Protect Against the Full Spectrum of Modern DDoS Attacks
F5 EMEA Webinar January 2015
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
Syrian 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
Frequency of Attacks – 2014

- **Feb 05**: Bitly – Outage as result of DDoS attack
- **Feb 11**: Elance Freelance Job Site – NTP Reflection Attack, temporary website disruption
- **Feb 20**: oDesk – Temporary website disruption as result of DDoS attack
- **Mar 04**: Meetup Event Planning – NTP Amplification attack carried out by extortionists
- **Mar 11**: GitHub Code Host – UDP based Amplification attack
- **Mar 17**: Royalty Free Stock Images – DDoS attack by extortionists
- **Mar 20**: Hootsuite – DDoS attack by extortionists
- **Mar 24**: Basecamp – DDoS attack by extortionists
- **Mar 27**: SurveyGizmo – DDoS attack; Site down 2 days, ISP abandoned recovery

**Script kiddies**

**The rise of hacktivism**

**Cyber war**
How Have Attacks Changed in the Last Year?

Instead compromise 3,000 to 5,000 commercial servers in major data centers.

Not known bad IP addresses (purchased legitimate resources to launch attack).

Big servers with lots of CPUs create more traffic.

Lots of 10 Gbps pipes are attached to those commercial servers.

Current attacks go beyond overwhelming the site and overwhelm the bandwidth pipe instead.

Largest single victim attacks 120 Gbps.

Largest concurrent attacks 190 Gbps (3 banks attacked simultaneously).

Average attack size increased 16 Times Q2 2013 over Q2 2012.
New Attack Vectors Emerge
Network Time Protocol (NTP) attacks zero to huge in 3 months

“Derp Trolling” attacks against all major game sites where “PhantomL0rd” was trying to play

FEB 14
325 Gbps

JAN 14
150 Gbps

DEC 13
100 Gbps
More Sophisticated Attacks are Multi-Layer

- Application
- SSL
- DNS
- Network
Layer 2-7 DDoS Mitigation

OSI stack

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

Increasing difficulty of attack detection

**Application attacks**
- OWASP Top 10 (SQL Injection, XSS, CSRF, etc.), Slowloris, Slow Post, HashDos, GET Floods

**Session attacks**
- DNS UDP Floods, DNS Query Floods, DNS NXDOMAIN Floods, SSL Floods, SSL Renegotiation

**Network attacks**
- SYN Flood, Connection Flood, UDP Flood, Push and ACK Floods, Teardrop, ICMP Floods, Ping Floods and Smurf Attacks
The Business Impact of DDoS

The business impact of DDoS
Cost of corrective action
Reputation management
Which DDoS Protection Technology to Use?

**CLOUD/HOSTED SERVICE**

**Strengths**
- Completely off-premises so DDoS attacks can’t reach you
- Amortised defense across thousands of customers
- DNS anycast and multiple data centers protect you

**Weaknesses**
- Customers pay, whether attacked or not
- Bound by terms of service agreement
- Solutions focus on specific layers (not all layers)

**ON-PREMISES DEFENSE**

**Strengths**
- Direct control over infrastructure
- Immediate mitigation with instant response and reporting
- Solutions can be architected to independently scale of one another

**Weaknesses**
- Many point solutions in market, few comprehensive DDoS solutions
- Can only mitigate up to max inbound connection size
- No other value, only providing benefit when you get attacked
Which DDoS Protection Technology to Use?

**HYBRID MODEL: CLOUD AND ON-PREMISES**

**Strengths**
- Comprehensive hybrid solution
- Complete protection against all DDoS attacks with combined on-premises and cloud solution
- Signalling between on-premises and cloud for dynamic detection and mitigation

![On-Premises Appliances + Cloud Services](image-url)
Protect Your Business and Stay Online During a DDoS Attack
On-premises and cloud-based services for comprehensive DDoS Protection

**CLOUD-BASED 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

**ON-PREMISES DDoS PROTECTION**

- Mitigate mid-volume, SSL, or application targeted attacks on-premises
- Complete infrastructure control
- Advanced L7 attack protections
Cloud-Based Scrubbing with On-Premises Defenses

Threat Intelligence Feed
- Scanner
- Anonymous Proxies
- Anonymous Requests
- Botnet
- Attackers

Cloud
- Cloud Scrubbing Service
  - Volumetric attacks and floods, operations center experts, L3-7 known signature attacks

Network
- Multiple ISP strategy
- ISPa/b
- Network attacks:
  - ICMP flood, UDP flood, SYN flood
- DNS attacks:
  - DNS amplification, query flood, dictionary attack, DNS poisoning

Application
- HTTP attacks:
  - Slowloris, slow POST, recursive POST/GET
- SSL attacks:
  - SSL renegotiation, SSL flood

Next-Generation Firewall

Corporate Users
- Financial Services
- E-Commerce
- Subscriber

Strategic Point of Control

© F5 Networks, Inc.
Cloud-Based Scrubbing with On-Premises Defenses

Cloud Scrubbing Service

- Real-time volumetric DDoS attack detection and mitigation in the cloud
- Multi-layered L3-L7 DDoS attack protection
- 24x7 expert Security Operations Center services
- Transparent attack reporting via customer portal
Cloud-Based Scrubbing with On-Premises Defenses

NETWORK KEY FEATURES

- The network tier at the perimeter is L3 and L4 network firewall services
- Simple load balancing to a second tier
- IP reputation database
- Mitigation of transient and low-volume attacks

Network attacks:
- ICMP flood, UDP flood, SYN flood

DNS attacks:
- DNS amplification
- Query flood
- Dictionary attack
- DNS poisoning

Network and DNS

Multiple ISP strategy

Threat Intelligence Feed

Scanner
Anonymous Proxies
Anonymous Requests
Botnet
Attackers

Volumetric attacks and floods, operations center experts, L3-7 known signature attacks

DDoS Attackers

Corporate Users

Financial Services

E-Commerce

Subscriber

Strategic Point of Control

Network

Next-Generation Firewall

Corporate Users

Internet Service Providers

Network

Network and DNS

Cloud Scrubbing Service

Cloud

Legitimate Users

© F5 Networks, Inc.
Cloud-Based Scrubbing with On-Premises Defenses

APPLICATION KEY FEATURES

- Application-aware, CPU-intensive defense mechanisms
- SSL termination
- Web application firewall
- Mitigation of asymmetric and SSL-based DDoS attacks
Multiple Ways to Direct Traffic to Massive Scrubbing Centers

- BGP (BORDER GATEWAY PROTOCOL) ANYCAST
- DNS / ANYCAST

Multiple Ways to Return Clean Traffic

- GRE TUNNELS
- PROXY
- IP REFLECTION
- AMAZON (AWS) DIRECT CONNECT
- FIBER INTERCONNECT
DDoS Architecture Scrubbing Center

Cloud Scrubbing Service

Tier 1

Legitimate Users

DDoS Attackers

Volumetric attacks and floods, operations center experts, L3-7 known signature attacks

Scrubbing Center

Inspection Plane

Inspection Toolsets

Traffic Actioner

Route Management

Flow Collection

Portal

Data Plane

Switching

Routing/ACL

Netflow

Netflow

GRE Tunnel

Proxy

IP Reflection

X-Connect

Customer

Strategic Point of Control
Cloud-Based DDoS Protection – Service Options

Always On
Primary protection as the first line of defense
Stops bad traffic from ever reaching your network by continuously processing all traffic through the cloud-scrubbing service and returning only legitimate traffic to your network

Always Available
Primary protection available on-demand
Runs on stand-by and can be initiated when under attack
Visibility Before, During, and After a DDoS Attack

Securely set up and manage services, configure proxy and routing, receive visibility and reporting of attack mitigation in real time.

Get instant details as an attack occurs

- Type and size of the attack
- IP origin
- Attack vectors
- Mitigation process
- Yellow-flagged annotations of the Security Operations Center communications
- Packet capture reports for download
Cloud-Based DDoS Protection

Benefits of cloud-based service

- Keep your business online during a DDoS Attack
- Protect your business
- Security Operations Center
- Access to DDoS experts 24/7
- Multi-layered, comprehensive L3-L7 protection
- Protect against all DDoS attack vectors
- Customer portal
- Protect against the largest of DDoS attacks
- The most attack mitigation bandwidth per customer
- Gain real-time attack mitigation insights
DDoS Protection for the Enterprise Data Center

DDoS Protection for the Enterprise Data Center

DDoS Protection

Cloud-Based Platform

Threat Intelligence Feed

Scanner
Anonymous Proxies
Anonymous Requests
Botnet
Attackers

Network

Network Firewall Services + DNS Services + Simple Load Balancing to Tier 3

ADC Platform

Network attacks:
- ICMP flood, UDP flood, SYN flood
- DNS amplification, query flood, dictionary attack, DNS poisoning

DNS attacks:
- DNS amplification, query flood, dictionary attack, DNS poisoning

ISP may provide rudimentary DDoS service

Volumetric attacks and size floods, operations center experts, L3-7 known signature attacks

Users leverage NGFW for outbound protection

Can inspect SSL at either tier

SSL attacks:
- SSL renegotiation, SSL flood

HTTP attacks:
- Slowloris, slow POST, recursive POST/GET

Employees

Financial Services

E-Commerce

Subscriber

Web Application Firewall Services + SSL Termination

Physical
Virtual

Next-Generation Firewall

Users

DDoS Attacker

Customer
Partner

DDoS Attacker

Volumetric attacks and size floods, operations center experts, L3-7 known signature attacks

ISP may provide rudimentary DDoS service
Complete DDoS Protection Solution
On-premises and cloud-based services for comprehensive DDoS Protection

Network firewall
Web application firewall
SSL inspection
DNS security

ON-PREMISES DDoS PROTECTION AND CLOUD SCRUBBING
Solutions for an Application World.