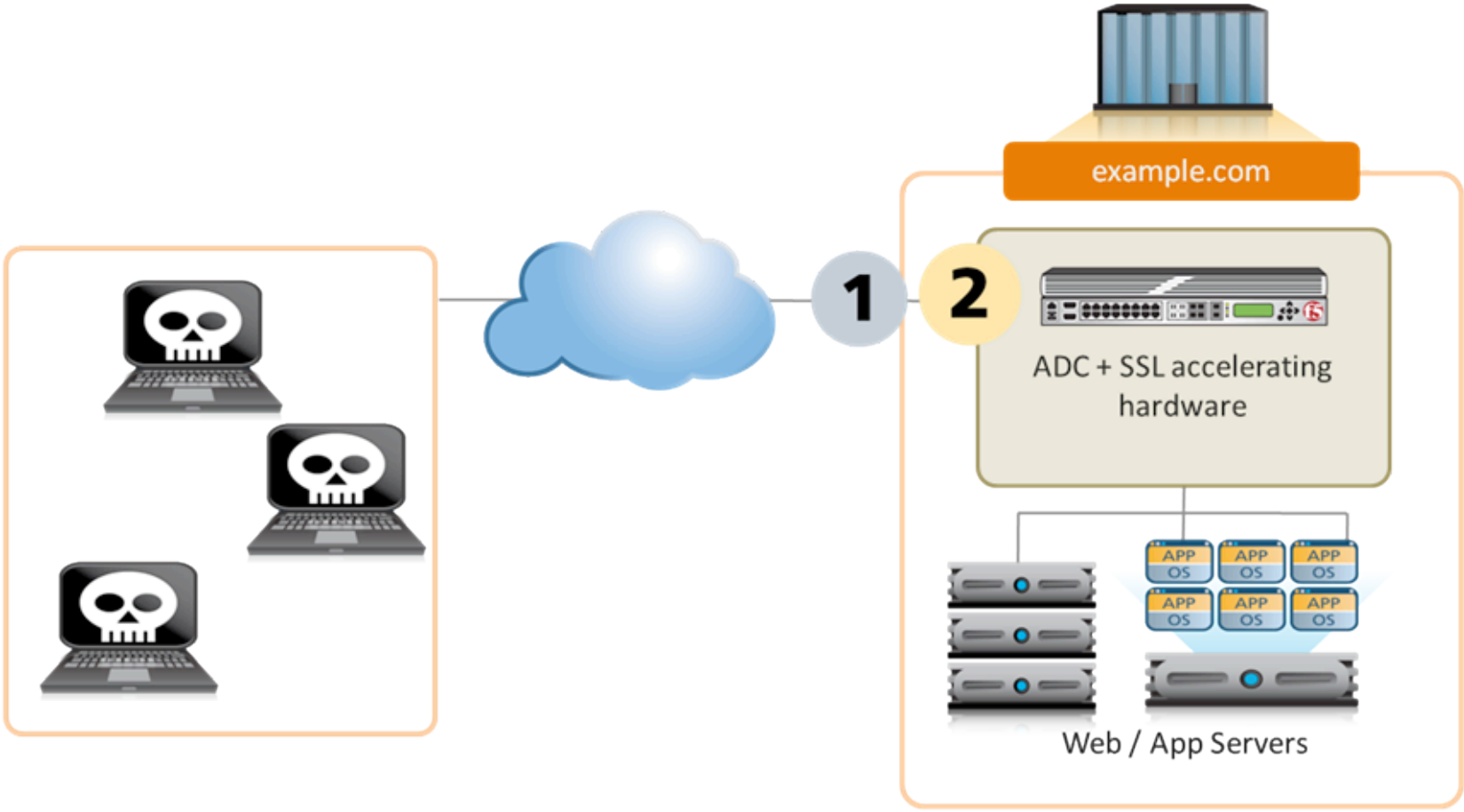
Establishing a secure SSL connection requires 15x more processing power on the server than on the client.

THC-SSL-DOS exploits this asymmetric property by overloading the server and knocking it off the Internet.

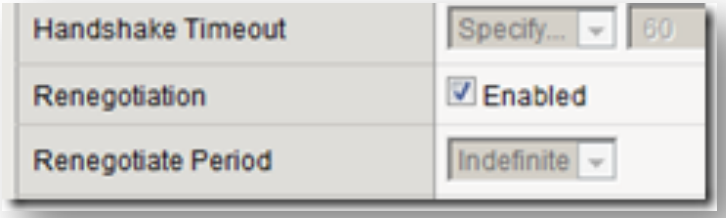
This problem affects all SSL implementations today. The vendors are aware of this problem since 2003 and the topic has been widely discussed.

This attack further exploits the SSL secure Renegotiation feature to trigger thousands of renegotiations via single TCP connection.

Mitigating the THC SSL DoS Threat



THC-SSL-DOS Mitigation for LTM




```
when RULE_INIT {
    set static::maxquery 5
    set static::mseconds 60000
}
when CLIENT_ACCEPTED {
    set ssl_hs_reqs 0
}
when CLIENTSSL_HANDSHAKE {
    incr ssl_hs_reqs
    after $static::mseconds { if {$ssl_hs_reqs > 0} {incr ssl_hs_reqs -1} }
    if { $ssl_hs_reqs > $static::maxquery } {
        after 5000
        log "Handshake attack detected, dropping [IP::client_addr]:[TCP::client_port]"
        drop
    }
}
```

Slow Read DoS

Do not accept connections with abnormally small advertised window sizes

Do not enable persistent connections and HTTP pipelining unless performance really benefits from it

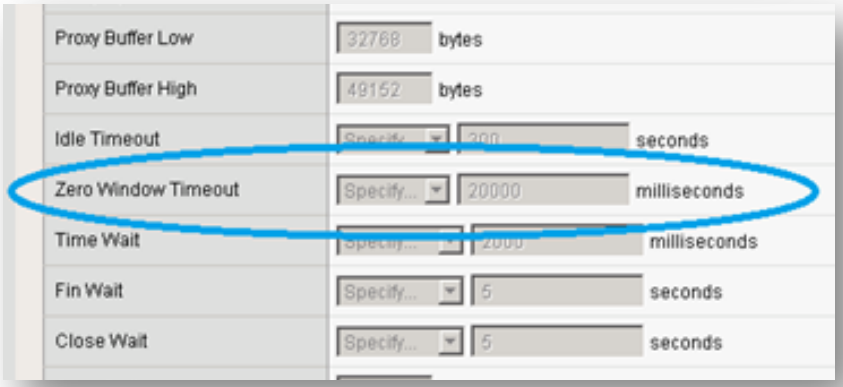
Limit the absolute connection lifetime to some reasonable value

SECURITY Jan 5, 2012 10:30 pm

Researcher Devises Hard-to-detect Denial-of-service Attack Against HTTP Servers

By Lucian Constantin, IDG-News-Service:Romania-Bureau

Qualys senior software engineer Sergey Shekyan has devised a new HTTP denial-of-service (DoS) attack method which relies on prolonging the time clients need to read Web server responses



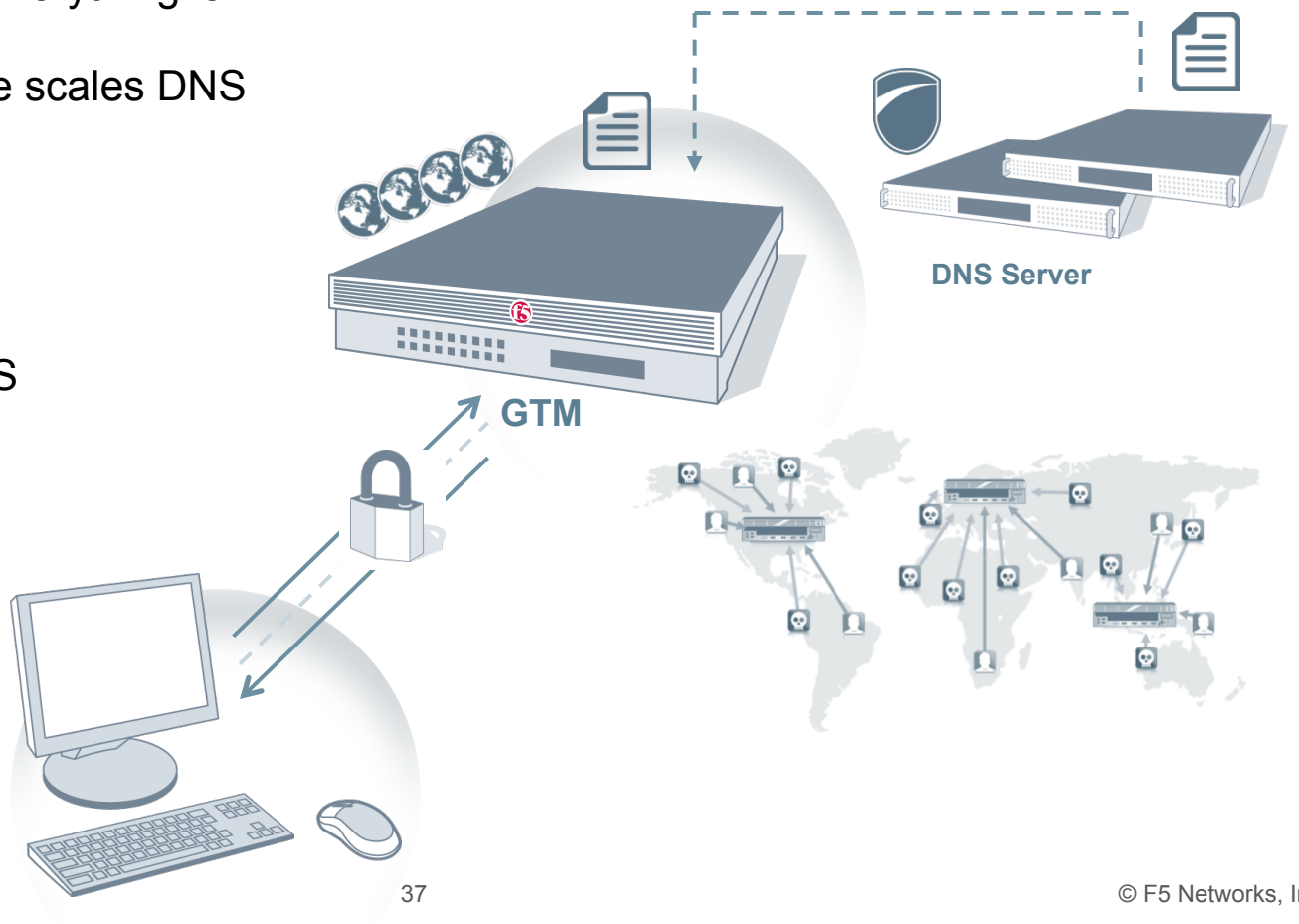
```
when SERVER_CONNECTED {
    TCP::collect
}

when SERVER_DATA {
    set rtimer 0
    # Time in milliseconds before HTTP response read is considered slow:
    after 5000 {
        if { not $rtimer} {
            # Slow read detected for this server response. Increment the count by adding a table entry:
            # Add the client source IP::port to the subtable with a timeout
            table set -subtable "MyApplication" "[IP::client_addr]:[TCP::client_port]" "ignored" 180

            # Are we over the concurrency limit?
            if { [table keys -subtable "MyApplication" -count] > 5} {

                # If so, reject connection:

                clientside {reject}
                table delete -subtable "MyApplication" "[IP::client_addr]:[TCP::client_port]"
                log local0. "Excessive HTTP slow reads detected (possible DoS attempt):
[IP::client_addr]:[TCP::client_port]"
            }
        }
    }
    TCP::notify response
    TCP::release
    TCP::collect
}

when USER_RESPONSE {
    set rtimer 1
}

when CLIENT_CLOSED {
    table delete -subtable "MyApplication" "[IP::client_addr]:[TCP::client_port]"
}
```

DNS Security (10)…

- DNS is a likely target
- Without DNS, virtually everything is down
- F5 DNS Services profile scales DNS infrastructure
- Full slave domain copy

Benefits

- High Performance DNS
- >1M DNS RPS
- Scalable DNS
- Secure DNS Queries
- BGP Anycast
- DNSSec
- IPv6



Practical Strategy for Data Center Security

Which is More Effective?

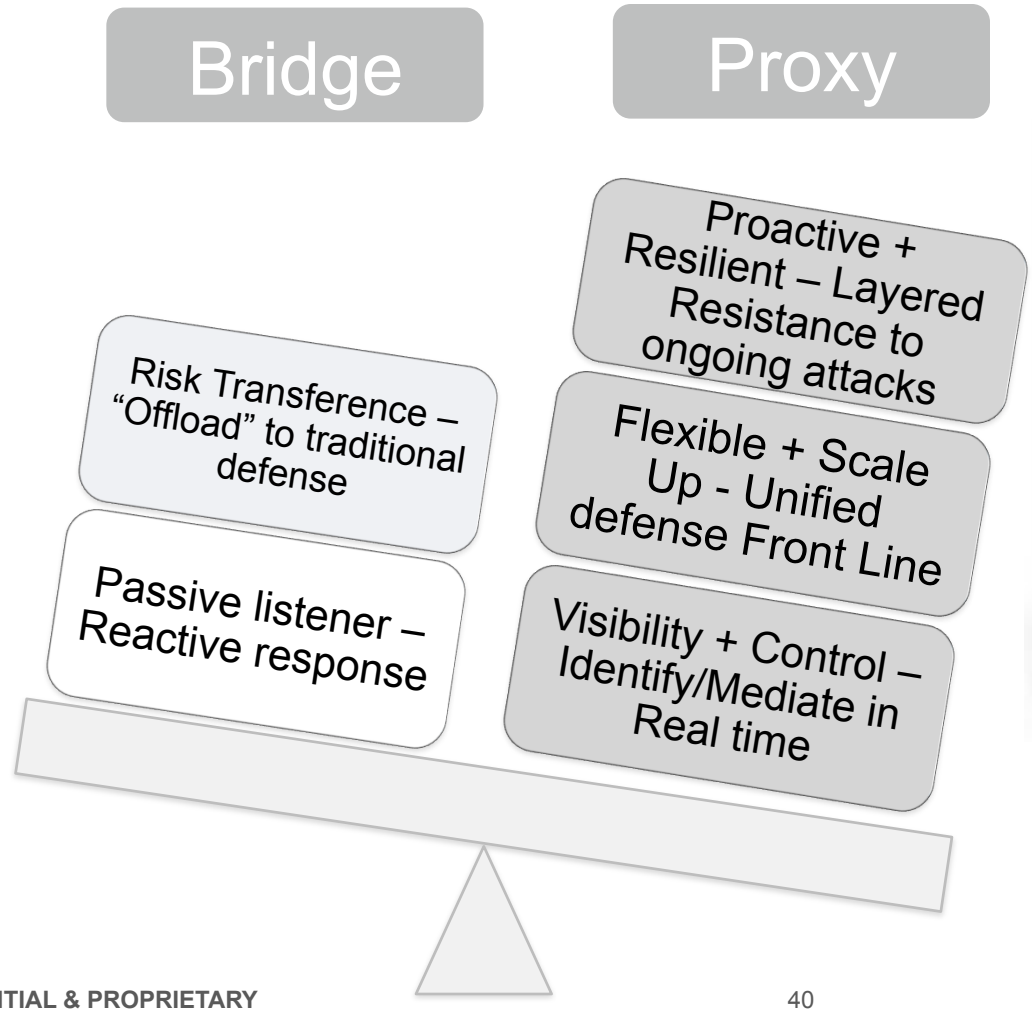
Patrol vs Moat

VS

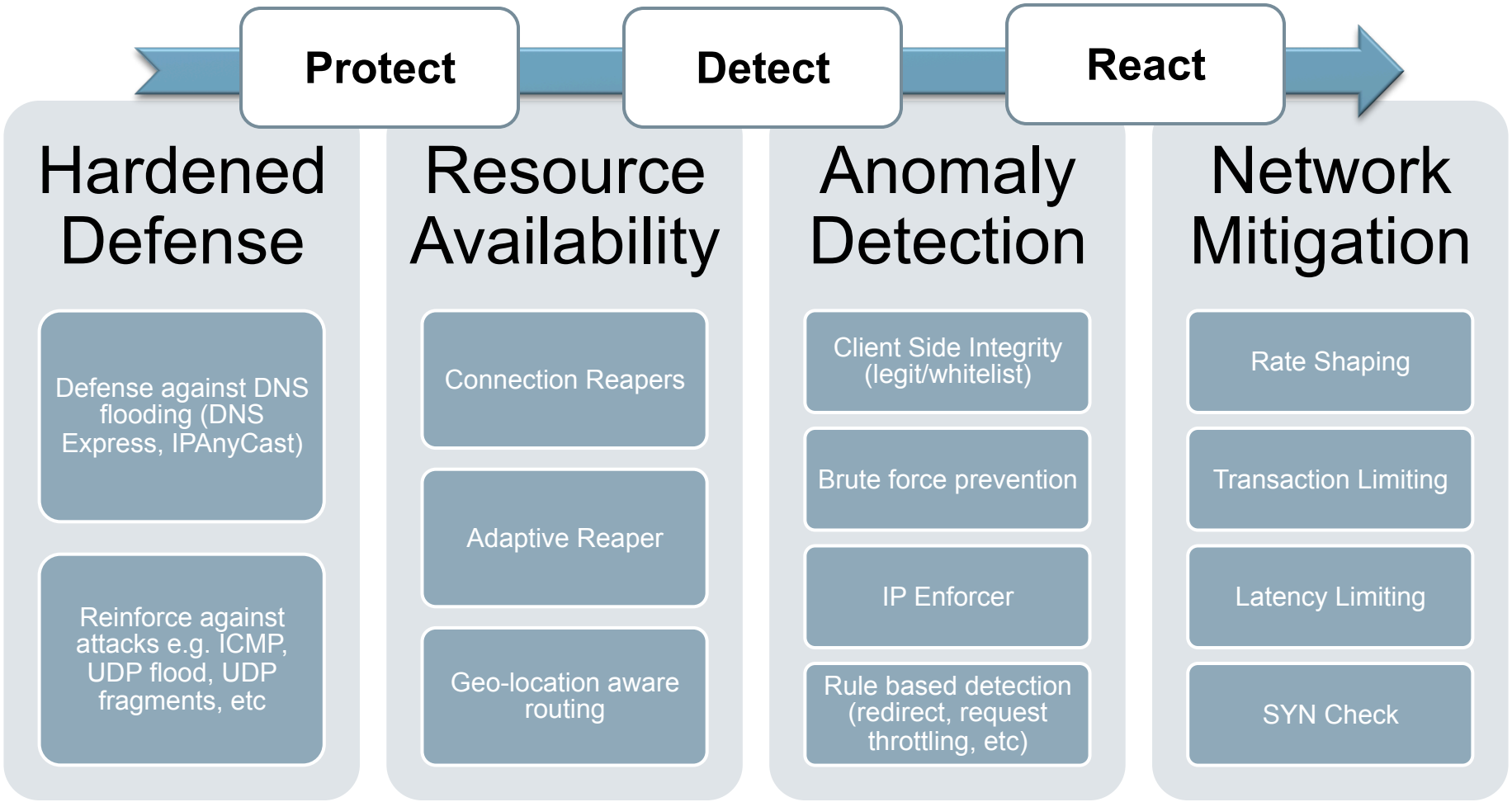
Bridge Mode

Full Proxy Mode

Bridge mode vs Proxy mode



DDoS mitigation



DDoS Strategic Mitigation Approach

Attack Identification

Traffic Thresholds

iRule/ASM Attack Signatures for Known DDoS attacks

DDoS attack relief

Modify WIP (global distro)

Attack Mitigations

Cleansing the traffic

Syn cookies, total sessions, ramp & dissolve rates

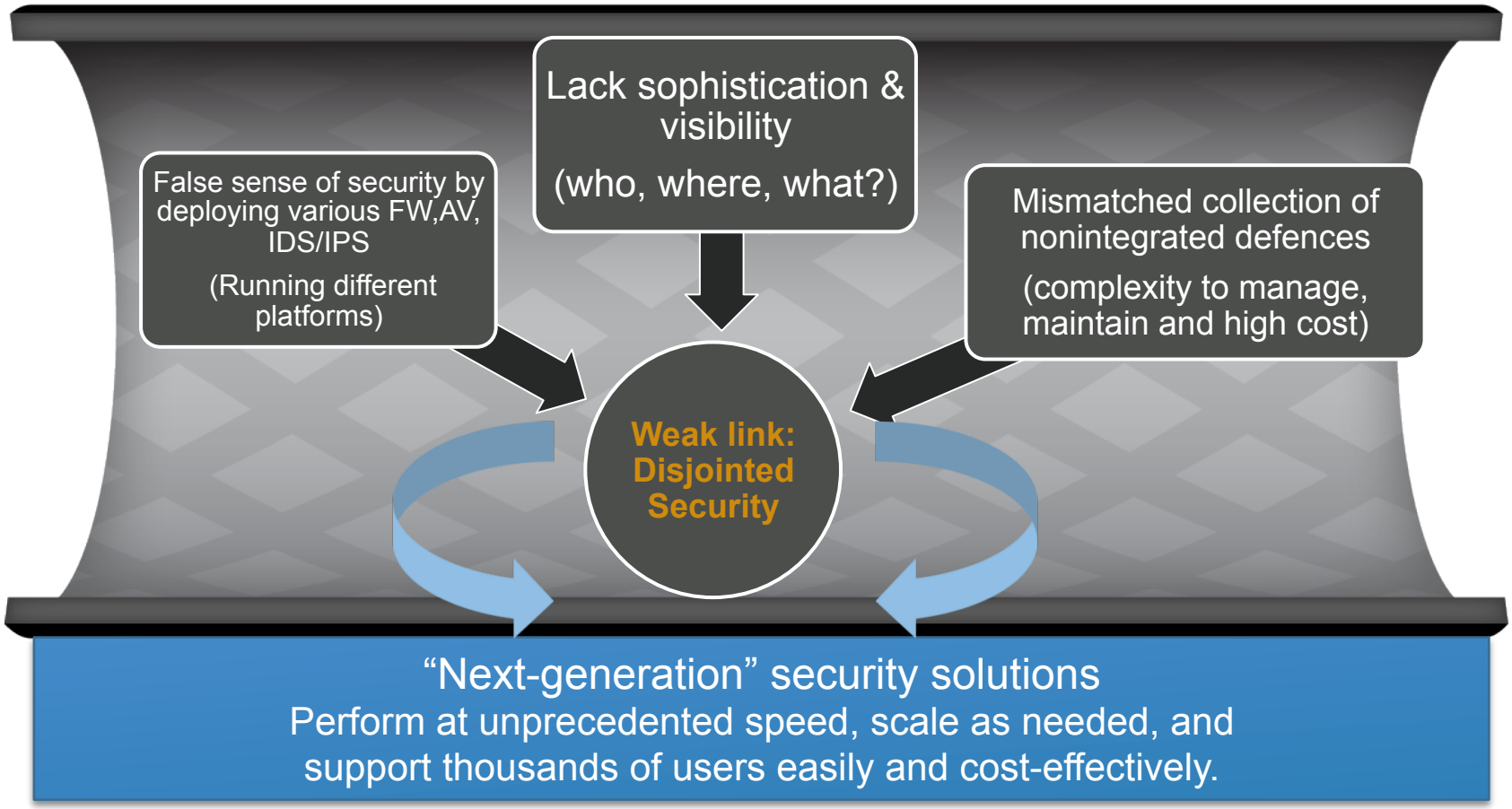
Line-Rate Hardware mitigation

iRule/ASM Attack Signatures for Known DDoS attacks

iRule/ASM Logging Signatures for analysis of unknown attack

iRule/ASM custom rule creation

Rethink Yesterday's Security Strategies



Questions?

IT agility. Your way.®