



Silverline - A Cloud Security Solution from F5

2016

Martin Budd – UKISSA Security Sales Manager

The Evolution Of Attackers

September 1996

First high profile DDoS attack. NY ISP Panix.com that was nearly put out of business.

January 2008

Anonymous executes a series of high-profile DDoS attacks against the Church of Scientology.

December 2010

WikiLeaks supporters hit PayPal, Visa, Mastercard, and other financial sites with DDoS attacks.

April 2011

Attackers use a DDoS attack against Sony to mask the theft of millions of customer records.

April 2012

Anonymous knocks down the sites of the U.S. Dept. of Justice, the CIA, and the British Secret Intelligence Service.

September 2012

Izz ad Din al Qassam Cyber Fighters Launch Operation Ababil with DDoS attacks on 13 U.S. banks to protest an anti-Muslim video.

1996

...

2008

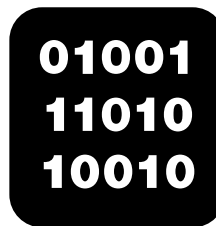
2009

2010

2011

2012

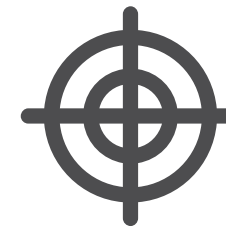
2013



Script
kiddies

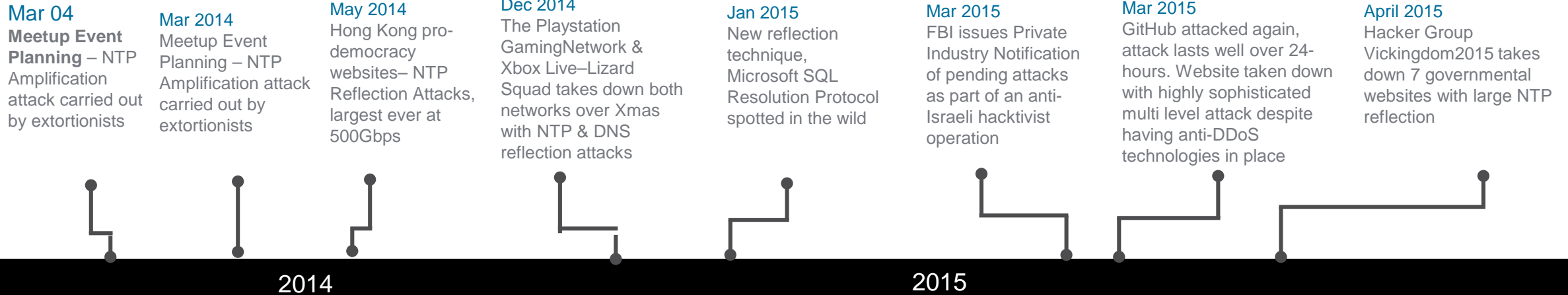


The rise
of hacktivism



Cyber
war

The Evolution Of Attackers



Reflection Attacks

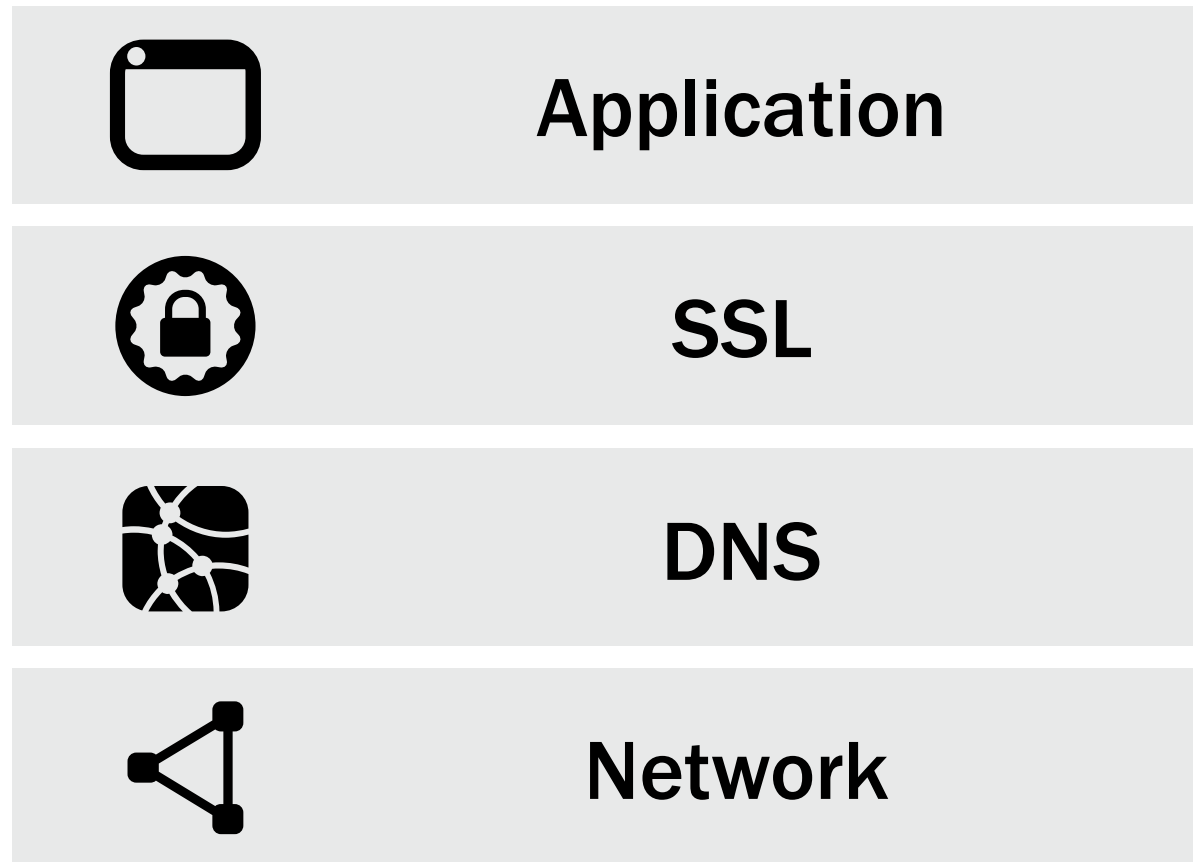


DDoS Extortion Attempts

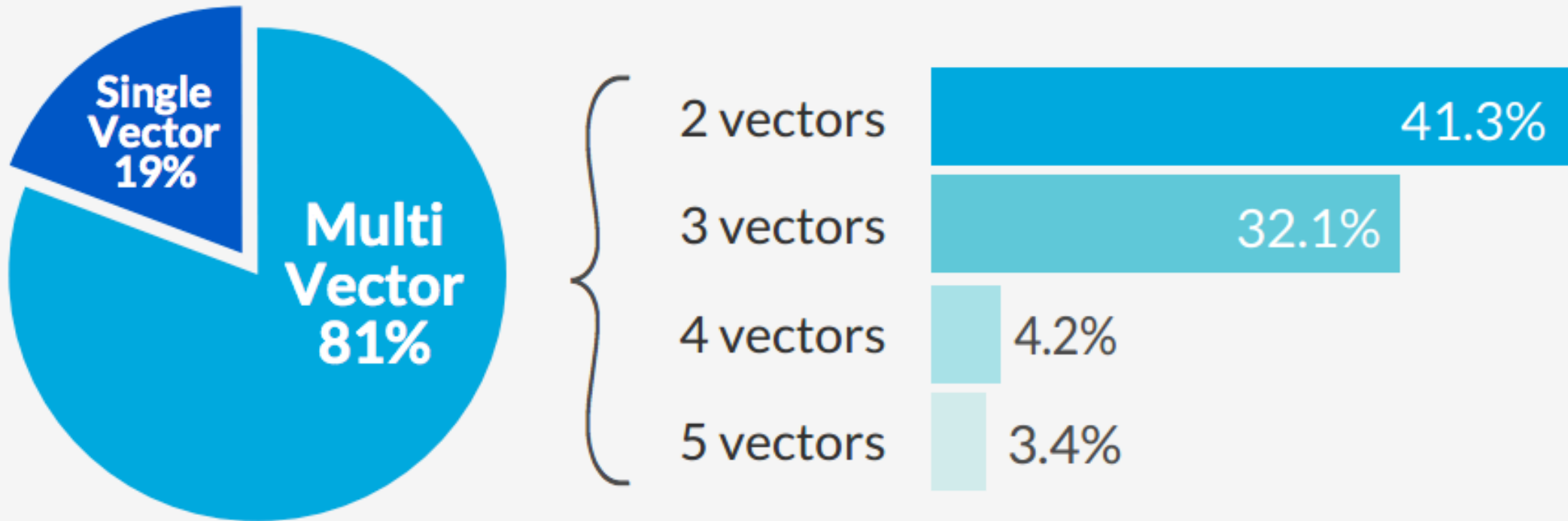


Sophisticated Multi-layered attacks

More Sophisticated Attacks Are Multi-layer



Network DDoS Attacks: Distribution by Number of Vectors



HaaS

Tickets

Purchase

Referral System

Our current power stands at 100-125Gbps average with a total network of 600Gbps!
VPNs are blocked through the payment system, please take them off for the next step!

Packages

Addons

100 Seconds

\$5.99 Monthly

N/A Lifetime*

Bitcoin

Credit Card

180 Seconds

\$8.99 Monthly

N/A Lifetime*

Bitcoin

Credit Card

500 Seconds

\$9.99 Monthly

\$29.99 Lifetime*

Bitcoin

Credit Card

1500 Seconds

\$28.99 Monthly

\$80.00 Lifetime*

Bitcoin

Credit Card

3500 Seconds

\$44.99 Monthly

\$120.00 Lifetime*

Bitcoin

Credit Card

7200 Seconds

\$69.99 Monthly

\$280 Lifetime*

Bitcoin

Credit Card

10800 Seconds

\$89.99 Monthly

\$350.00 Lifetime*

Bitcoin

Credit Card

30k Seconds

\$129.99 Monthly

\$500 Lifetime*

Bitcoin

Credit Card

Total Boots: 17439

Your Total Boots: 0

Boots Running: 7

Total Power Available: 88%

Username:

Current Date: 01-12-2015, 11:51:43 pm

Max Boot Time:

Expire date:

Max concurrent attacks:

CHF Owner/Founder

Julius Kivimaki Co-Owner

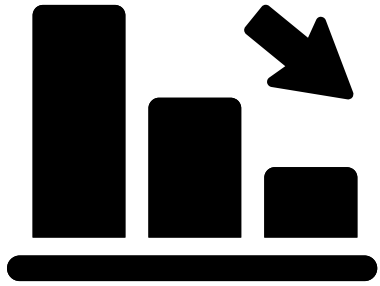
Mike Virus Trial-Admin

Logout

Packages do not automatically get charged every month by default
* Lifetime is 5 years, the expected lifetime of lizardstreser

If you are planning on disputing [open a ticket](#)

What's the impact of a DDoS attack?



**The business
impact of DDoS**



**Cost of
corrective action**



**Reputation
management**

[Archive](#)[Spam](#)[Delete](#)[Move to Inbox](#)[Labels ▾](#)[More ▾](#)

DDOS ATTACK!

[Inbox x](#)[Hostmaster x](#)

May 7 (4 days ago) ☆

[Reply](#)

Hello,

To introduce ourselves first:

<https://blogs.akamai.com/2014/12/dd4bc-anatomy-of-a-bitcoin-extortion-campaign.html>

<http://bitcoinbountyhunter.com/bitalo.html>

<http://cointelegraph.com/news/113499/notorious-hacker-group-involved-in-excoin-theft-owner-accuses-ccedk-of-withholding-info>

Recently we were DDoS-ing Neteller:

<https://twitter.com/neteller/status/583363894665715712>

Yes, our attacks are powerful.

So, it's your turn!

Your site is going under attack unless you pay 25 Bitcoin.

Pay to 155JPhzJmLBNqk12xaGRoDcNkAXNbmejjj

Please note that it will not be easy to mitigate our attack, because our current UDP flood power is 400-500 Gbps, so don't even bother. At least, don't expect cheap services like CloudFlare or Incapsula to help...but you can try. :)

Right now we are running small demonstrative attack on 1 of your IPs

Don't worry, it will not be that hard and it will stop in 1 hour.
It's just to prove that we are serious.

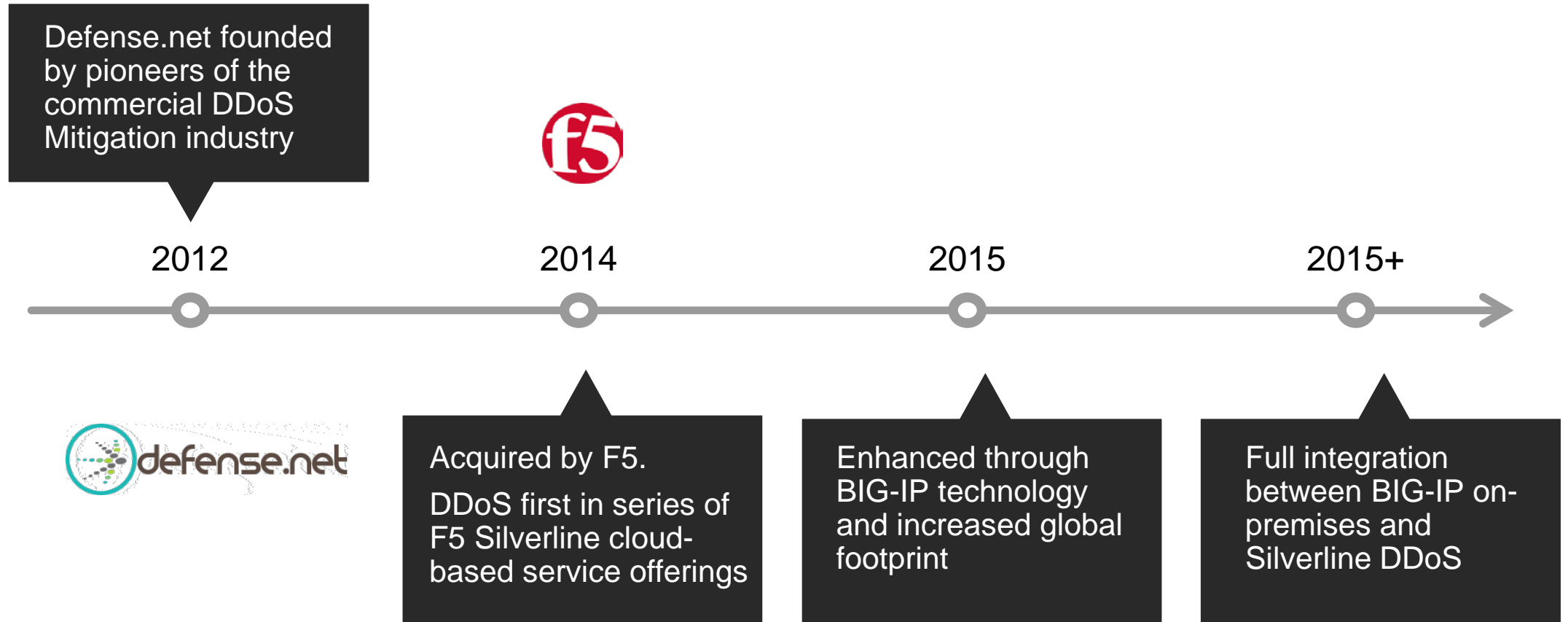
© 2016 [Emails from the Internet](#)
We are aware that you probably don't have 25 BTC at the moment, so we are giving you 24 hours.

“We do bad things, but we keep our word.”

Introducing F5 Silverline DDoS



The Silverline DDoS protection story



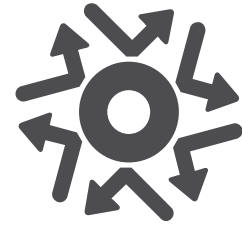
Traditional Cloud Platform Limitations



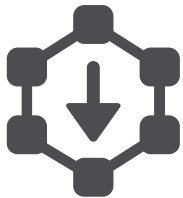
Scale per Customer:



Concentration Risk



Solution Side Effects



**Slow Mitigation
Startup**

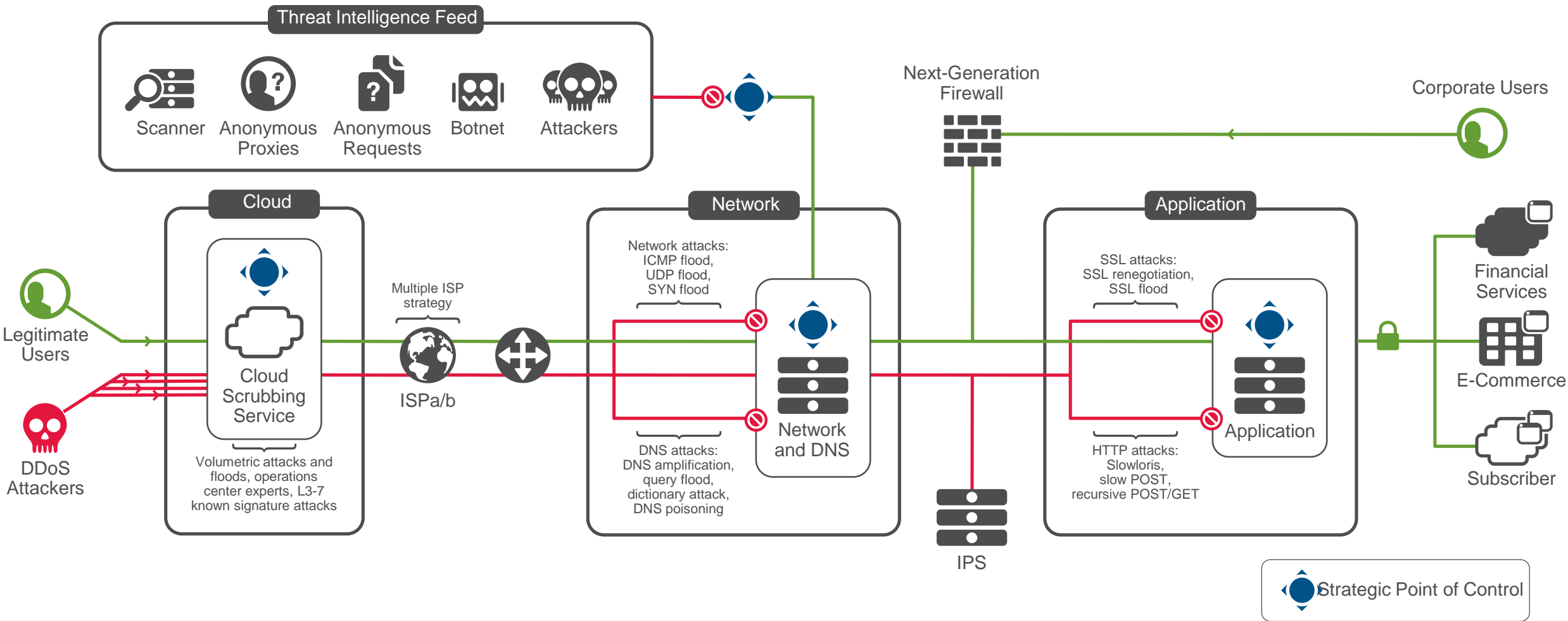


False Positives



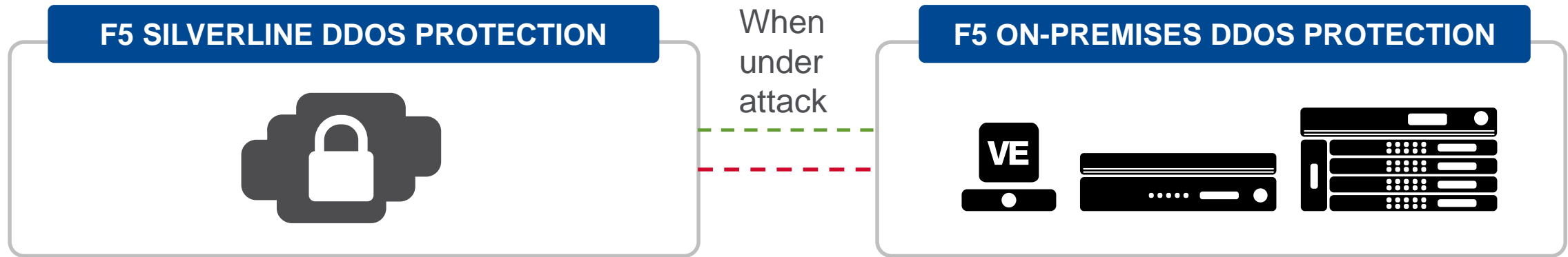
**Not Enough Visibility
into Attacks**

F5 Offers Comprehensive DDoS Protection



Protect Your Business and Stay Online During a DDoS Attack

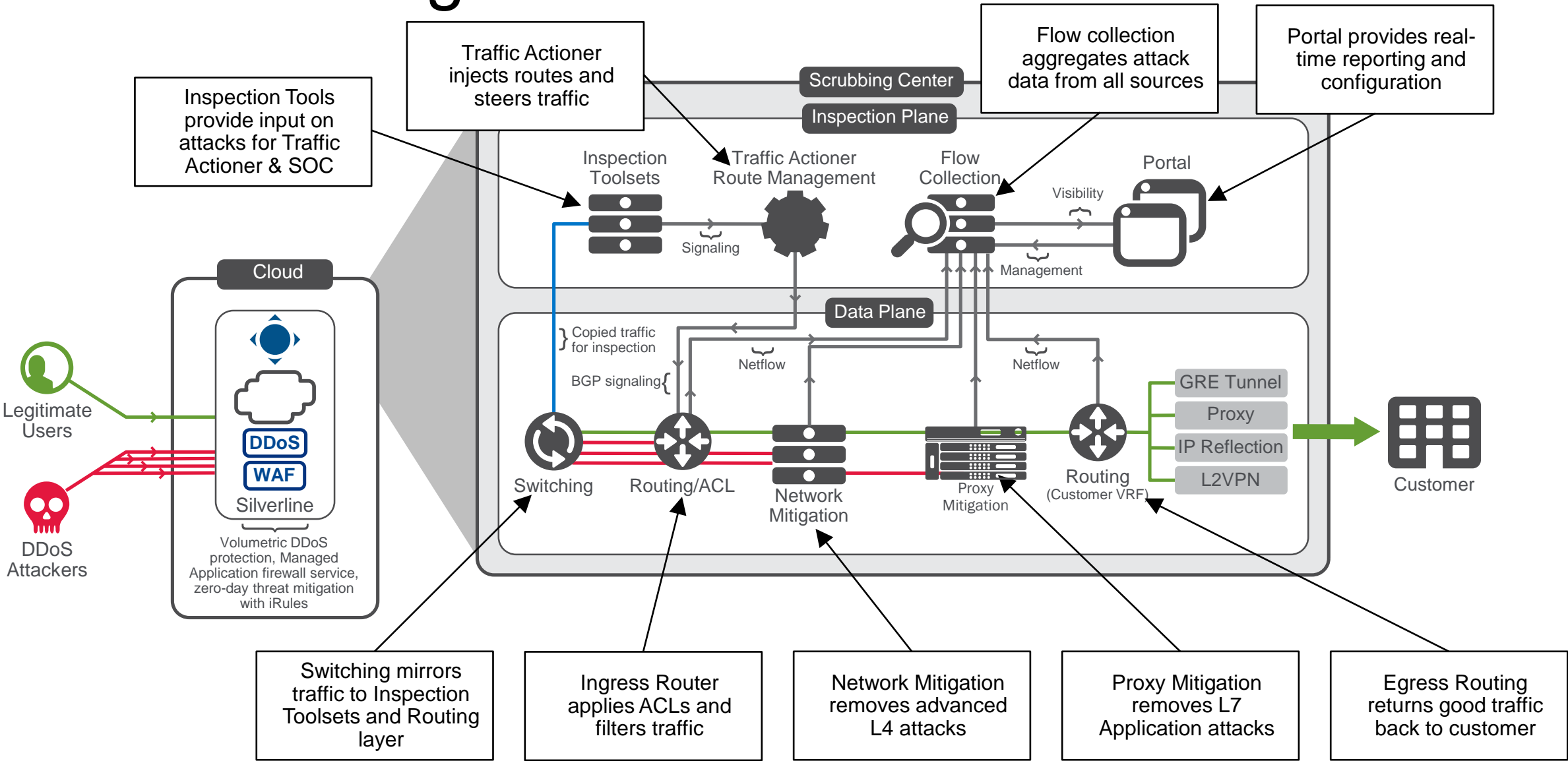
On-premises and cloud-based services for comprehensive DDoS Protection



- 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

- Mitigate mid-volume, SSL, or application targeted attacks on-premises

F5 Scrubbing Center



SSAE 16
SOC I TYPE II

CERTIFIED



AMERICAS

EMEA

ASIA-PACIFIC

24/7 Support

F5 Security Operations Center (SOC) is available 24/7 with security experts ready to respond to DDoS attacks within minutes

- Seattle, WA US
- Poland (European Soc)

Global Coverage

Fully redundant and globally distributed data centers world wide in each geographic region

- San Jose, CA US
- Ashburn, VA US
- Frankfurt, DE
- Singapore, SG

Industry-Leading Bandwidth

- Attack mitigation bandwidth capacity over 2.0 Tbps
- Scrubbing capacity of over 1.0 Tbps
- Guaranteed bandwidth with Tier 1 carriers

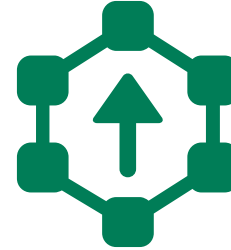
F5 Silverline DDoS Protection - Service Options



Always on

Primary protection as the first line of defense

The Always On service stops bad traffic from ever reaching your network by continuously processing all traffic through the cloud-scrubbing service and returning only legitimate traffic through your website.



Always available

Primary protection available on-demand

The Always Available service runs on standby and can be initiated when under a DDoS attack. F5 Silverline will begin mitigation as soon as your traffic is sent to us.

Traffic Steering to SL

VS

Capabilities

BGP (BORDER GATEWAY
PROTOCOL)
ROUTED MODE

PROTECT ENTIRE NETBLOCK /24

ASYMETRIC L3/L4

TUNNEL CLEAN TRAFFIC

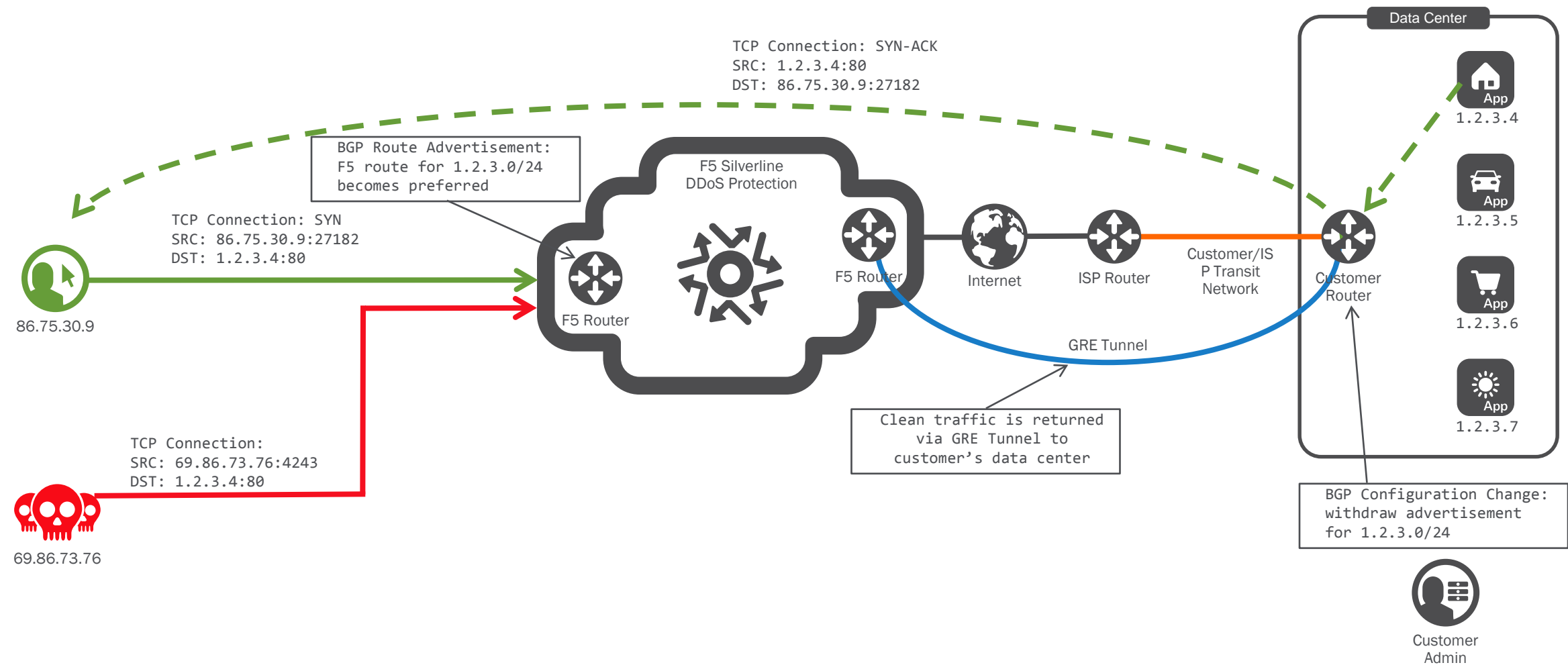
DNS
PROXY MODE

SINGLE APPLICATION (IP)

FULL PROXY
L7
SSL TERMINATION
WAF

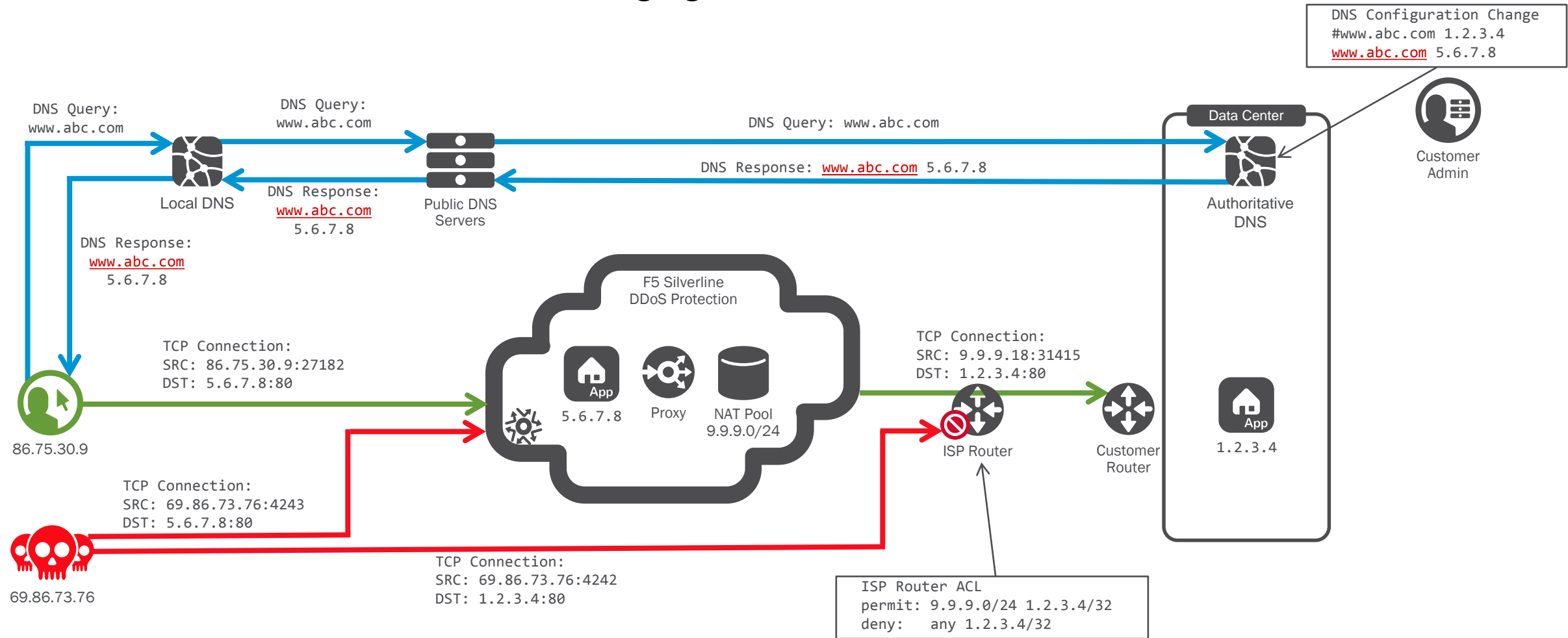
Routed Configuration

F5 Silverline DDoS Protection Engaged



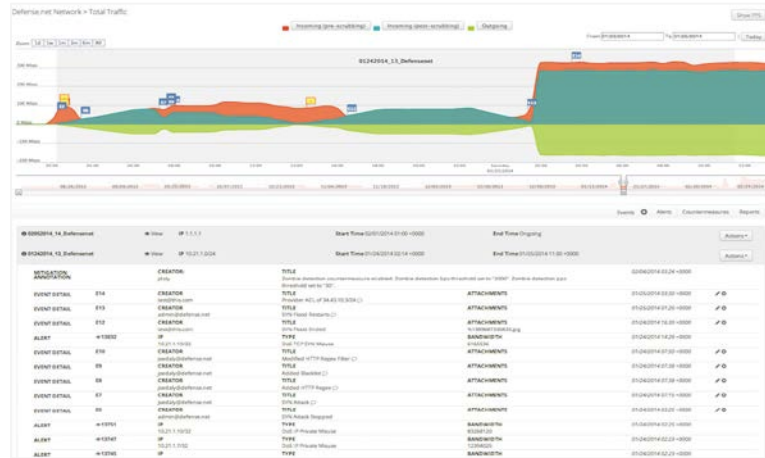
Proxy Configuration

F5 Silverline DDoS Protection Engaged



F5 Silverline AttackView Portal

Unprecedented Transparency



Attack Data

- Instant inspection on the filters and countermeasures used for mitigation
- Detailed timeline analysis on type, size, origin, and attack vector

Configuration and Provisioning

- **Configure/ review/ modify settings for both Proxy and GRE mode through the portal**

Detailed Communication

- Real time attack communications
- **Detailed events showing attack attributes and SOC mitigations applied**

F5 Emergency Response Service

**UNDER DDoS
ATTACK?**


Get back to business with
F5 Silverline DDoS Protection.



CALL
00-800-7000-5050
ddos@f5.com




Get F5® Silverline™
DDoS Protection Services



24x7 Security Operations Centre

- Fully automated DDoS attack detection and mitigation in the cloud
- Layer 3-7 protection against all known attack vectors

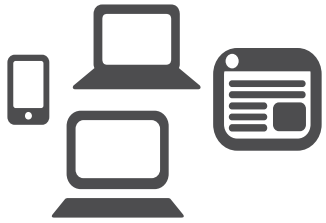


f5.com/silverline

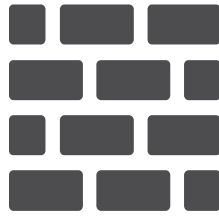
Introducing F5 Silverline WAF (WaaS)



Why Do Enterprises Need a Web Application Firewall?



Explosion of
web applications



Secure data
and web
applications



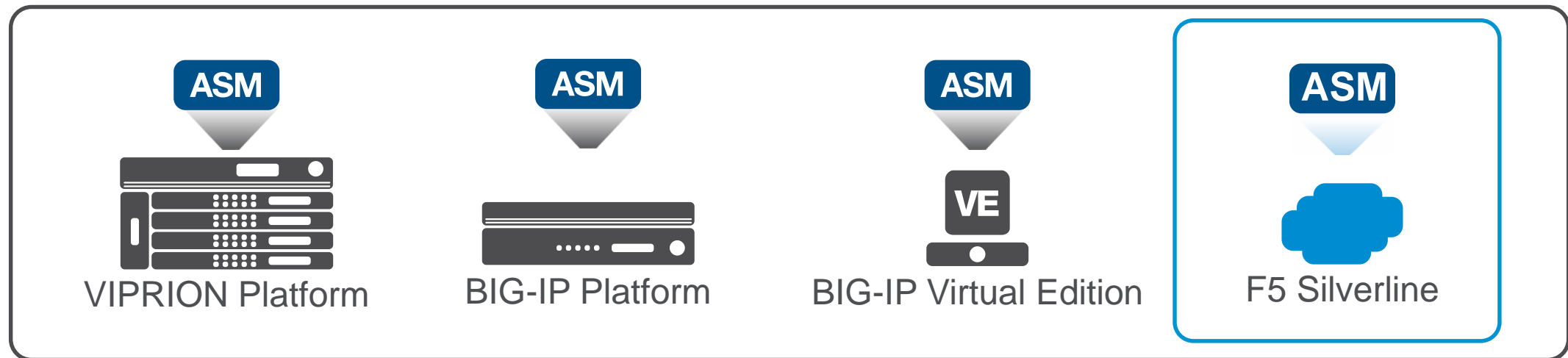
Maintain
compliance
(PCI DSS)



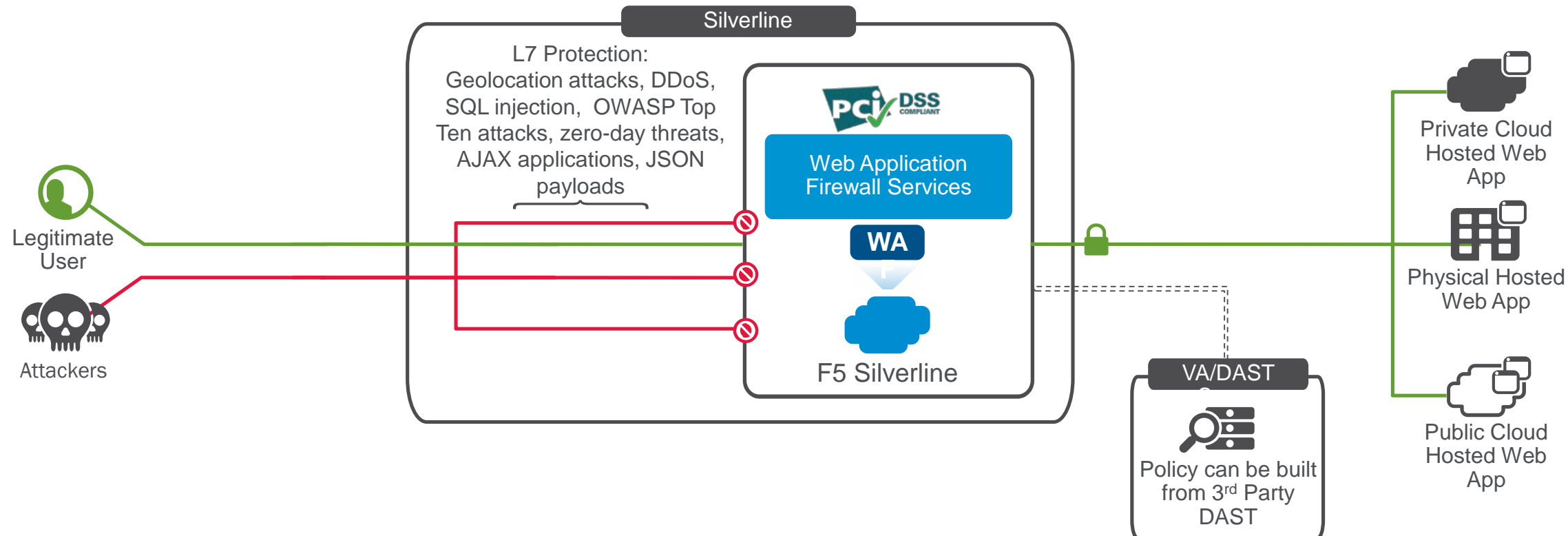
Defend against
Layer 7 attacks

F5's Web Application Firewall

Recognized as the most scalable, comprehensive WAF on the market Deployed in more datacenters worldwide than any other WAF



F5's Web Application Firewall



F5 Silverline WAF – Key Takeaways



Leverage proven security efficacy

Protect against critical web attacks with an enterprise-grade service built on BIG-IP ASM which is recommended by NSS Labs with 99.89% overall security effectiveness*.



Reduce operating costs

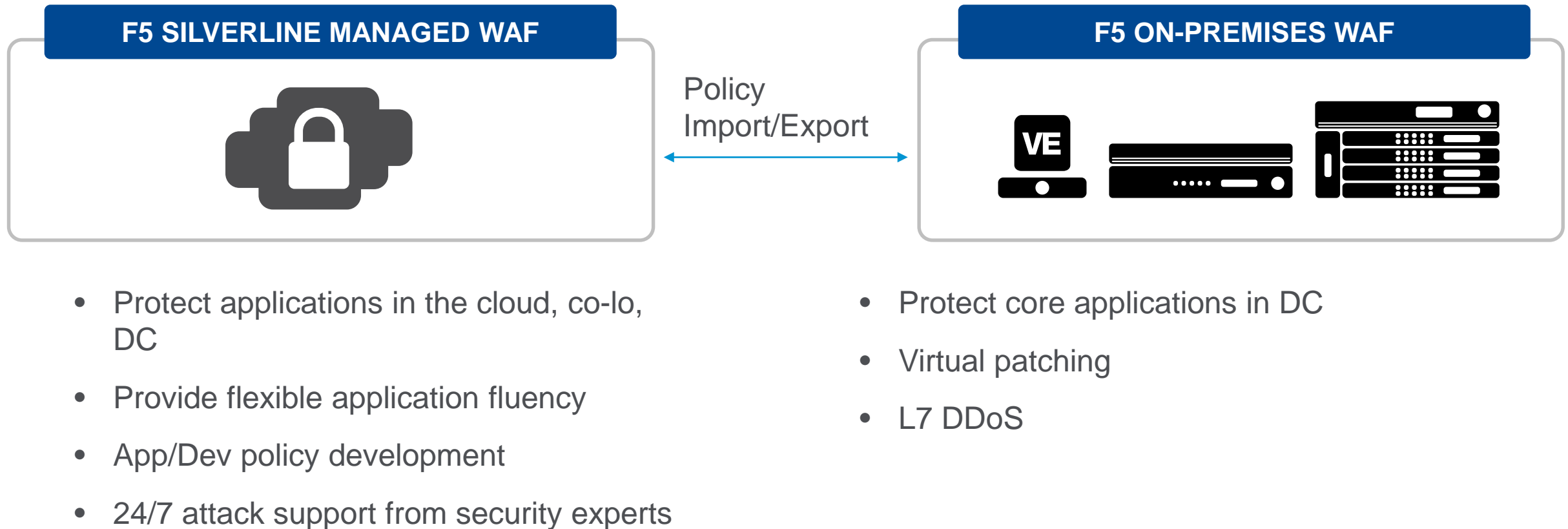
Rapidly deploy WAF protections and drive operational and cost efficiencies by outsourcing WAF policy management to F5 security experts.



Protect web apps, anywhere

Protect web apps, no matter where they reside with consistent policies across hybrid environments in conjunction with BIG-IP deployments.

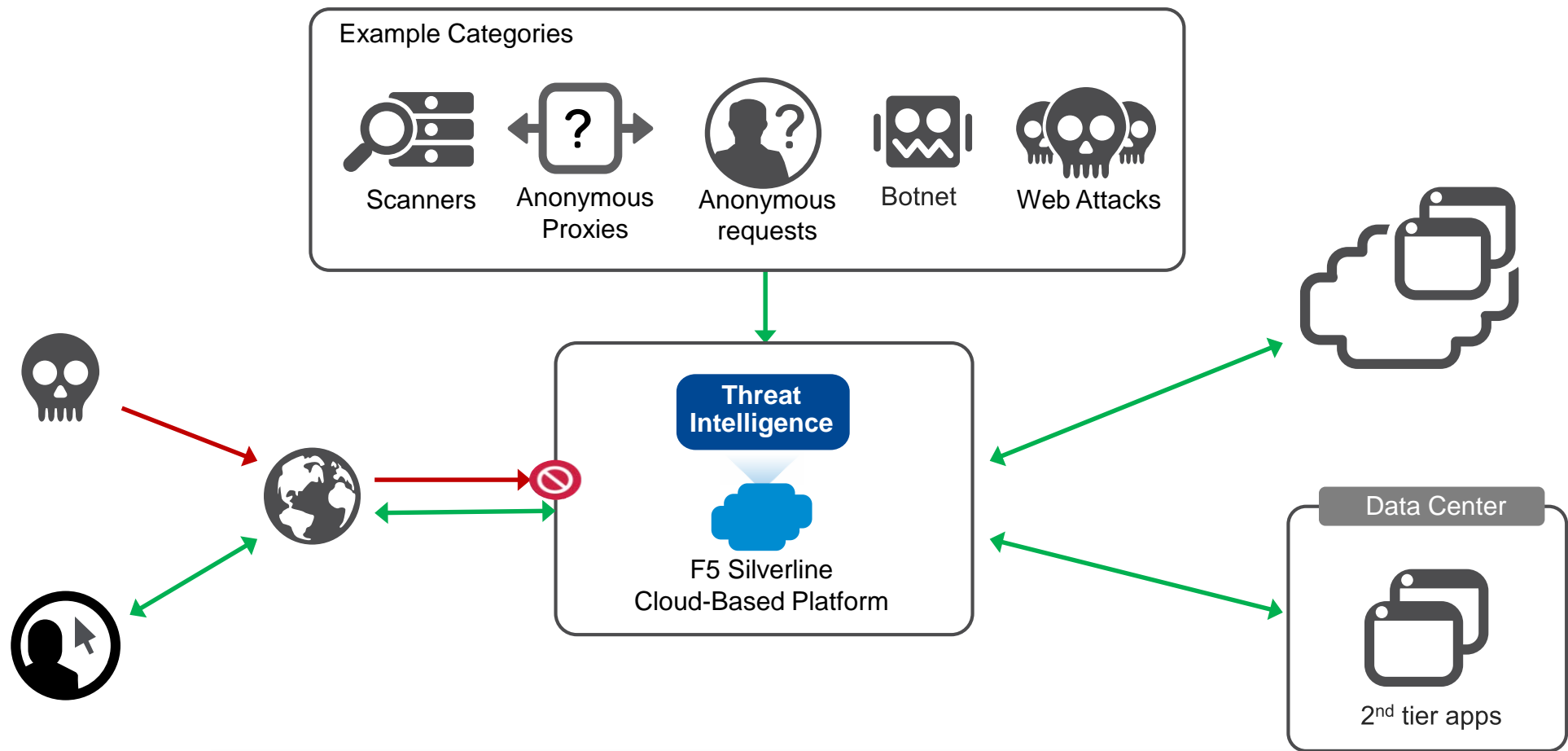
Hybrid Protection from Advanced Application Attacks



Introducing F5 Silverline Threat Intelligence



Silverline Threat Intelligence – IP Reputation Service



Ensure IP Threat Protection and Improve Threat Visibility
Optimize Threat Security and Reduce Malicious Communications
Reduce Threat Risks and Keep Apps Online

Portal

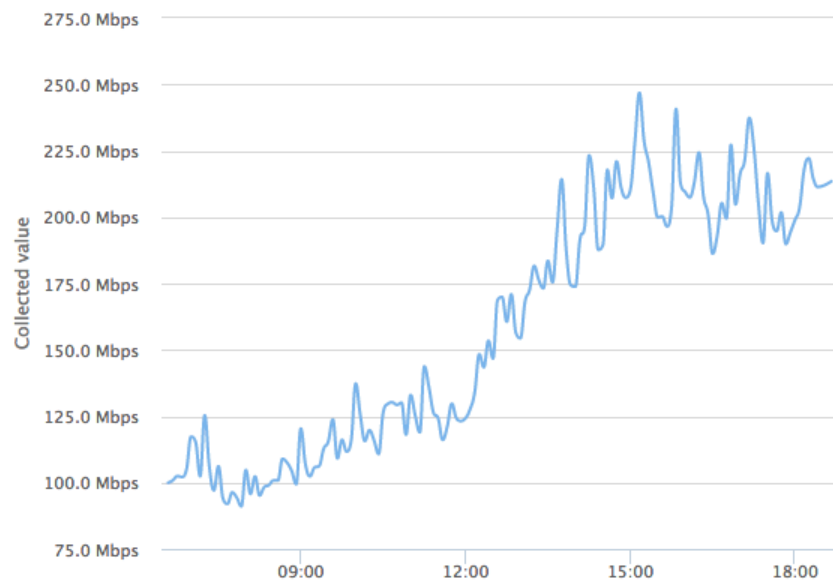




DDoS Overview

Current Traffic

🔥 Ongoing Mitigation

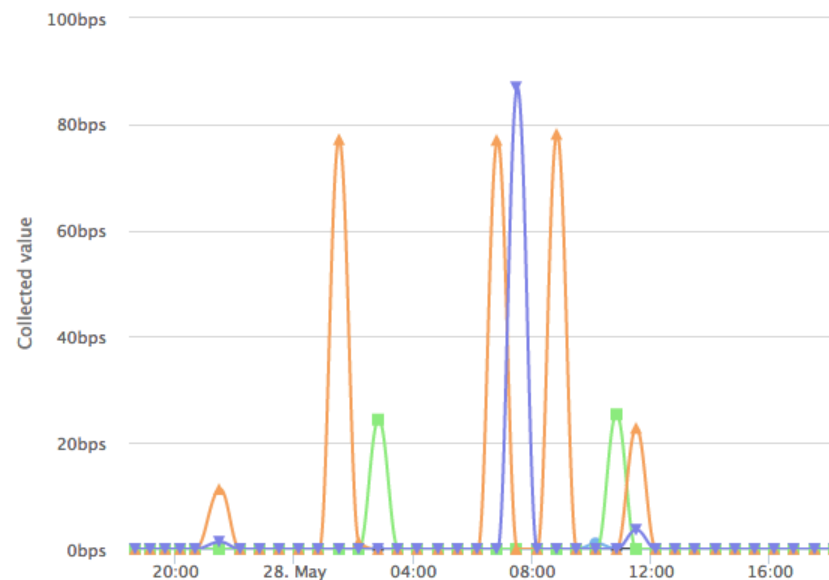
[More Details](#)**Current Active Countermeasures (2) ▶****Alerts (0) and Events (1) ▶****Top Talkers ▶**

Overview



Web Application Firewall Overview

Current Traffic

[More Details](#)**Last Web Application Firewall Policy Change**2015-05-27 15:25Z - test234**Unreviewed Logs**433**Web Application Firewall Violations (7 days) ▶****Proxy Stats ▶**[More Details](#)



DDoS Information

[Dashboard](#)[Countermeasures](#)[Alerts for F5 Network](#)[Alerts for Local Network](#)

Stats

[Proxy Stats](#)

Routed Configuration

[IP Network Management](#)[GRE Tunnel Management](#)[Routing](#)

Proxy Configuration

[L7 Profiles](#)[iRule Editor](#)[Proxy Configuration](#)[SSL Certificate Management](#)

ACL Filter Management

[IP Whitelists](#)[IP Blacklists](#)[Firewall Rules](#)

Cache Management

[Clear Cache](#)

Available Options

Proxy Configuration

Proxy configurations can be found here. This will include information such as VIP, VIP protocol, backend-ip, backend port, and cert information.

L7 Profiles

View and manage Layer-7 profiles.

iRule Editor

Create custom iRules to block or allow traffic based on URI, Headers, Method and more.

Caching

Remove items from a proxy cache.

GRE Configuration

GRE tunnels are configured to deliver clean traffic (post-scrubbed) back to your infrastructure. Configuration information will be found here.

Routing

Manage routing information and see BGP Peer status.

IP Blacklists

If you've requested IPs be blacklisted, or you wish to blacklist additional IPs, find it here.

IP Whitelists

If you've requested IPs be whitelisted, or you wish to whitelist additional IPs, find it here.

SSL Certificate Management

Specific SSL Cert management can be found here.



F5 Network

Local Networks

Application

Zones

F5 Network > Total Traffic

Show PPS

Incoming (pre-scrubbing)

Incoming (post-scrubbing)

Outgoing

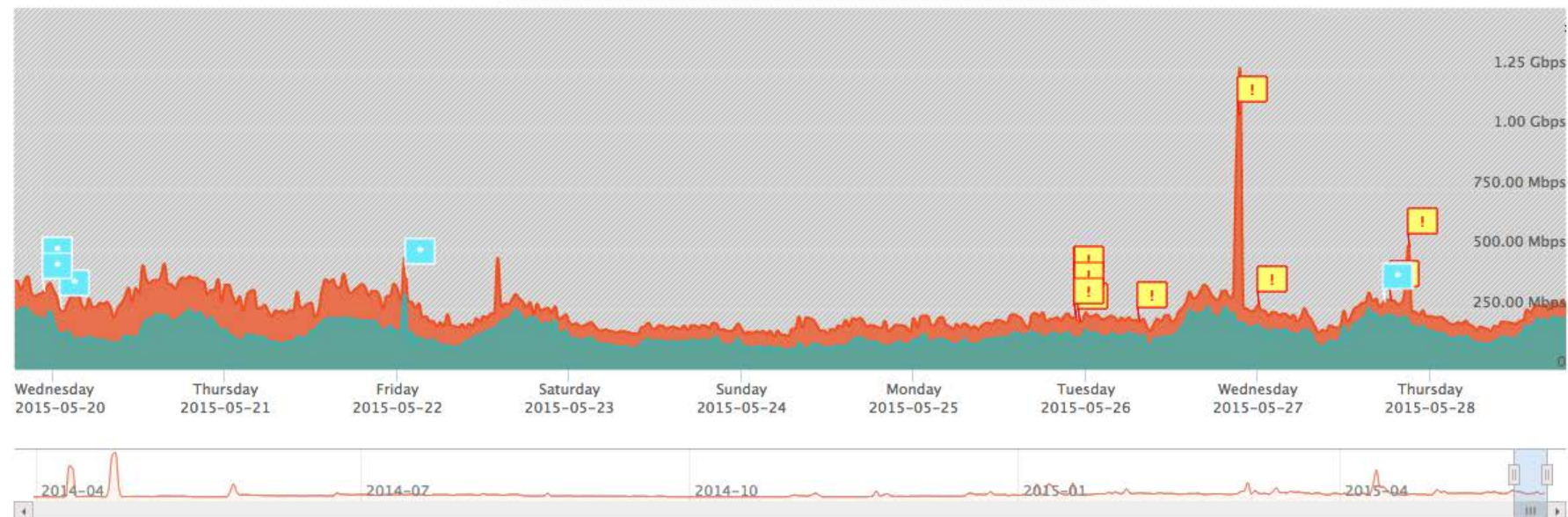
Zoom 1d 1w 1m 3m 6m All

From 2015-05-19

To 2015-05-28

Now

Reload Interval Never



Add Event

Events

Alerts

Countermeasures

Top Talkers

Reports

20150527_1742_	IP	Start Time	End Time	Chat Transcript	Actions
Created By: System	View Graph	2015-05-27 17:42Z	Ongoing	View	
20150519_2240_	IP: /32	Start Time	End Time	Chat Transcript	Actions
Created By: System	View Graph	2015-05-19 22:40Z	Ongoing	None	
MITIGATION ANNOTATION	CREATOR:	Black/White filters set to "drop src port 123".		2015-05-22 01:14Z	
	mapeterson				
MITIGATION ANNOTATION	CREATOR:	SYN authentication countermeasure disabled.		2015-05-20 01:01Z	



Web Application Firewall

[Violations](#)[Policy Audits](#)

Stats

[Proxy Stats](#)[Violation Stats](#)

IP Management

[IP Blacklists](#)

Cache Management

[Clear Cache](#)

Configuration

[Web Application Firewall Policies](#)[Secure Uploads](#)[L7 Profiles](#)[iRule Editor](#)[Proxy Configuration](#)[SSL Certificate Management](#)

Silverline Web Application Firewall Configuration

[Proxy Stats](#)

Traffic statistics for vservers (proxies)

[Web Application Firewall Policies](#)

View and manage Web Application Firewall Policies.

[Violations](#)

View the Web Application Firewall violations log.

[iRule Editor](#)

Create custom iRules to block or allow traffic based on URI, Headers, Method and more.

[Proxy Configuration](#)

Proxy configurations can be found here. This will include information such as VIP, VIP protocol, backend-ip, backend port, and cert information.

[L7 Profiles](#)

View and manage Layer-7 profiles.

[IP Blacklists](#)

If you've requested IPs be blacklisted, or you wish to blacklist additional IPs, find it here.

[SSL Certificate Management](#)

Specific SSL Cert management can be found here.



Web Application Firewall

[Violations](#)[Policy Audits](#)

Stats

[Proxy Stats](#)[Violation Stats](#)

IP Management

[IP Blacklists](#)

Cache Management

[Clear Cache](#)

Configuration

[Web Application Firewall Policies](#)[Secure Uploads](#)[L7 Profiles](#)[iRule Editor](#)[Proxy Configuration](#)[SSL Certificate Management](#)[General](#)[Web
Scraping](#)[Session
Awareness](#)[CSRF](#)[File Types](#)[Blocking](#)[URLs](#)[Policy
Builder](#)[Headers](#)[Methods](#)[Flows](#)[Header](#)[Redirection](#)[Parameters](#)

Configuration for [redacted]

Policy in Blocking Mode

[History](#)

Grace Threshold	100	Session Prevention Threshold	100
Revalidation Threshold	2000	Rapid Surf Max Time Duration	1000
Rapid Surf Max Page Changes	5	Web Scraping Alarm	⊘
Web Scraping Block	⊘	Session Opening Anomaly Block	⊘
Session Opening Anomaly Alarm	⊘	Session Transactions Anomaly Alarm	⊘
Session Transactions Anomaly Block	⊘	Opening Client Side Integrity Defense	⊘
Opening Rate Limiting	⊘	Sessions Opened Per Second Increase Rate	500
Sessions Opened Per Second Maximum	50	Sessions Opened Per Second Minimum	25
Opening Max Prevention Duration	1800	Opening Drop Ip With Reputation	⊘
Transactions Tps Increase Rate	500	Transactions Per Second Maximum	400
Transactions Per Second Minimum	200	Transactions Max Prevention Duration	1800
Opening Persistent Storage Inconsistency	✔	Opening Persistent Storage Resets	✔
Opening Persistent Storage Inconsistency Events Maximum	3	Opening Persistent Storage Inconsistency Events Duration	600
Opening Persistent Storage Resets Maximum	2	Opening Persistent Storage Resets Duration	600
Persistent Storage Max Prevention Duration	1800	Use Persistent Storage	⊘
Persistent Data Validity Period	120	Session Opening Anomaly Enable	✔
Suspicious Clients Alarm	⊘	Suspicious Clients Block	⊘
Fingerprinting Enable	⊘	Fingerprint Resets Enabled	⊘
Fingerprint Resets Threshold	5	Fingerprint Resets Time Window	600
Detect Plugins	⊘	Suspicious Clients Prevention Duration	300



Web Application Firewall

[Violations](#)[Policy Audits](#)

Stats

[Proxy Stats](#)[Violation Stats](#)

IP Management

[IP Blacklists](#)

Cache Management

[Clear Cache](#)

Configuration

[Web Application Firewall Policies](#)[Secure Uploads](#)[L7 Profiles](#)[iRule Editor](#)[Proxy Configuration](#)[SSL Certificate Management](#)

Violation Stats

View ▾

From 2015-05-20

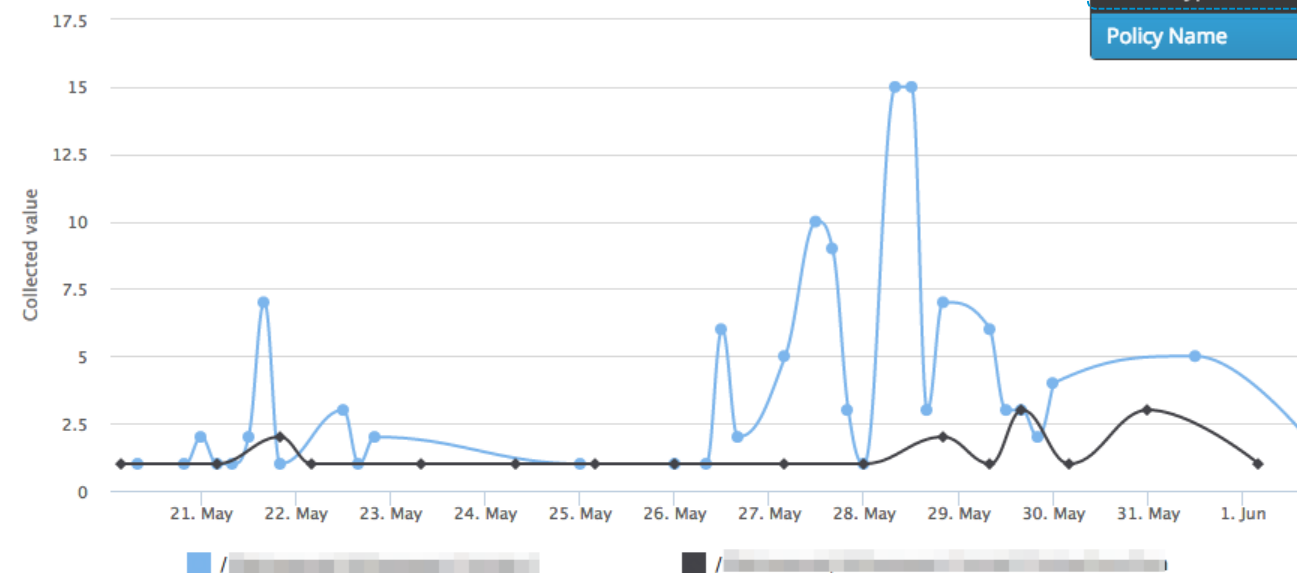
To 2015-06-30

Refresh

Violations

Attack Type

Policy Name



Cloud-Based Enterprise-Grade Application Services



- Defend against DDoS attacks with cloud-scrubbing
- Keep your business online when under attack
- Rapidly deploy DDoS protection in minutes
- Ensure applications are available anywhere
- All Silverline managed services operated 24x7x365 by F5 SOC
- Protect web applications and data from layer 7 attacks
- Enable compliance, such as PCI DSS
- Expert policy setup and fine-tuning
- Built on BIG-IP® Application Security Manager™ (ASM)
- Designed and managed security policies, by security experts at F5 SOC
- Ensure IP Threat Protection and Improve Threat Visibility
- Optimize Threat Security and Reduce Malicious Communications
- Reduce Threat Risks and Keep Apps Online
- Incorporate IP context into DDoS Protection and App. Security services



SOLUTIONS FOR AN APPLICATION WORLD