(D)DoS Story

Luboš Klokner

F5 System Engineer

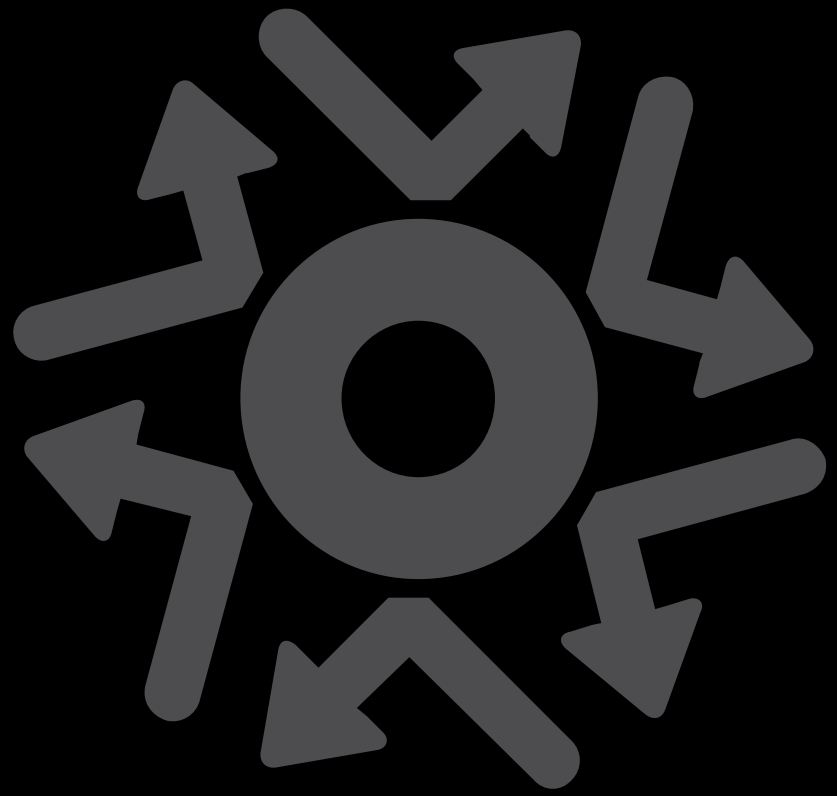
l.klokner@f5.com

+421 908 755152

@lklokner

Agenda

- Intro
- Main Part
- Tools
- Different sorts of (D)DoS Attacks
- F5 Multilayer (D)DoS Protection
- IPv6
- FW + ADC Deployments
- F5 Application Delivery Firewall



© 2016 F5 Networks

Introduction

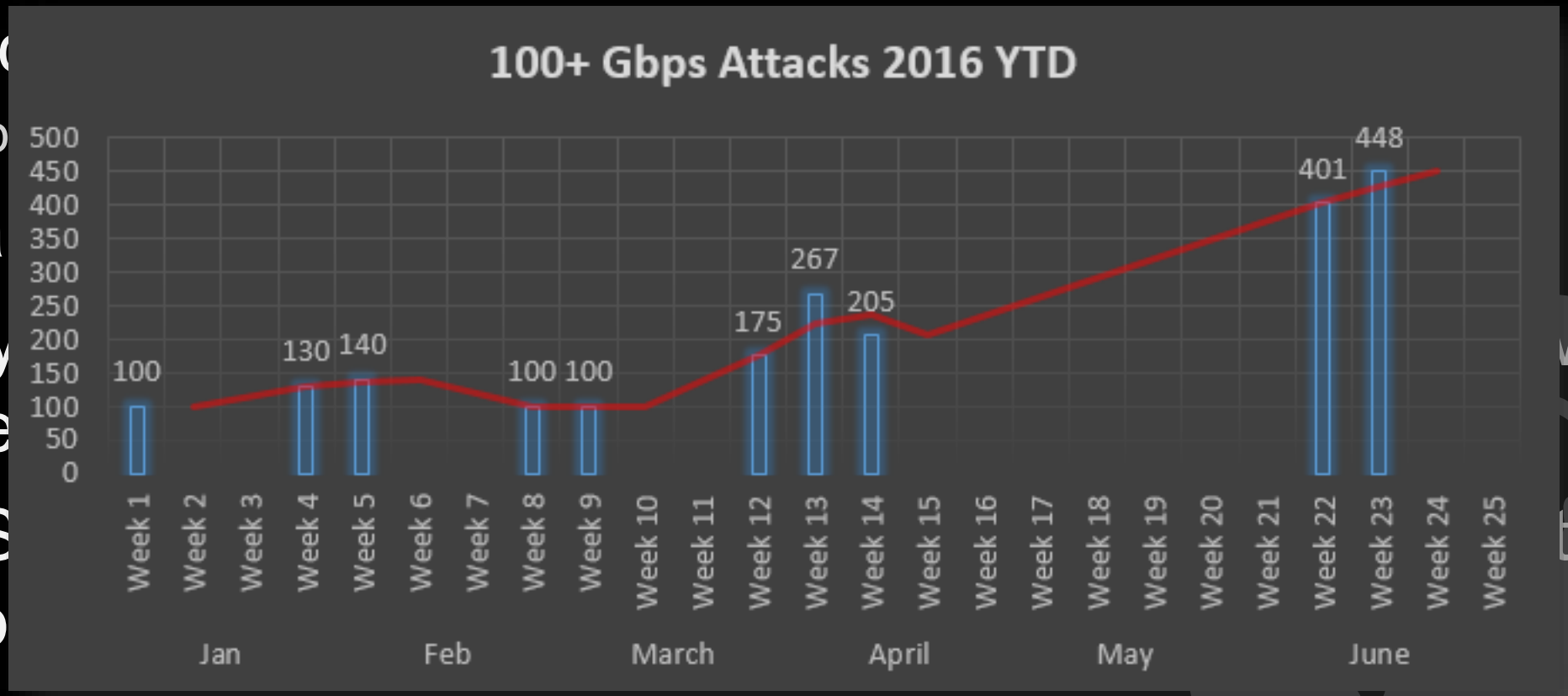
F5 Silverline

- Attack mitigation bandwidth capacity over 2.0 Tbps
- Scrubbing capacity of over 1.0 Tbps
- Guaranteed bandwidth with Tier 1 carriers
- Fully redundant and globally distributed data centers world wide in each geographic region
- F5 SOC is available 24/7 with security experts ready to respond to DDoS attacks within minutes

© 2016 F5 Networks

F5 Silverline

- Atta
- Scrub
- Gua
- Fully world wide
- F5 S to resp

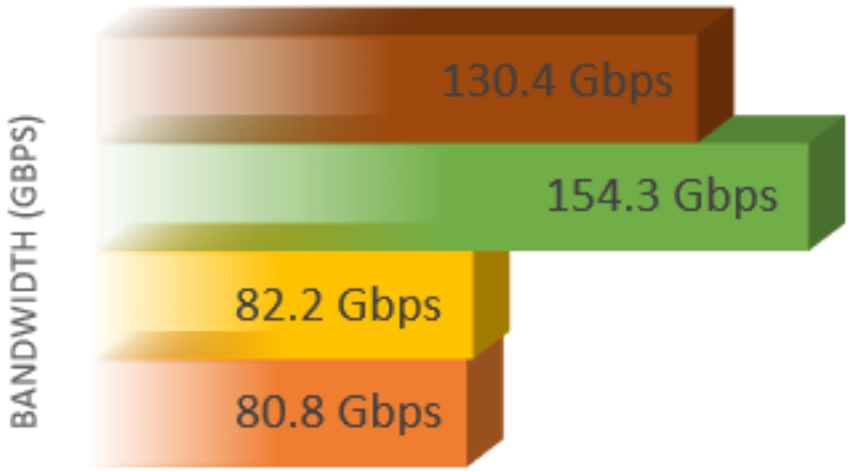


© 2016 F5 Networks

F5 Silverline

- Atta
- Scrul
- Gua
- Full world wide
- F5 S o resp

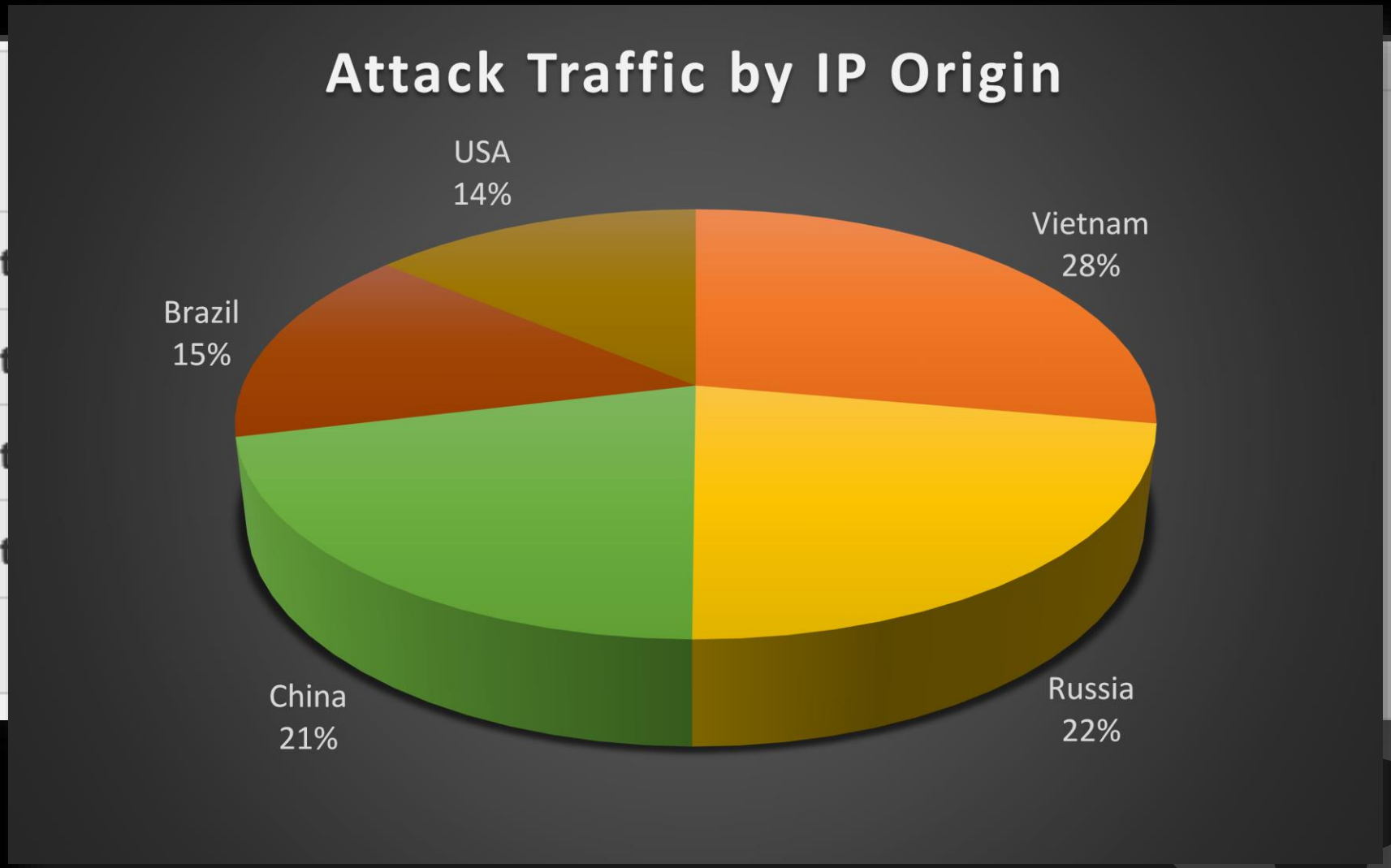
	Bandwidth (Gbps)
Data Center 1	130.4
Data Center 2	154.3
Data Center 3	82.2
Data Center 4	80.8
TOTAL	447.7



© 2016 F5 Networks

F5 Silverline

- Atta
- Scrul
- Gua
- Full wide
- F5 S resp



world

o

© 2016 F5 Networks

Brian Krebs

briankrebs @briankrebs 1d

20gbps ddos on my site this afternoon. guess that's what happens when you expose a ddos for hire service krebsonsecurity.com/2016/09/israel...

You

briankrebs @briankrebs 1d

actually make that 128Gpbs. shit just got real.

briankrebs @briankrebs 1d

word from three sources now that vDOS proprietor AppleJ4ck just got raided in Israel. guess that explains a lot.

© 2016 F5 Networks

Brian Krebs

HackedByKyoto @HackedByKyoto 1d

Yo @briankrebs guess he luck ran out... twitter.com/AppleJ4ck_vDos...

> **Yarden Bidani** @AppleJ4ck_vDos
> @FBI dns-pub-01-u.pentagon.mil #DDOSED arrest me pussies

briankrebs

briankrebs @briankrebs

Alleged co-owners of attack-for-hire site vDOS arrested in Israel. CEO of a victim company admits to BGP hijacking krebsonsecurity.com/2016/09/allege...

© 2016 F5 Networks

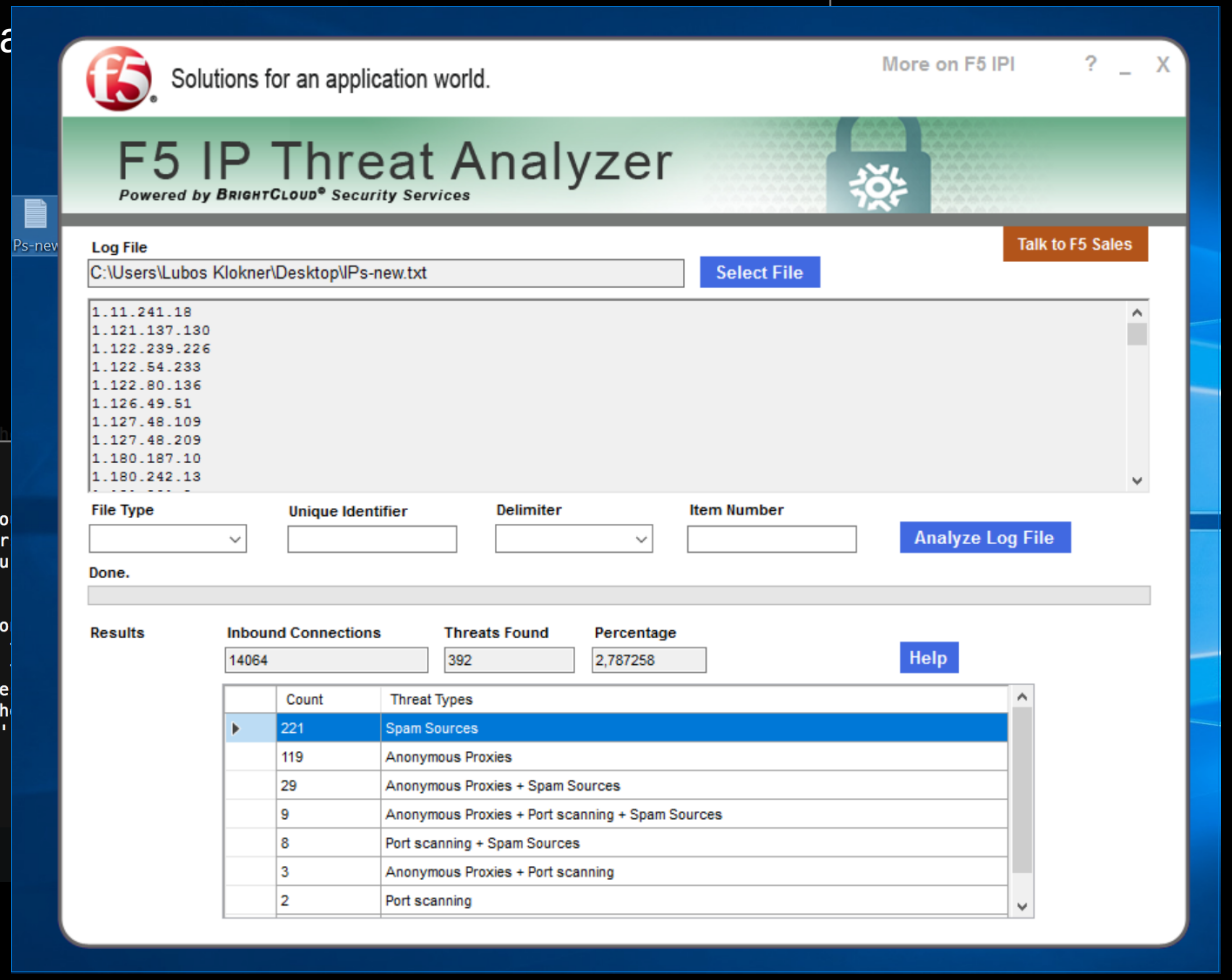
vDoS Victims

```
erkacs-MBP:Desktop erkac$ awk -F "," '{ print $4 }' atta
IPs.txt
erkacs-MBP:Desktop erkac$ wc -l IPs.txt
  171003 IPs.txt
erkacs-MBP:Desktop erkac$ sort -u IPs.txt | wc –l
   14066
erkacs-MBP:Desktop erkac$
```

attacks.txt UNREGISTERED

```
site claims:


51,'DDoS','We\'re a legitimate stress testing company, not a DDoS service. yo
from stressing internet connections and/or servers that you do not have owner
authorization to test.\r\n\r\nAbuse of our services or use in violation of ou
service will result in being banned from our services.'

131,'prc','It is necessary to raise our prices due to users stressing home co
addresses which they do not have the authorization to do so. If users desire
services for legitimate reasons, there shouldnâ€™t be an issue when it comes
slightly more than they used to. Like Iâ€™ve stated, we are a legitimate stre
company which is dedicated to assisting pentesters as well as normal users wh
in testing their own serverâ€™s resilience to multiple varieties of attacks.'



Decide for yourself.
```

Line 1, Column 1



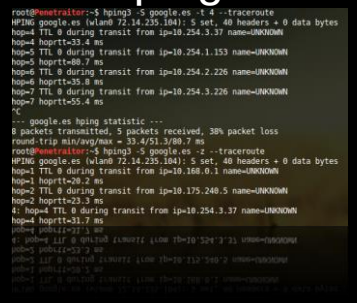
© 2016 F5 Networks

Handy Tools

Available tools

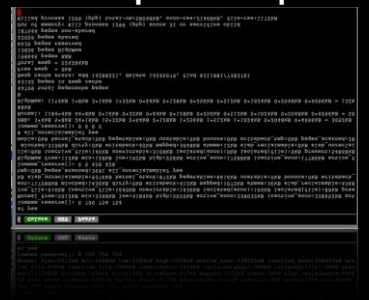
Press button and forget

hping3

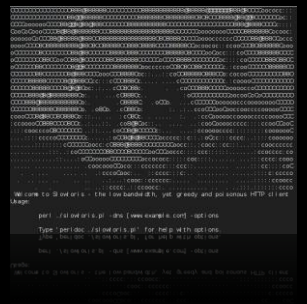


nmap

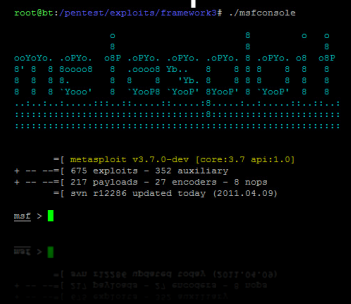
killapache.pl



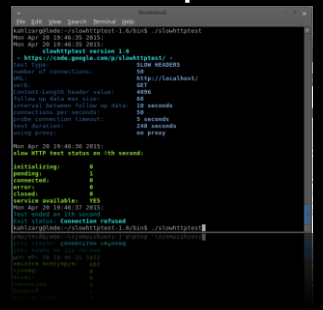
slowloris



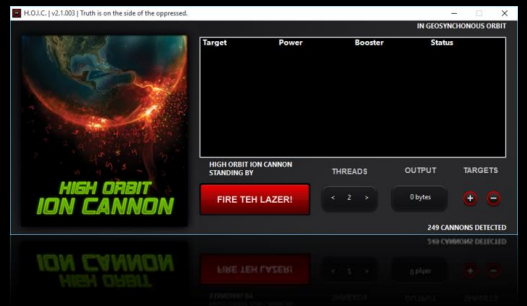
metasploit



slowhttptest



High Orbit ION



Low Orbit ION

Dirt Jumper

RussKill

Pandora

© 2016 F5 Networks

Available tools

Press button and forget

hping3

nmap

killapache.pl

slowhttptest

AND MANY MORE!!

Dirt Ju

RussKill

Pandora

© 2016 F5 Networks

Available tools

Log in Request account

Page Discussion Read View source View history Search

OWASP HTTP Post Tool

Home
About OWASP
Acknowledgements
Advertising
AppSec Events
Books
Brand Resources
Chapters
Donate to OWASP
Downloads
Funding
Governance
Initiatives
Mailing Lists
Membership
Merchandise
News
Community portal
Presentations
Press
Projects
Video
Volunteer

Reference
Activities
Attacks
Code Snippets
Controls
Glossary

Main

OWASP Switchblade

Introduction

OWASP Switchblade is a denial of service tool used for testing the availability, performance and capacity planning of a web application to be proactive about this type of risk condition

Description

The projected started in early 2000 as a way to test the capacity of simultaneous users connected to a web application and was not public tool. In 2010 the tool was created by ProactiveRISK to educate the OWASP Community about the Denial of Service conditions that can exist with Layer7

Licensing

OWASP Switchblade is free to use. It is licensed under the http://creativecommons.org/licenses/by-sa/3.0/ Creative Commons Attribution-ShareAlike 3.0 license], so you can copy, distribute and transmit the work, and you can adapt it, and use it commercially, but all provided that you attribute the work and if you alter, transform, or build upon this work, you may distribute the resulting work only

What is Switchblade

OWASP Switchblade provides (3) different types of denial of service conditions that can be tested from a single machine

- SSL Half Connect
- HTTP Post Attack
- Slowloris

Presentation

Link to presentation

Project Leader

Tom Brennan

Related Projects

OWASP Testing Guide

Openhub

Quick Download

- Windows Installer [1]
- GITHUB

Email List

N/A

News and Events

- [12 June 2015] Page Updated New Template

In Print

N/A

Classifications

Builders

Defenders

© 2016 F5 Networks

Available tools

- `erkac@geck$`
- `for i in $( seq 1 1000 ); do`
- `  wget -O /dev/null -m http://site?xyz &`
- `done`

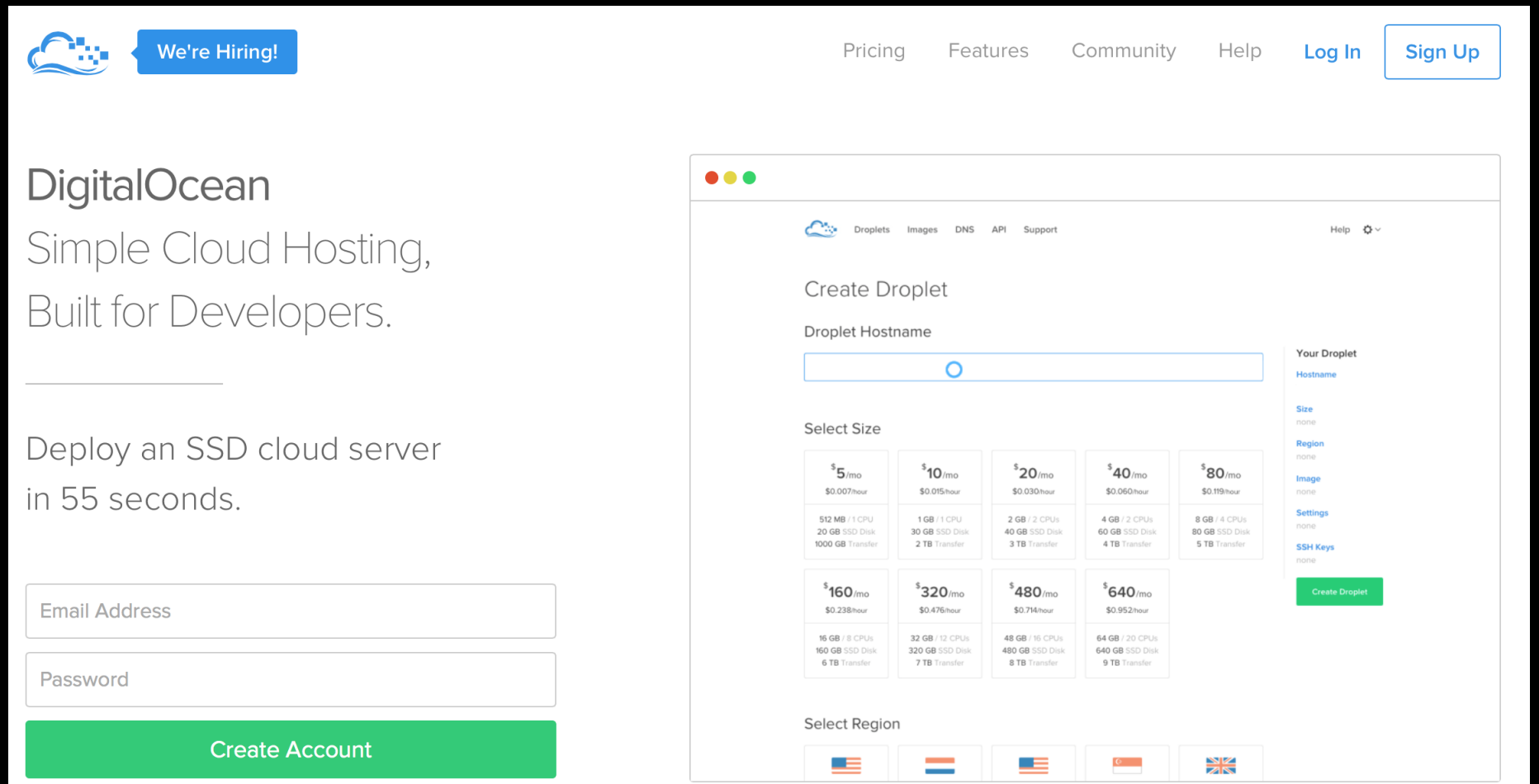
Available tools

```
[erkac@geck]-[~]$ wc -l hulk.py
155 hulk.py
[erkac@geck]-[~]$ python hulk.py
-----------------------------------------------
USAGE: python hulk.py <url>
you can add "safe" after url, to autoshut after dos
-----------------------------------------------
[erkac@geck]-[~]$ less hulk.py
…
```

Available tools

```
# ------------------------------------------------------------------------------------
# HULK - HTTP Unbearable Load King
#
# this tool is a dos tool that is meant to put heavy load on HTTP servers in order to bring them
# to their knees by exhausting the resource pool, its is meant for research purposes only
# and any malicious usage of this tool is prohibited.
#
# author :  Barry Shteiman , version 1.0
# ------------------------------------------------------------------------------------
```

How to execute L7 DoS?



https://m.do.co/c/f9d15bf38488

KrebsOnSecurity

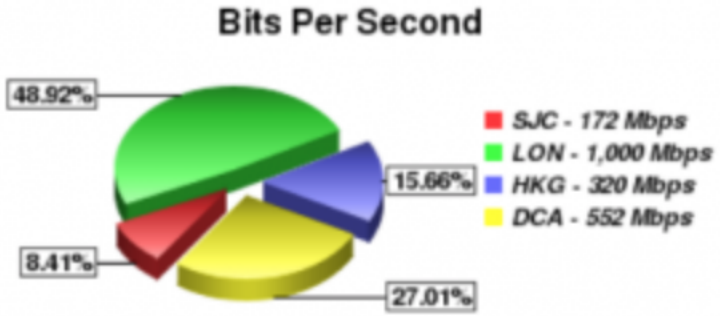
8
AUG 12

Triple DDoS vs. KrebsOnSecurity

"When nobody hates you, nobody knows you're alive." – Diplomacy, by Chris Smither

During the last week of July, a series of steadily escalating cyber attacks directed at my Web site and hosting provider prevented many readers from being able to reach the site or read the content via RSS. Sorry about that. What follows is a post-mortem on those digital sieges, which featured a mix of new and old-but-effective attack methods.

I still don't know who was attacking my site or why. It's not as if the perpetrator(s) sent a love letter along with the traffic flood. There was one indication that a story I published just



© 2016 F5 Networks

KrebsOnSecurity

8 Triple DDoS vs. KrebsOnSecurity

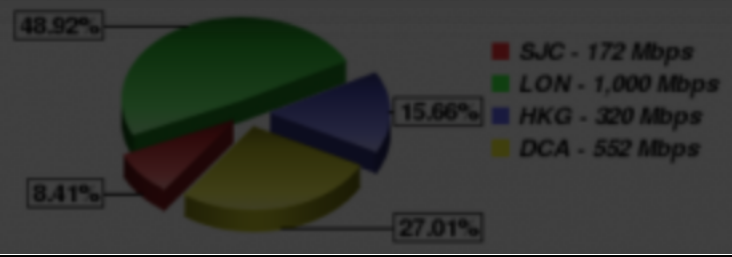
AUG 12

"When nobody hates you, nobody knows you're alive." – Diplomacy, by Chris Smither

During the last we
my Web site and h
the site or read t
mortem on those
attack methods.

Pandora's creators boast that it only takes 10 PCs infected with the DDoS bot to bring down small sites, and about 30 bots to put down a mid-sized site that lacks protection against DDoS attacks. They claim 1,000 Pandora bots are enough to bring Russian search engine giant **yandex.ru** to a crawl, but that strikes me as a bit of salesmanship and exaggeration. Prolexic said more than 1,500 Pandora-infected bots were used in the assault on my site.

I still don't know who was attacking my site or why. It's not as if the perpetrator(s) sent a love letter along with the traffic flood. There was one indication that a story I published just



© 2016 F5 Networks

Different kinds of DDoS Attacks

Types of DDoS Attacks

Layer 7	Application		OWASP Top 10 (e.g. XSS), Slowloris, Slow Post/Read, HTTP GET/POST floods,...
Layer 6	Session	SSL	DNS UDP floods, DNS query floods, DNS NXDOMAIN floods SSL floods, SSL renegotiation, ...
Layer 5		DNS, NTP	
Layer 4	Network		SYN/UDP/Conn. floods, PUSH and ACK floods, ICMP/Ping floods, Teardrop, Smurf Attacks, ...
Layer 3			
Layer 2			

© 2016 F5 Networks

Types of DDoS Attacks

Blended

Application

OWASP Top 10 (e.g. XSS), Slowloris, Slow Post/Read, HTTP GET/POST floods,...

Session

SSL

DNS, NTP

Network

Volumetric

© 2016 F5 Networks

ISO/OSI and F5 Modules

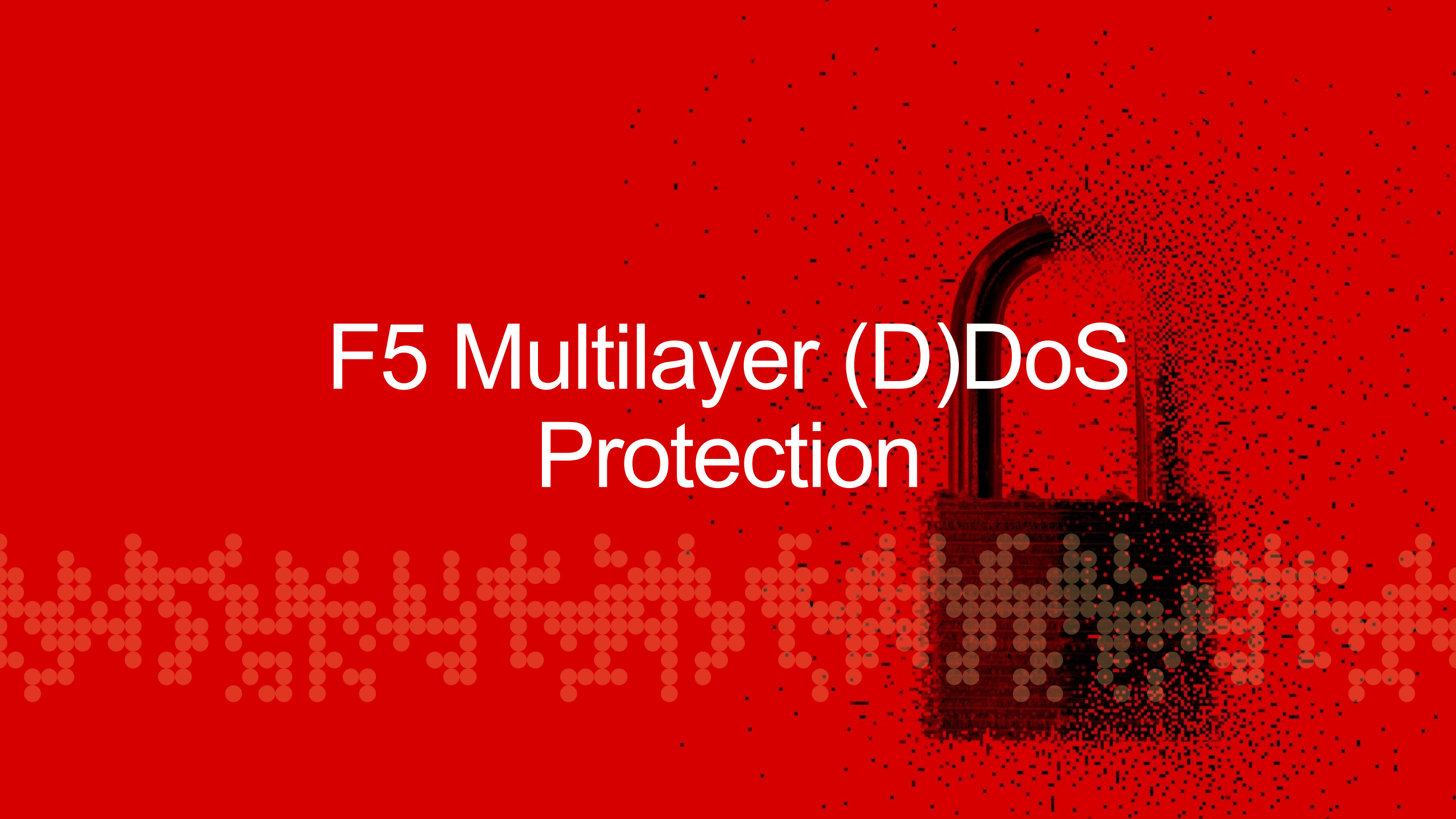
Increasing difficulty of attack detection

OSI stack	Physical (1)	Data Link (2)	Network (3)	Transport (4)	Session (5)	Presentation (6)	Application (7)	OSI stack

	Network attacks	Session attacks	Application attacks
	SYN Flood, Connection Flood, UDP Flood, Push and ACK Floods, Teardrop, ICMP Floods, Ping Floods and Smurf Attacks	DNS UDP Floods, DNS Query Floods, DNS NXDOMAIN Floods, SSL Floods, SSL Renegotiation	Slowloris, Slow Post, HashDos, GET Floods
F5 mitigation technologies	**BIG-IP AFM** SynCheck, default-deny posture, high-capacity connection table, full-proxy traffic visibility, rate-limiting, strict TCP forwarding. Packet Velocity Accelerator (PVA) is a purpose-built, customized hardware solution that increases scale by an order of magnitude above software-only solutions.	**BIG-IP LTM and GTM** High-scale performance, DNS Express, SSL termination, iRules, SSL renegotiation validation	**BIG-IP ASM** Positive and negative policy reinforcement, iRules, full proxy for HTTP, server performance anomaly detection
F5 Mitigation Technologies			

© 2016 F5 Networks

F5 Multilayer (D)DoS Protection



F5 Networks DDoS Protection

On-premises and cloud-based services for comprehensive DDoS Protection

F5 SILVERLINE DDOS PROTECTION

- Turn on cloud-based service to stop volumetric attacks from ever reaching your network
- Multi-layered L3-L7 DDoS attack protection against all attack vectors
- 24/7 attack support from security experts

When under attack

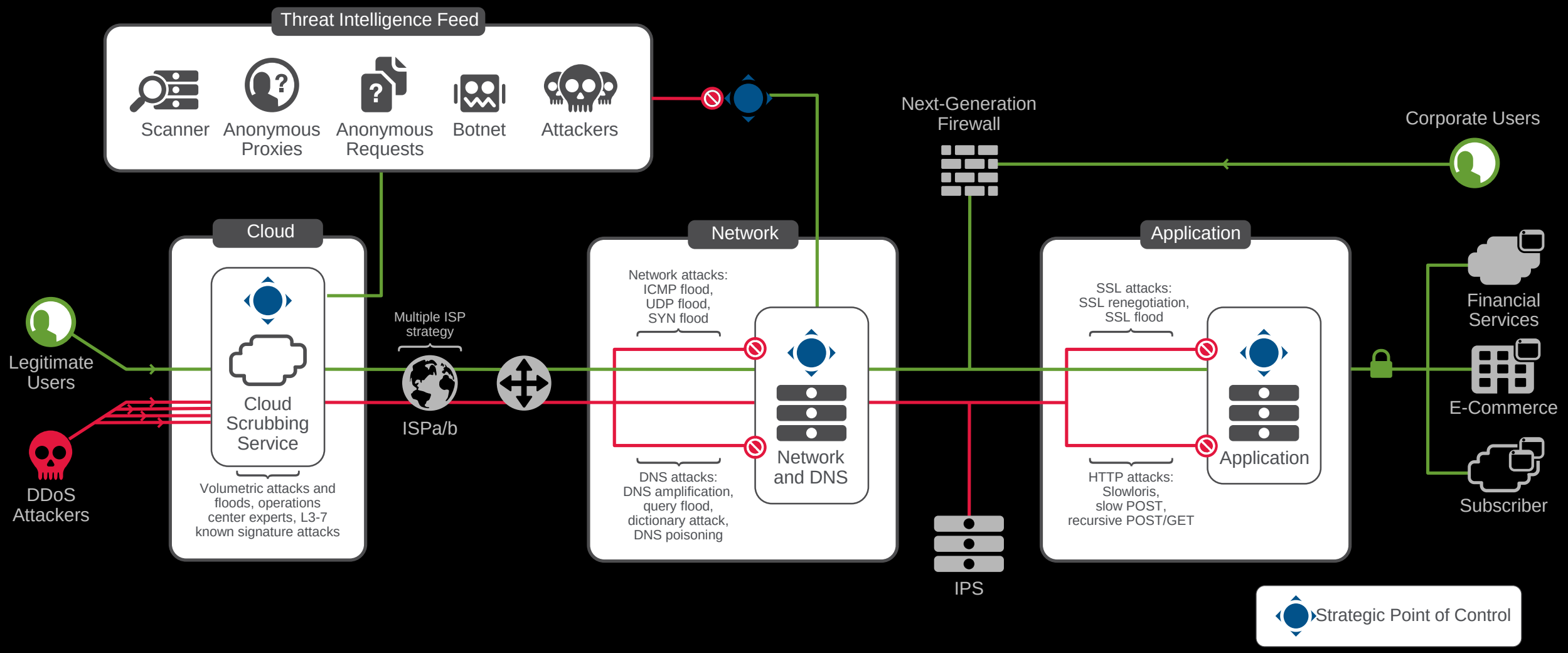
F5 ON-PREMISES DDOS PROTECTION

- Mitigate mid-volume, SSL, or application targeted attacks on-premises
- Complete infrastructure control
- Advanced L7 attack protections

Protect Your Business and Stay Online During a DDoS Attack

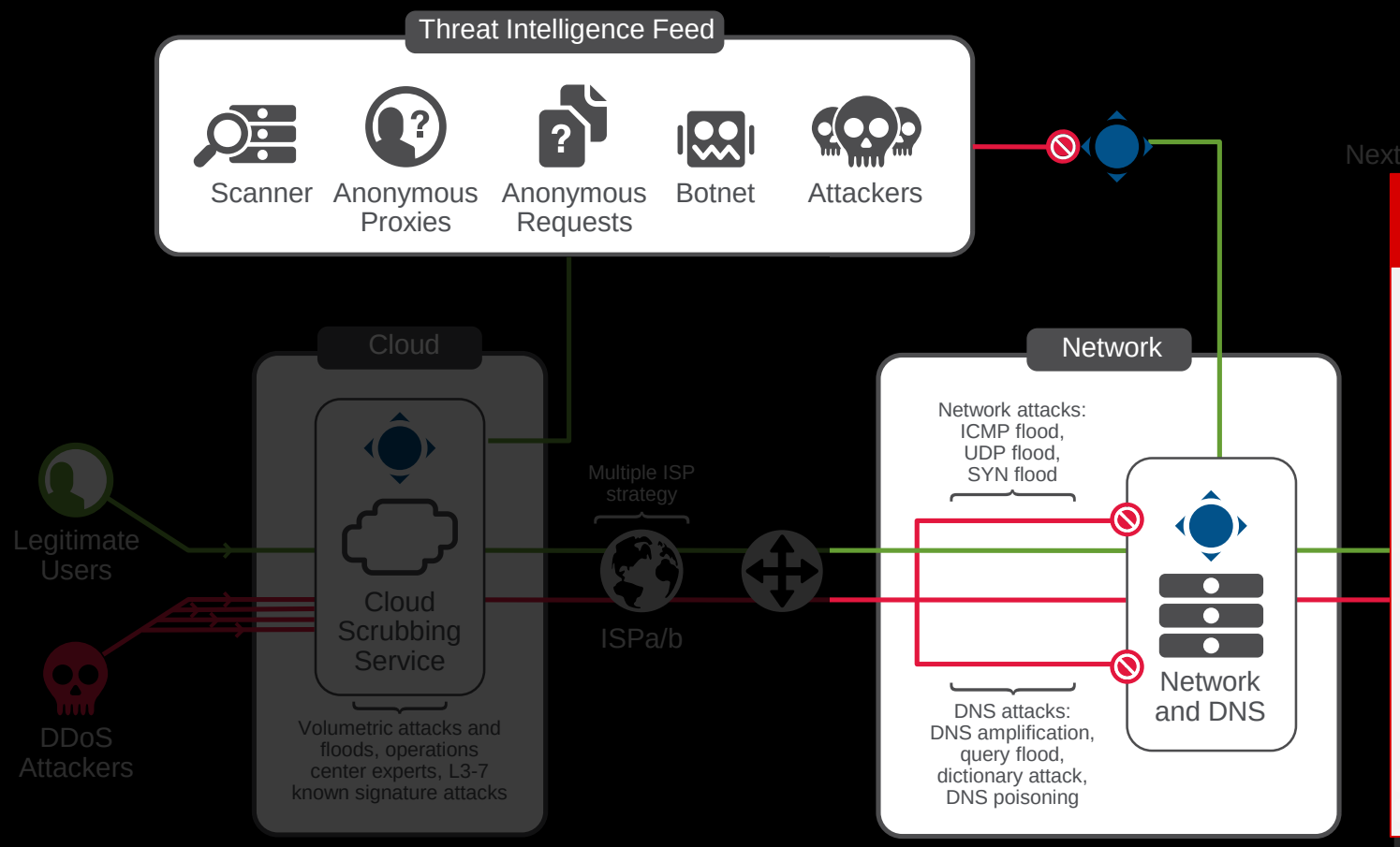
© 2016 F5 Networks

F5 Networks DDoS Protection - Reference Architecture



© 2016 F5 Networks

Network DDoS Mitigation

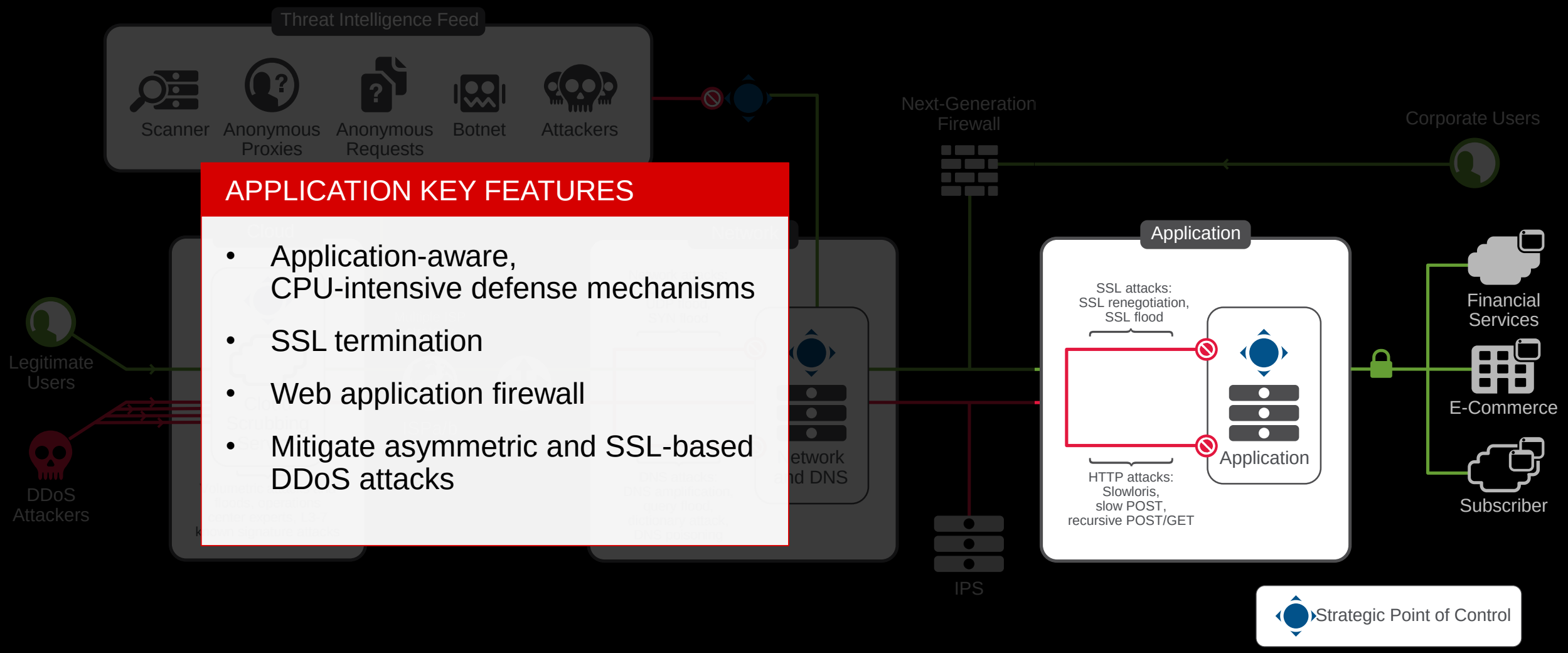


NETWORK KEY FEATURES

- The network tier at the perimeter is layer 3 and 4 network firewall services
- Simple load balancing to a second tier
- IP reputation database
- Mitigates transient and low-volume attacks

© 2016 F5 Networks

L7 DDoS Mitigation

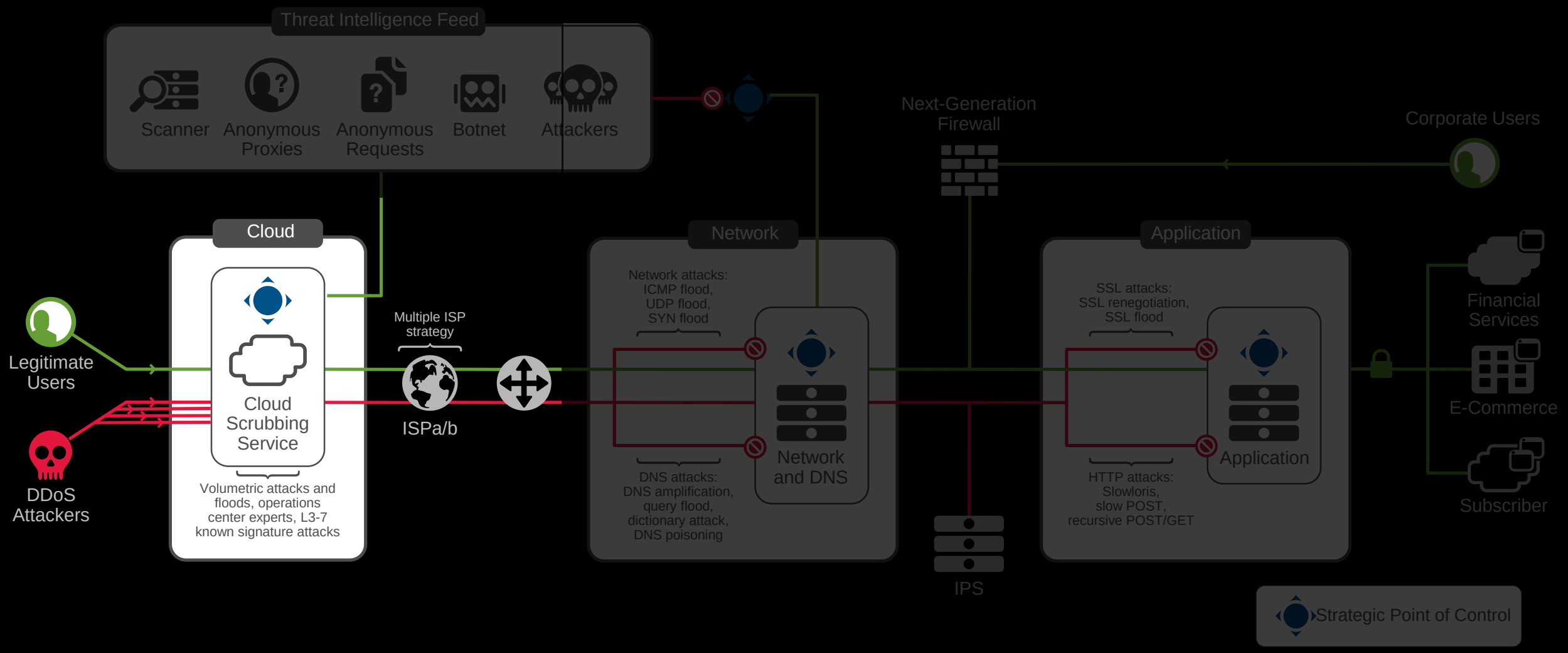


APPLICATION KEY FEATURES

- Application-aware, CPU-intensive defense mechanisms
- SSL termination
- Web application firewall
- Mitigate asymmetric and SSL-based DDoS attacks

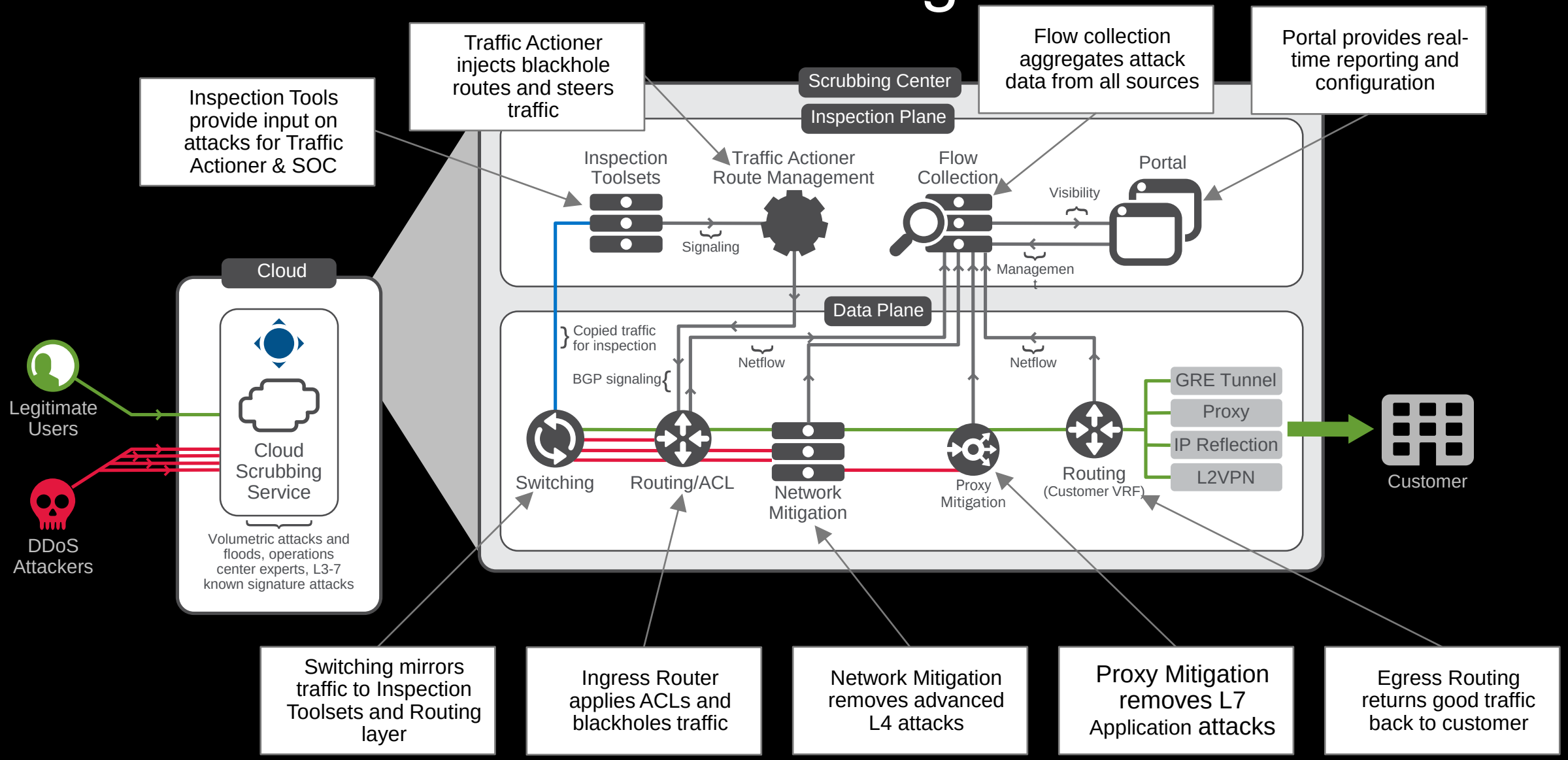
© 2016 F5 Networks

Cloud DDoS Protection



© 2016 F5 Networks

DDoS Architecture Scrubbing Center



© 2016 F5 Networks

IPv6

IPv6 Story

- RFC2460 – 12/1998
- Challenges
  - Operational
  - Security
- F5 Solution
  - Network
  - DNS

© 2016 F5 Networks

IPv6 Operational Challenges

- Many devices and content will not be IPv6 ready
  - IPv4 and IPv6 are not backwards compatible
- Implement a strategy where both IPv4 and IPv6 co-exist until a complete migration to IPv6
  - IPv4 address management
  - IPv6 migration
- Manage the depletion of IPv4 addresses in
- How to connect IPv6 client to IPv4 services and vice versa
- How to publish IPv4 services for IPv4 client

© 2016 F5 Networks

IPv6 Security Challenges

- Who really knows IPv6?
- Does your firewall vendor really support IPv6?
- Visibility on IPv6
- IPv6 DDoS Mitigation

© 2016 F5 Networks

F5 IPv6 Answers

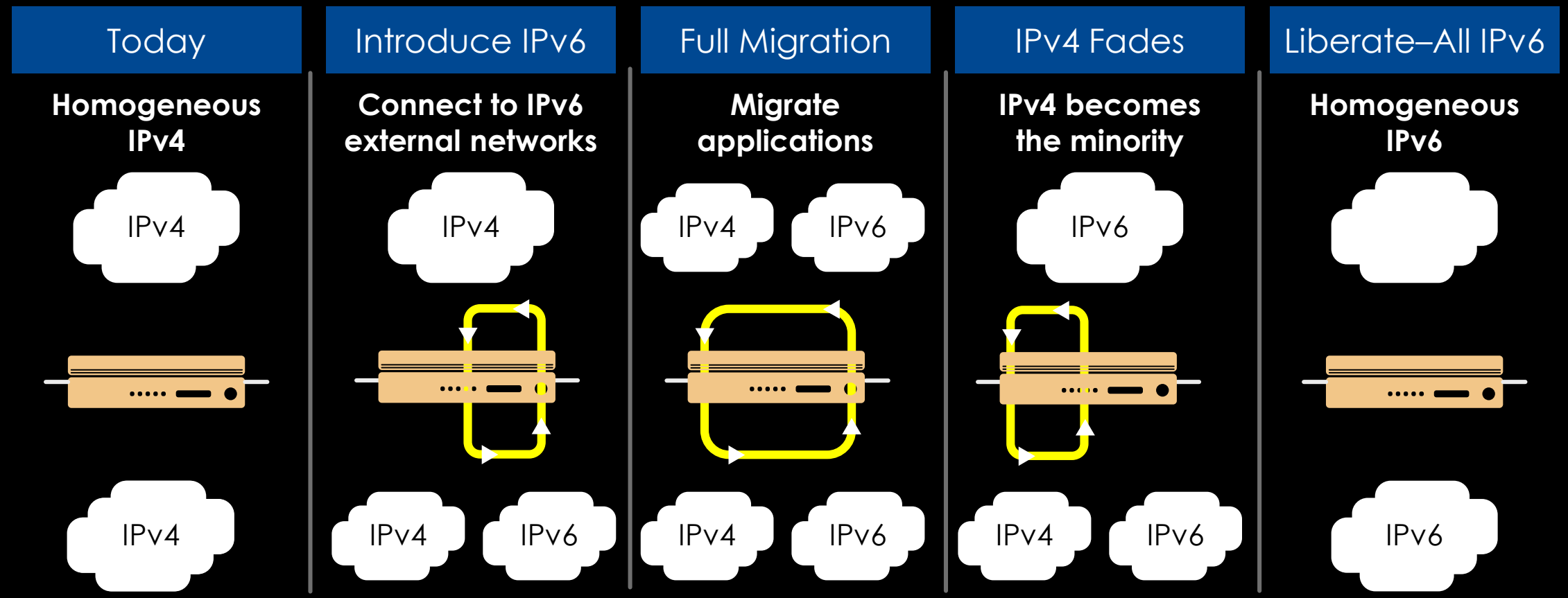
- Full IPv6 support
- Internal communication on IPv6
- Full Proxy
  - DNS/GTM module
  - Firewall Module
  - ADC Module

F5 Full-Proxy Architecture

© 2016 F5 Networks

IPv4 to IPv6 Network Migration Model

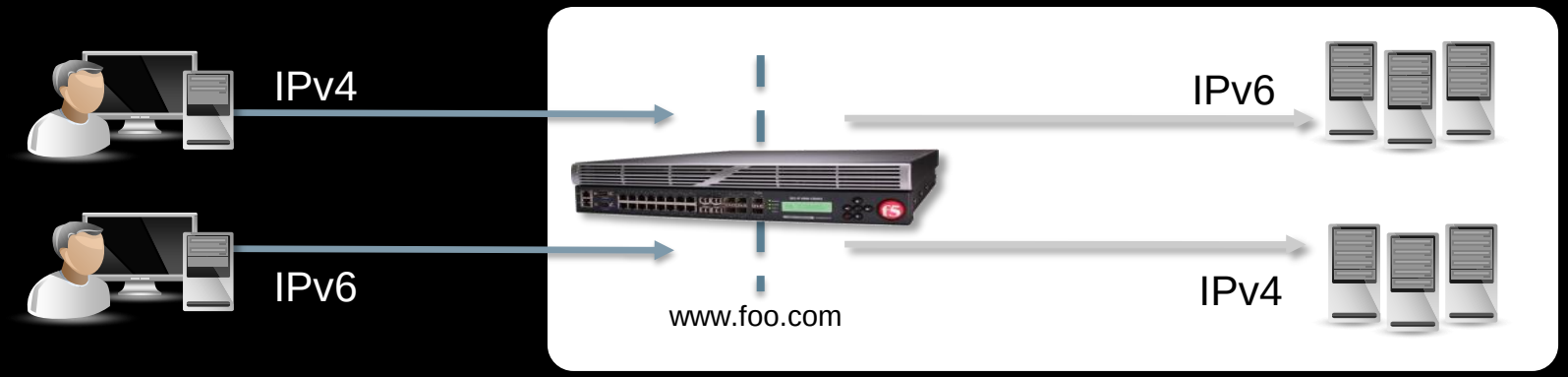
Network migration and application migration



© 2016 F5 Networks

IPv6 and IPv4 Support Included

Simplify IPv6 migrations with an IPv4 / IPv6 gateway



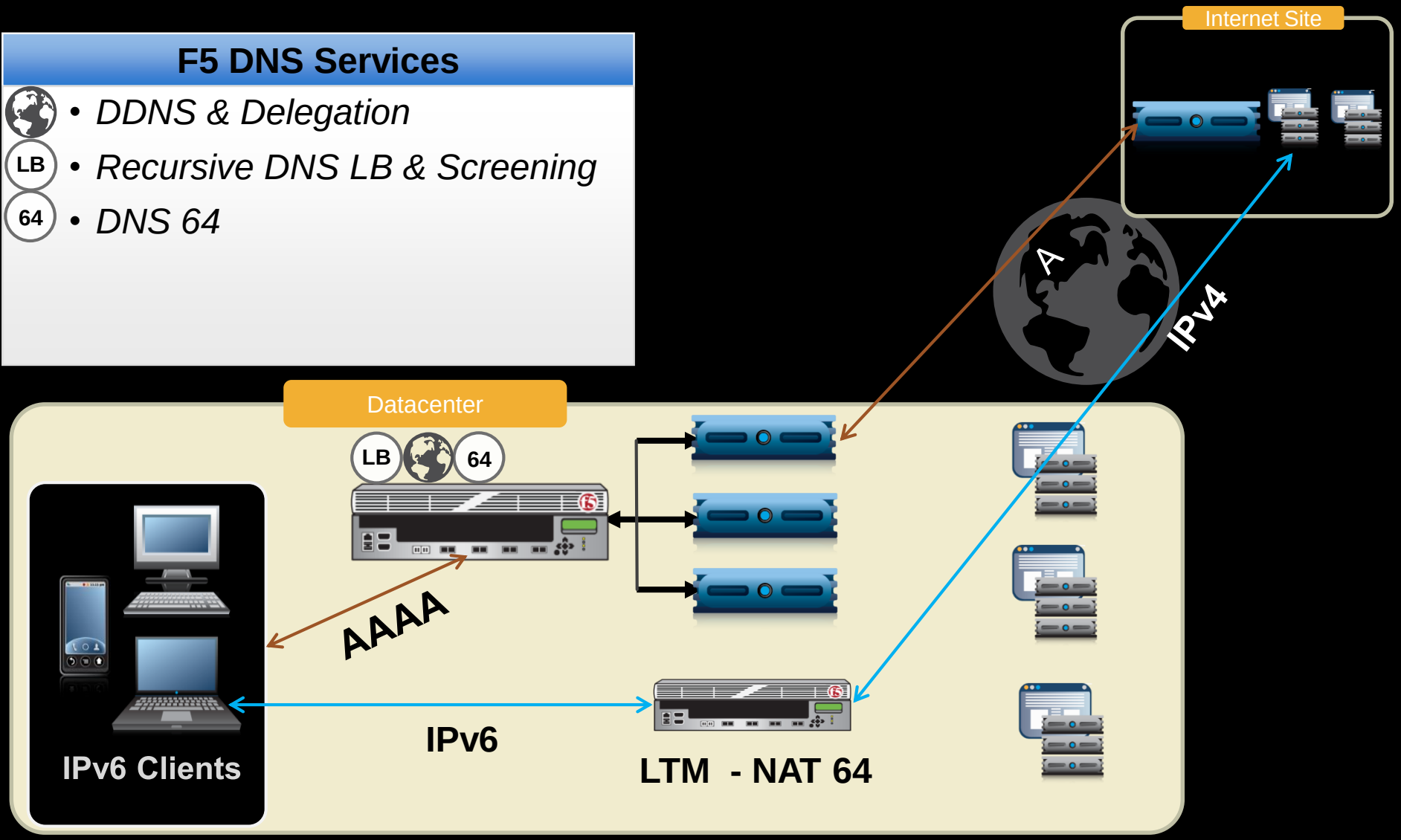
- No need to tunnel
- “no dual stack clients or servers required”
- NAT IPv4 to IPv6 (and vice-versa)
  - Clients can be a mix of IPv4 and IPv6
  - Servers can be a mix of IPv4 and IPv6
- DNS 4-6 / 6-4

© 2016 F5 Networks

DNS 64: IPv6 AAAA to IPv4 A

F5 DNS Services

- *DDNS & Delegation*
- *Recursive DNS LB & Screening*
- *DNS 64*



© 2016 F5 Networks

Deployments of FW+ADC

AFM Benefits

Consolidated datacenter security and application protection

App-centric policy enforcement

- Application access controls
- Simplified policy management
- Extensibility with iRules

DoS protection

- Secure against L3-L4 D/DOS attacks
- 120+ DoS vectors & Hardware-based DoS protections
- Dynamic IP intelligence & Blacklisting
- RTBH & Accelerated IP Shun (auto-blacklisting)
- Port misues policy

Manageability and Visibility

- High speed customizable FW logs/Syslogs
- Granular reporting on attacks
- Centrally managed with BIG-IQ
- On-demand rules compilation
- Self-tuning DDoS threshold settings
- Simplified NAT/PAT work flows

© 2016 F5 Networks

AFM Benefits

Policies written specifically for applications rather than against network traffic.

- Attaches **policies to the applications** that traffic is ultimately directed towards
- Provides a richer set of attributes and objects for each policy context
- 3-tiered hierarchical policy context
- HTTP, SMTP, FTP, SIP, DNS **protocol validation** and **enforcement** on granular details
- **Streamlines rule** life-cycle **management**, reduces misconfiguration, and increases policy effectiveness and visibility

© 2016 F5 Networks

LTM Benefits

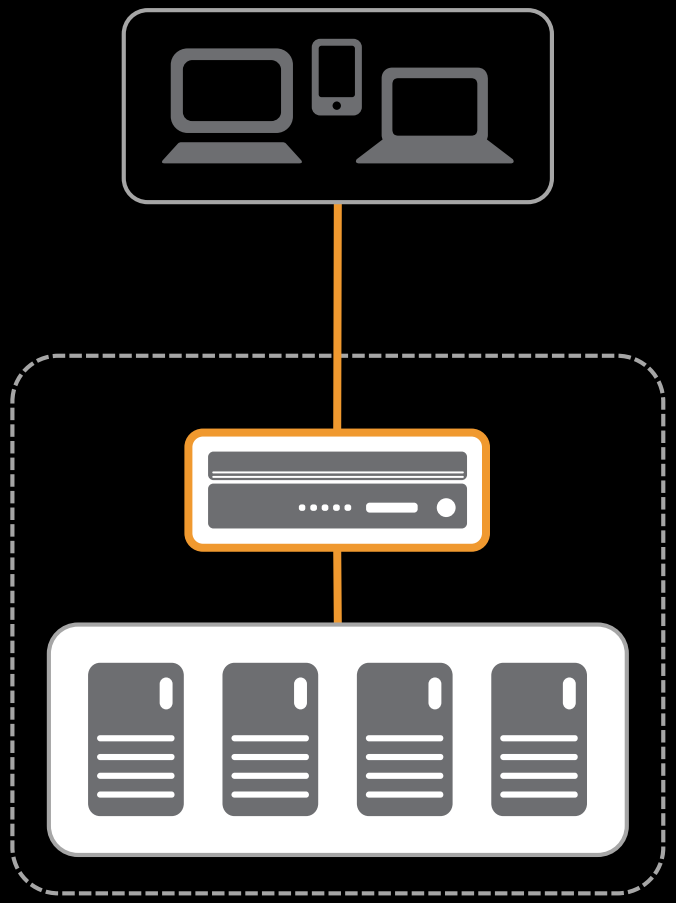
Application Fluency

Load Balance

Distribute application load across multiple servers to increase availability

Health Monitoring

Verify health and performance to check the status of applications and resources



Traffic Steering

Direct a particular type of traffic to resources designed to handle that type of workload

Connection Management

Mirror connection and persistence information to prevent interruption in service

© 2016 F5 Networks

LTM Benefits

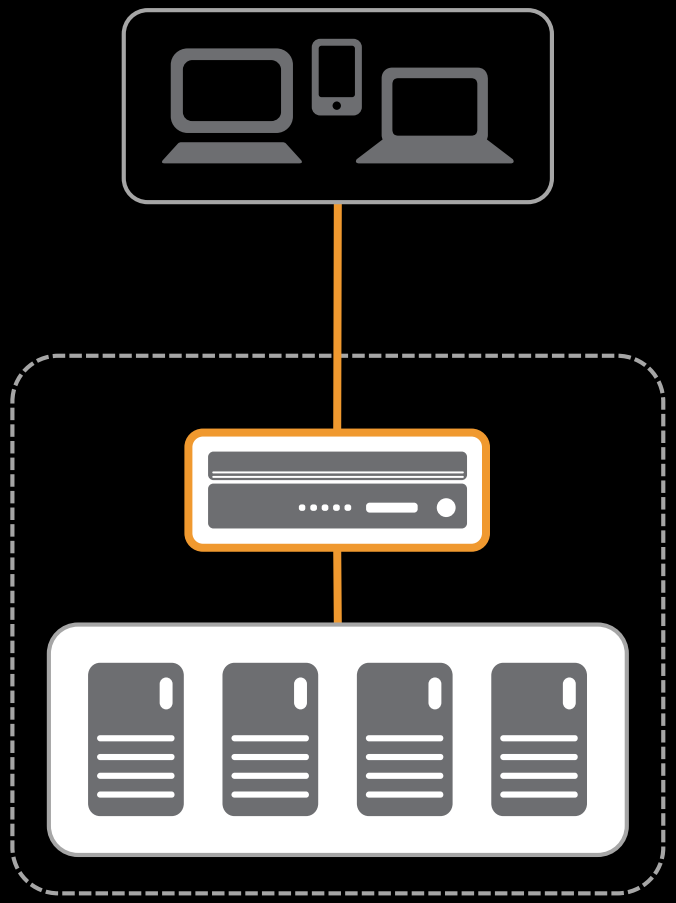
Performance Optimization

TCP Optimization

Enable state-of-the-art optimization to dramatically improve mobile performance

Emerging Protocols

Leverage new technologies like SPDY, HTTP/2 and WebSockets without re-architecting



Caching

Offload repetitive traffic from application servers to improve performance and scale

Compression

Compress data from applications to reduce traffic and overcome latency

© 2016 F5 Networks

LTM Benefits

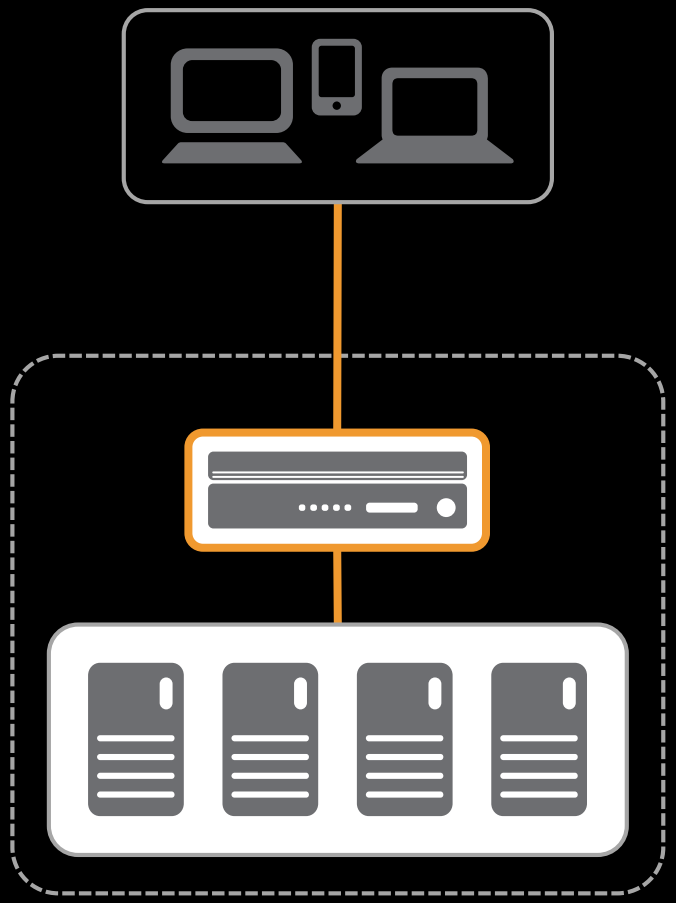
SSL Encryption

Data Protection

Encrypt traffic with a choice of ciphers suites based on policy, compliance, or mobile needs

Perfect Forward Secrecy

Protect customer privacy from future decryption with a unique key for each session



Visibility and Control

Remove the blind spot that is created by encryption for inbound and outbound traffic

Key Protection

Protect and manage keys with hardware security modules for physical, virtual, and AWS cloud

© 2016 F5 Networks

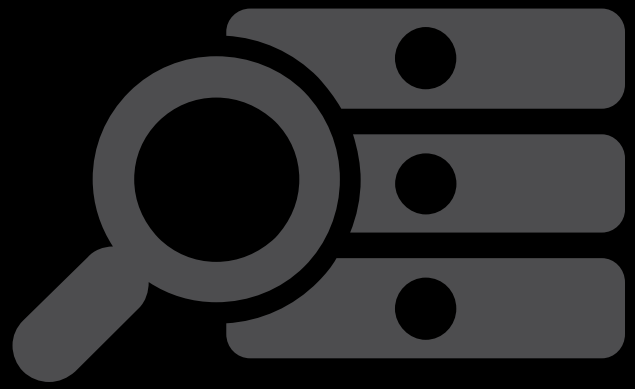
FW+ADC Performance

- Network accelerators
- SSL accelerators
- Compression HW
- No useless NGFW features
- Full Proxy
- TMOS

© 2016 F5 Networks

FW+ADC Visibility

- Full network data visibility
- SSL offload and termination
- Provides visibility for 3rd party security devices (IPS, NGFW)
- Emerging protocols
  - HTTP/2
  - SPDY
  - WebSockets
- Protocol Security
  - DNS Tunneling
  - SSH Proxy
- Magic and Miracles



© 2016 F5 Networks

FW+ADC Flexibility

- iRules
  - Data Plane - Inspect, transform, and make decisions based application traffic
- iControl
  - Management API - Realize new levels of automation and configuration management
- TMSH/iCall
  - Control Plane - Automate tasks based on events to improve operations and resouce utilization
- iApps
  - Application Policies - Define and deploy security, optimization and availability services for applications

01001
11010
10010

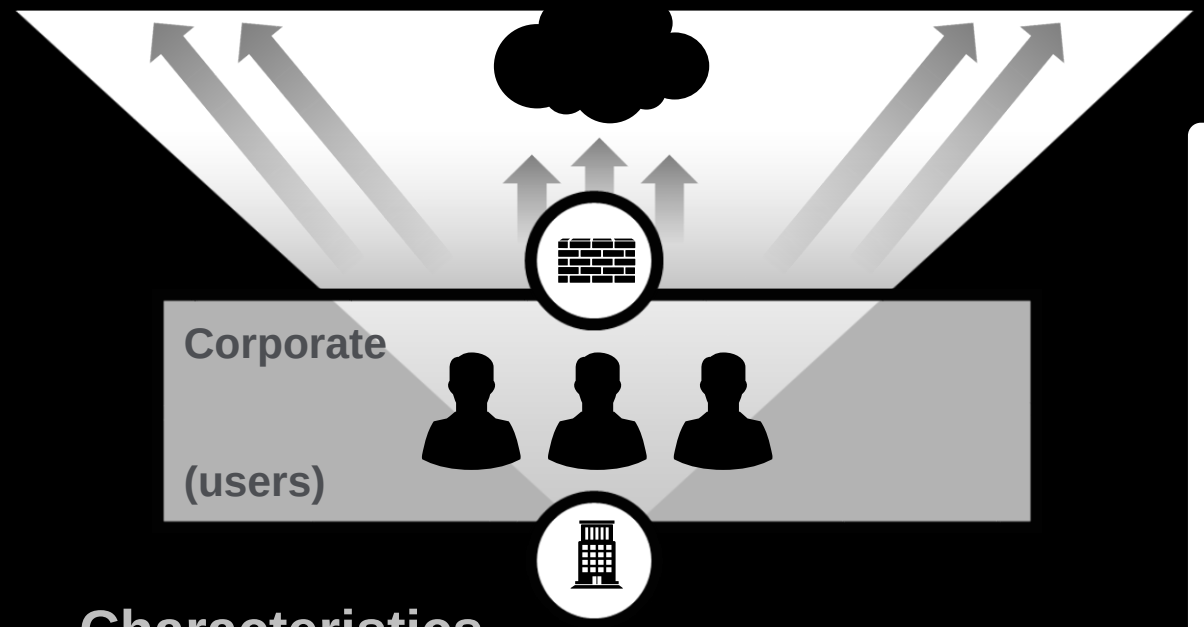
© 2016 F5 Networks

F5 Application Delivery Firewall

© 2016 F5 Networks

Using the Right Tool

"Next generation" firewall

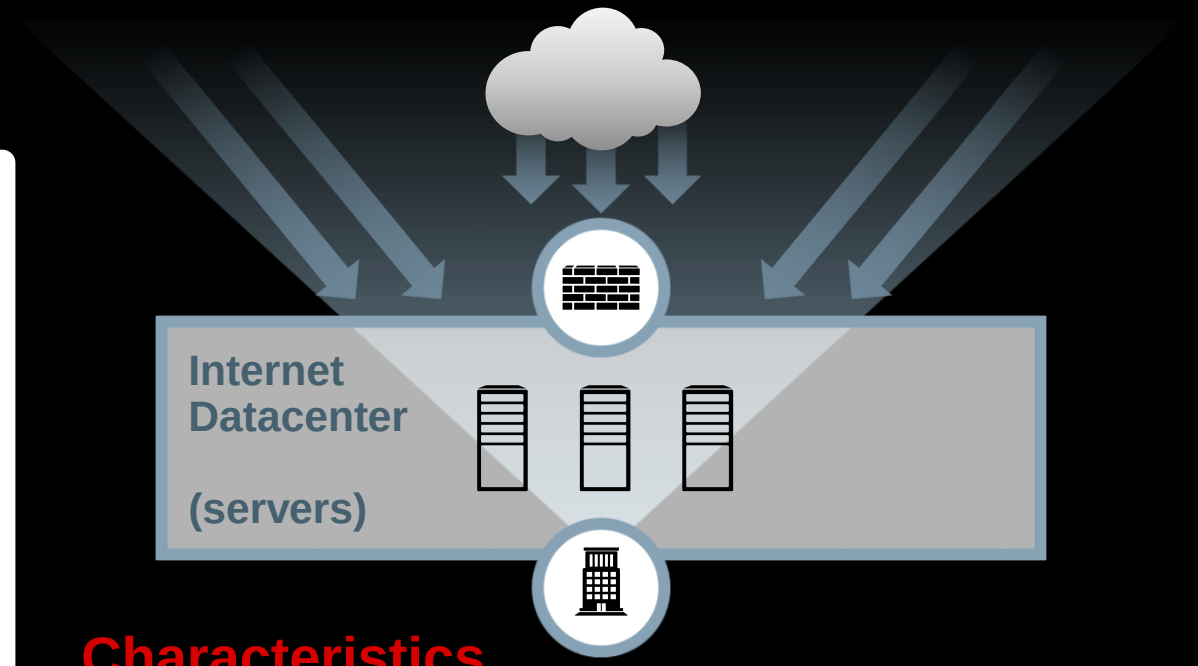


Characteristics

- **Outbound** user inspection
- UserID and AppID
- Who is doing what?
- 1K users to 10K web sites
- Broad but shallow

BIFURCATION OF FIREWALLS

F5 Application Delivery Firewall



Characteristics

- **Inbound** application protection
- Application delivery focus
- 1M users to 100 apps
- Narrow but deep
- 12 protocols (HTTP, SSL, etc.)

© 2016 F5 Networks

Using the Right Tool

"Next generation" firewall

Secures Users when they are on the corporate network

Characteristics

- **Outbound** user inspection
- UserID and AppID
- Who is doing what?
- 1K users to 10K web sites
- Broad but shallow

BIFURCATION OF FIREWALLS

F5 Application Delivery Firewall

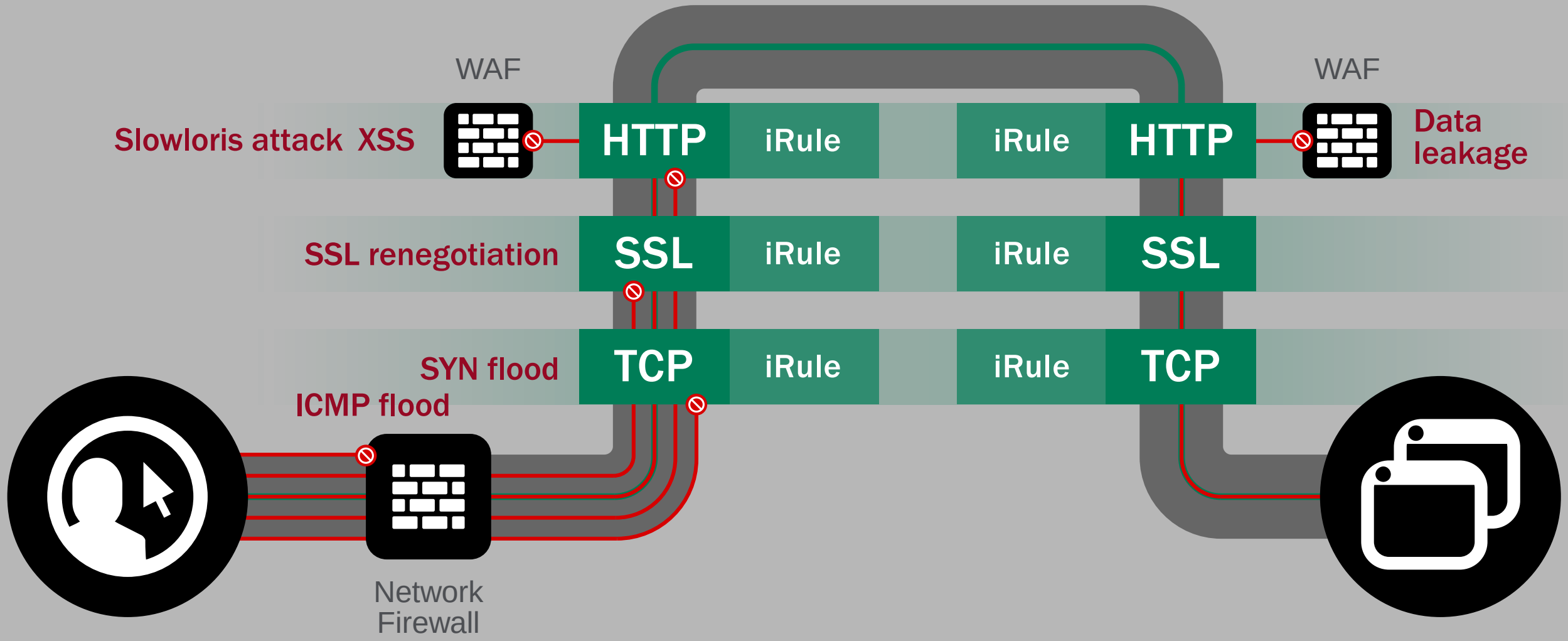
Secures Apps wherever they Live

Characteristics

- **Inbound** application protection
- Application delivery focus
- 1M users to 100 apps
- Narrow but deep
- 12 protocols (HTTP, SSL, etc.)

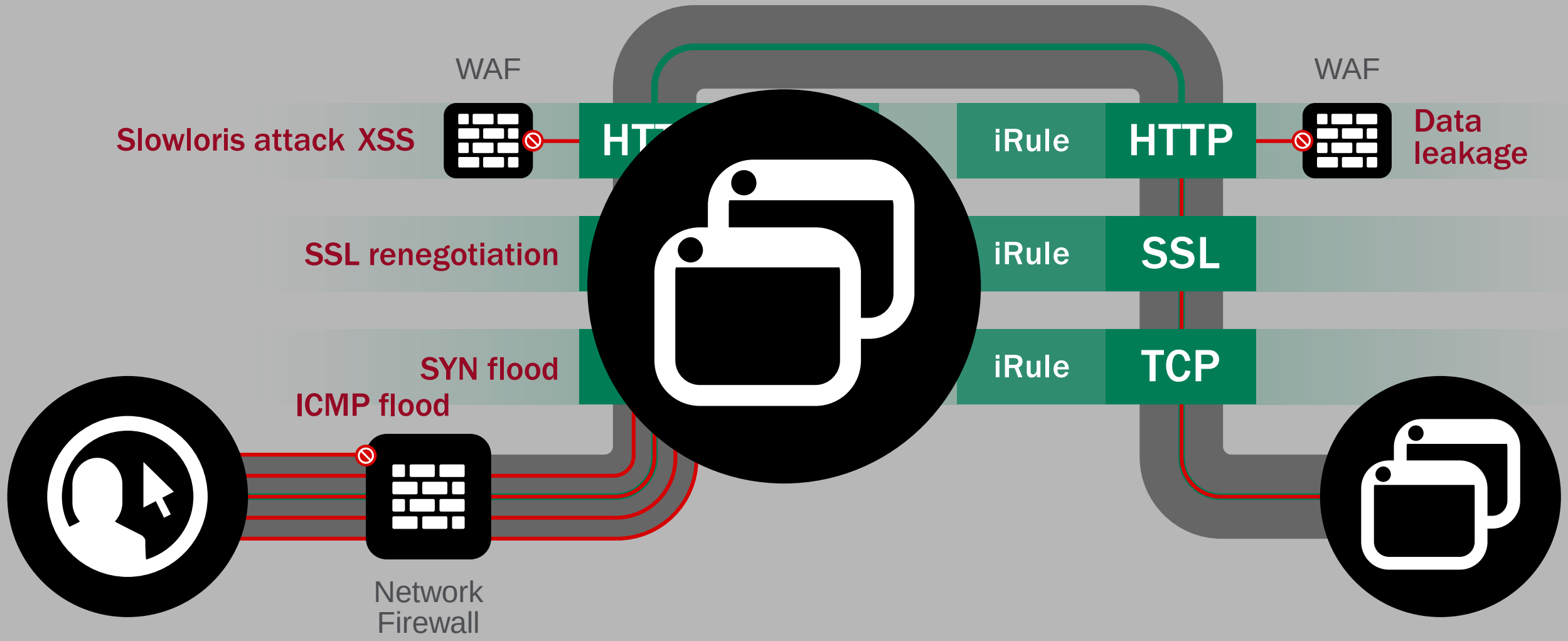
© 2016 F5 Networks

F5 Full Proxy Architecture



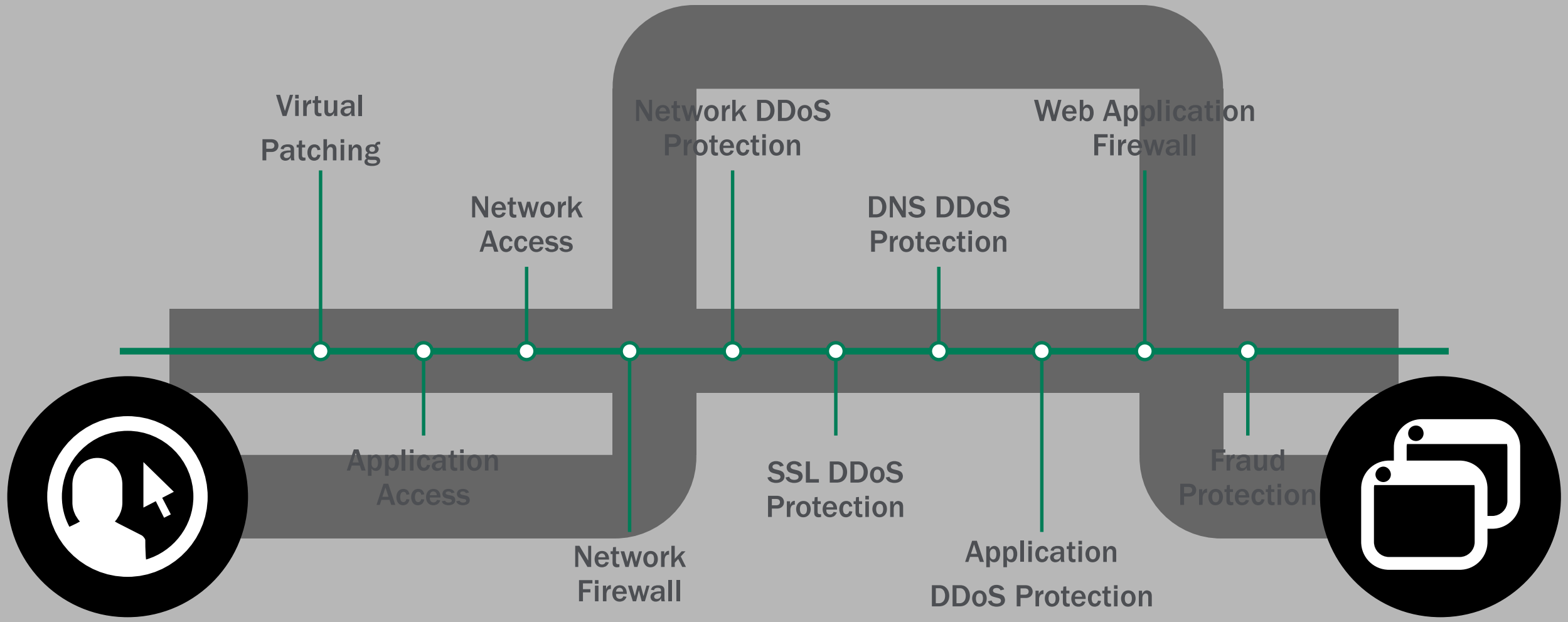
© 2016 F5 Networks

F5 Full Proxy Architecture



© 2016 F5 Networks

F5 Full Proxy Architecture



© 2016 F5 Networks

F5 Synthesis	https://synthesis.f5.com/
DevCentral	https://devcentral.f5.com/
AskF5/Support	https://ask.f5.com/
iHealth	https://ihealth.f5.com/
University	https://university.f5.com/

For further assistance please, contact me:

l.klokner@f5.com | +421 908 755152

SOLUTIONS FOR AN APPLICATION WORLD

BACKUP SLIDES

© 2016 F5 Networks

F5 On-premises DDoS protection

DDoS vectors hardware accelerated

Over 110+ L2/4 DDoS vectors with majority of them mitigated in hardware (IPI also).

Even with vCMP enabled.

Solutions Products Community Support Partners Education About Us

SUPPORT

LOGIN SELF-HELP DOCUMENTATION SERVICES DOWNLOADS

DOS CATEGORY	ATTACK NAME	DOS VECTOR NAME	INFORMATION	HARDWARE ACCELERATED
Bad Header - DNS	DNS Oversize	dns-oversize	Detects oversized DNS headers. To tune this value, in tmsh: `modify sys db dos.maxdnssize value` , where **value** is **256-8192**.	Yes
	DNS Malformed	dns-malformed	Malformed DNS packet	Yes
	DNS QDCount Limit	dns-qdcount-limit	UDP packet, DNS qdcount neq 1, VLAN is <tunable>. To tune this value, in **tmsh**: `modify sys db dos.dnsvlan value` , where **value** is **0-4094**.	Yes
Bad Header - ICMP	Bad ICMP Checksum	bad-icmp-chksum	An ICMP frame checksum is bad. Reuse the TCP or UDP checksum bits in the packet	Yes
	Bad ICMP Frame	bad-icmp-frame	The ICMP frame is either the wrong size, or not of one of the valid IPv4 or IPv6 types. Valid IPv4 types: • 0 Echo Reply • 3 Destination Unreachable • 4 Source Quench • 5 Redirect • 8 Echo • 11 Time Exceeded • 12 Parameter Problem • 13 Timestamp • 14 Timestamp Reply • 15 Information Request • 16 Information Reply • 17 Address Mask Request • 18 Address Mask Reply Valid IPv6 types: • 1 Destination Unreachable • 2 Packet Too Big	Yes

© 2016 F5 Networks

Demo TCP SYN Flood - Attack Mitigated in Hardware!

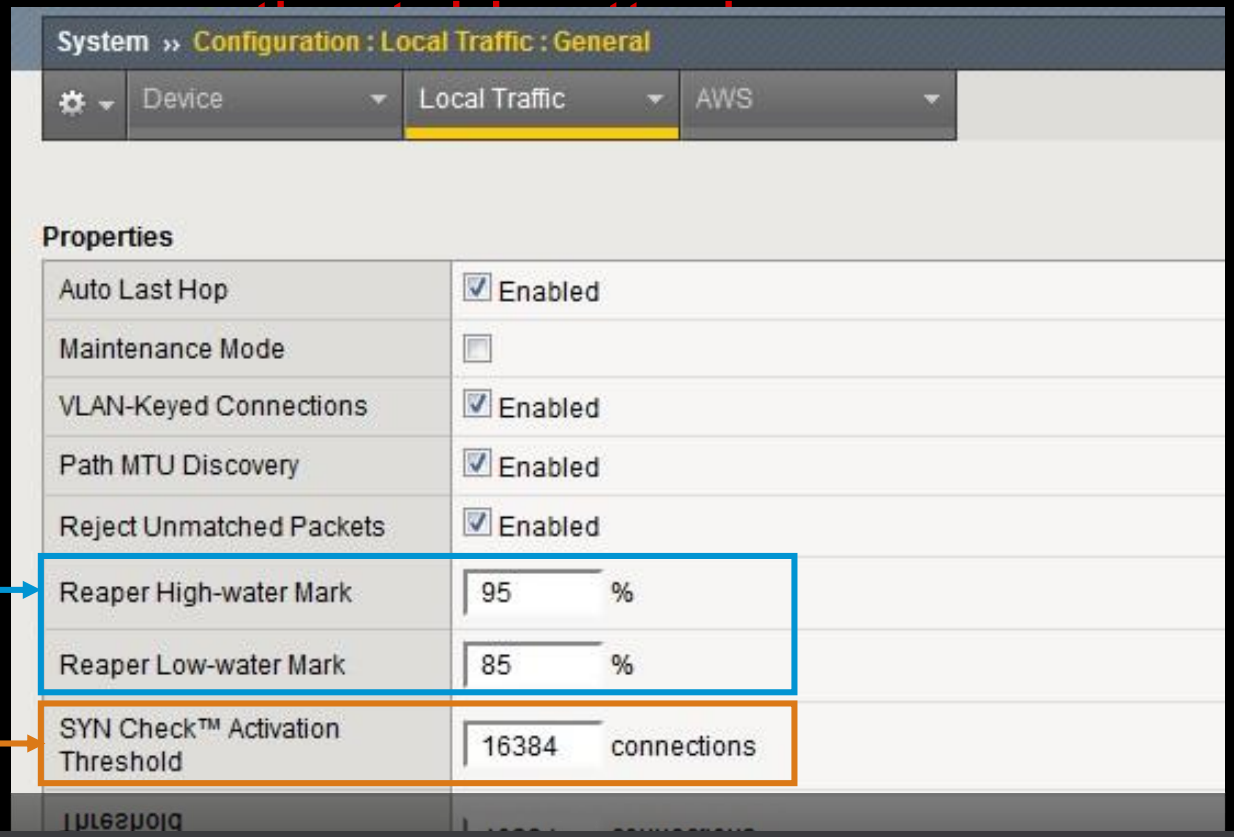
Using LTM flow reaper to mitigate

Reaper Threshold

- Controls when connection reaping occurs
- Uses variety of algorithms
  - 1st: Longest Idle Connections
  - 2nd: Bps/PPS/Throughput Statistics
  - 3rd: Random Eviction
- Always avoids reaping BigIP-initiated connections

TCP SYN Cookies to challenge Client TCP stacks

- Configurable Threshold (Global)
  - Kicks in only when needed



Future Plans

- Per-VS Connection Table Quotas for both ALL flows, and for “Slow” Flows
- Additional User-Specified Reap Choices: Geo-based, Port-Based, Oldest

© 2016 F5 Networks

TCP SYN Flood - AFM signatures mitigation

Main | Help | About

Security » DoS Protection : Device Configuration

DoS Profiles | Device Configuration | White List

- Statistics
- iApps
- DNS
- Local Traffic
- Traffic Intelligence
- Acceleration
- Device Management
- Security
  - Overview
  - Application Security
  - Protocol Security
  - Network Firewall
  - Network Address Translation
  - DoS Protection
  - Event Logs
  - Reporting
  - Security Updates
  - Options
- Network
- System

Properties

Log Publisher	None
Auto Threshold Sensitivity	1 — 50 — 100 (50)

Update

Category	Attack Type	Detection Threshold PPS	Detection Threshold Percent	Rate/Leak Limit	Auto Threshold	Bad Actor
Bad Header - DNS						
Bad Header - ICMP						
Bad Header - IGMP						
Bad Header - IPv4						
Bad Header - IPv6						
Bad Header - L2						
Bad Header - TCP						
Bad Header - UDP						
DNS						
Flood						
	ARP Flood	10000	500	100000		
	Ethernet Broadcast Packet	10000	500	100000		
	Ethernet Multicast Packet	10000	500	100000		
	ICMPv4 flood	10000	500	100000		
	ICMPv6 flood	10000	500	100000		
	IGMP Flood	10000	500	100000		
	IGMP Fragment Flood	100	500	1000		
	IPv6 Fragment Flood	Infinite	Infinite	Infinite		
	IP Fragment Flood	Infinite	Infinite	Infinite		
	Routing Header Type 0	10000	500	100000		
	TCP BADACK Flood	1000	500	10000		
	TCP PUSH Flood	Infinite	Infinite	Infinite		
	TCP RST Flood	10000	500	100000		
	TCP SYN ACK Flood	500000	Infinite	Infinite		
	TCP SYN Flood	90000	Infinite	Infinite		

© 2016 F5 Networks

Network DDoS Attacks - F5 signatures

Category
Bad Header - DNS
Bad Header - ICMP
Bad Header - IGMP
Bad Header - IPv4
Bad Header - IPv6
Bad Header - L2
Bad Header - TCP
Bad Header - UDP
DNS
Flood
Fragmentation
Single Endpoint
SIP
Bad Header - SCTP
Other

Category	Attack Type	Detection Threshold PPS	Detection Threshold Percent	Rate/Leak Limit	Auto Threshold	Bad Actor
Bad Header - DNS						
	DNS Oversize	1000	500	10000		
	DNS Malformed	1000	500	10000		
	DNS QDCount Limit	1000	500	Infinite		
Bad Header - ICMP						
	Bad ICMP Checksum	10	500	100		
	Bad ICMP Frame	1000	500	10000		
	ICMP Frame Too Large	1000	500	10000		
Bad Header - IGMP						
	Bad IGMP Frame	1000	500	10000		
Flood						
	ARP Flood	10000	500	100000		
	Ethernet Broadcast Packet	10000	500	100000		
	Ethernet Multicast Packet	10000	500	100000		
	ICMPv4 flood	10	100	10		
	ICMPv6 flood	10000	500	100000		
	IGMP Flood	10000	500	100000		
	IGMP Fragment Flood	100	500	1000		
	IPv6 Fragment Flood	Infinite	Infinite	Infinite		
	IP Fragment Flood	Infinite	Infinite	Infinite		
	Routing Header Type 0	10000	500	100000		
	TCP BADACK Flood	1000	500	10000		
	TCP PUSH Flood	Infinite	Infinite	Infinite		
	TCP RST Flood	25	100	25		
	TCP SYN ACK Flood	500000	Infinite	Infinite		
	TCP SYN Flood	90000	Infinite	Infinite		
	TCP SYN Oversize	1000	500	10000		
	TCP Window Size	100000	500	Infinite		
	UDP Flood	400000	Infinite	Infinite		

© 2016 F5 Networks

Different Network DDoS Attacks

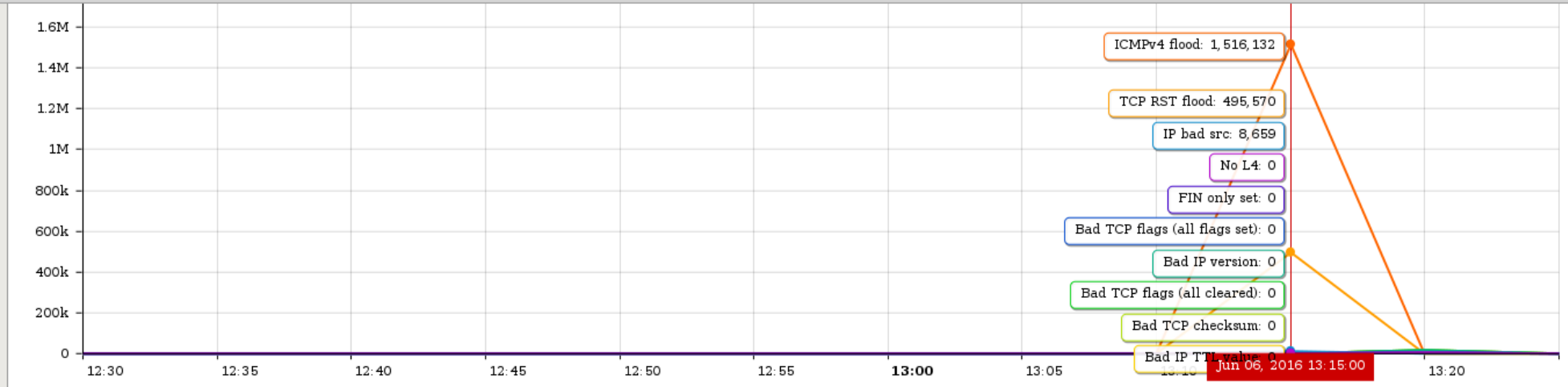
BIG-IP® - bigipA.f5demo.com (10.1.1.245) - Iceweasel

BIG-IP® - bigipA.f5de... | F5 Denial of Service De... | F5 Denial of Service De... | F5 Denial of Service De... | F5 Denial of Service De... | Using virtual server 10.1...

https://10.1.1.245/xui/

Device Management
Security
- Overview
- Application Security
- Protocol Security
- Network Firewall
- Network Address Translation
- DoS Protection
- Event Logs
- Reporting
- Security Updates
- Options

Network
System



Details

Attack Type	Allowed Requests	Dropped Requests	▼ Total Requests
ICMPv4 flood	339	1,515,829	1,516,168
TCP RST flood	287	495,283	495,570
Bad IP TTL value	0	16,094	16,094
Bad TCP checksum	0	16,066	16,066
Bad TCP flags (all cleared)	0	16,043	16,043
Bad IP version	0	16,039	16,039
IP bad src	0	8,659	8,659
Bad TCP flags (all flags set)	0	8,454	8,454
FIN only set	0	8,435	8,435
No L4	2,156	1,699	3,855
Overall	2,782	2,120,050	2,122,832

© 2016 F5 Networks

DNS DDoS Mitigation - AFM: DDoS Singnatures

Category	Attack Type	Detection Threshold PPS	Detection Threshold Percent	Rate/Leak Limit	Auto Threshold	Bad Actor
DNS						
	DNS AAAA Query	50000	500	Infinite		
	DNS Any Query	500	500	2000		
	DNS AXFR Query	5000	500	Infinite		
	DNS A Query	50000	500	Infinite		
	DNS CNAME Query	5000	500	Infinite		
	DNS IXFR Query	5000	500	Infinite		
	DNS MX Query	50000	500	Infinite		
	DNS NS Query	5000	500	Infinite		
	DNS OTHER Query	5000	500	Infinite		
	DNS PTR Query	50000	500	Infinite		
	DNS Response Flood	10000	500	Infinite		
	DNS SOA Query	5000	500	Infinite		
	DNS SRV Query	50000	500	Infinite		
	DNS TXT Query	500	500	2000		

© 2016 F5 Networks

DNS DDoS Mitigation

AFM: Stateless App. Layer DoS Detection

Protocol Errors Attack Detection

☑ Enabled
Rate threshold: 250000 packets per second
Rate increased by: 500 %

SIP Method Attack Detection

Method Type	Detection Status	Threshold	Rate Increase
invite	☑ Enabled	250000 packets per second	500 %
ack	☐ Enabled	250000 packets per second	500 %
options	☐ Enabled	250000 packets per second	500 %
bye	☐ Enabled	250000 packets per second	500 %
cancel	☐ Enabled	250000 packets per second	500 %
register	☐ Enabled	250000 packets per second	500 %
publish	☐ Enabled	250000 packets per second	500 %
notify	☐ Enabled	250000 packets per second	500 %
subscribe	☐ Enabled	250000 packets per second	500 %
message	☐ Enabled	250000 packets per second	500 %
prack	☐ Enabled	250000 packets per second	500 %
other	☐ Enabled	250000 packets per second	500 %

Malformed/Protocol Violations Detection

DNS DOS Detection by Query Type

When to *report* and attack. Absolute and Relative Increase Detection Thresholds

Protocol Errors Attack Detection

☐ Enabled
Rate increased by: 500 %

DNS Query Attack Detection

Query Type	Detection Status	Threshold	Rate Increase
a	☐ Enabled	250000 packets per second	500 %
ptr	☐ Enabled	250000 packets per second	500 %
ns	☐ Enabled	250000 packets per second	500 %
soa	☐ Enabled	250000 packets per second	500 %
cname	☐ Enabled	250000 packets per second	500 %
mx	☐ Enabled	250000 packets per second	500 %
aaaa	☐ Enabled	250000 packets per second	500 %
txt	☐ Enabled	250000 packets per second	500 %
srv	☐ Enabled	250000 packets per second	500 %
axfr	☐ Enabled	250000 packets per second	500 %
ixfr	☐ Enabled	250000 packets per second	500 %
any	☑ Enabled	250000 packets per second	500 %
other	☐ Enabled	250000 packets per second	500 %

SIP DOS Detection by Method

When to *report* and attack

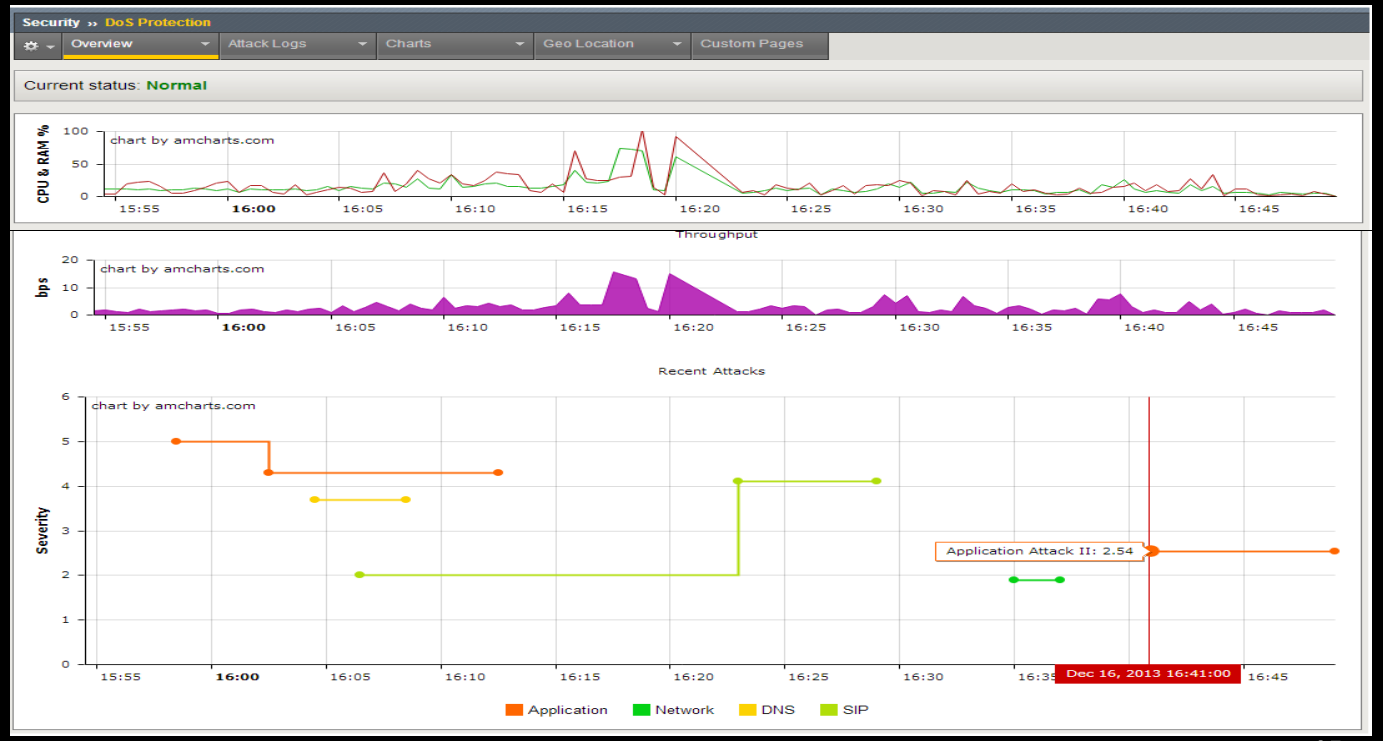
Absolute and Relative Increase Detection Thresholds

© 2016 F5 Networks

Application DDoS Mitigation - ASM

Layer 7 HTTP/S DoS attack protection

- Guards against RPS (TPS) and latency-based anomalies
- Provides predictive indicators
- Support IP, geolocation, URL and site wide detection criteria
- Provides heavy URL protection
- Protects against threats proactively
- Simplified reports access and added qkView violations export support
- Advanced Prevention techniques
- Client Side Integrity Defense
- CAPTCHA (HTML or JS response)
- Source IP Blocking
- Geolocation blacklisting



© 2016 F5 Networks