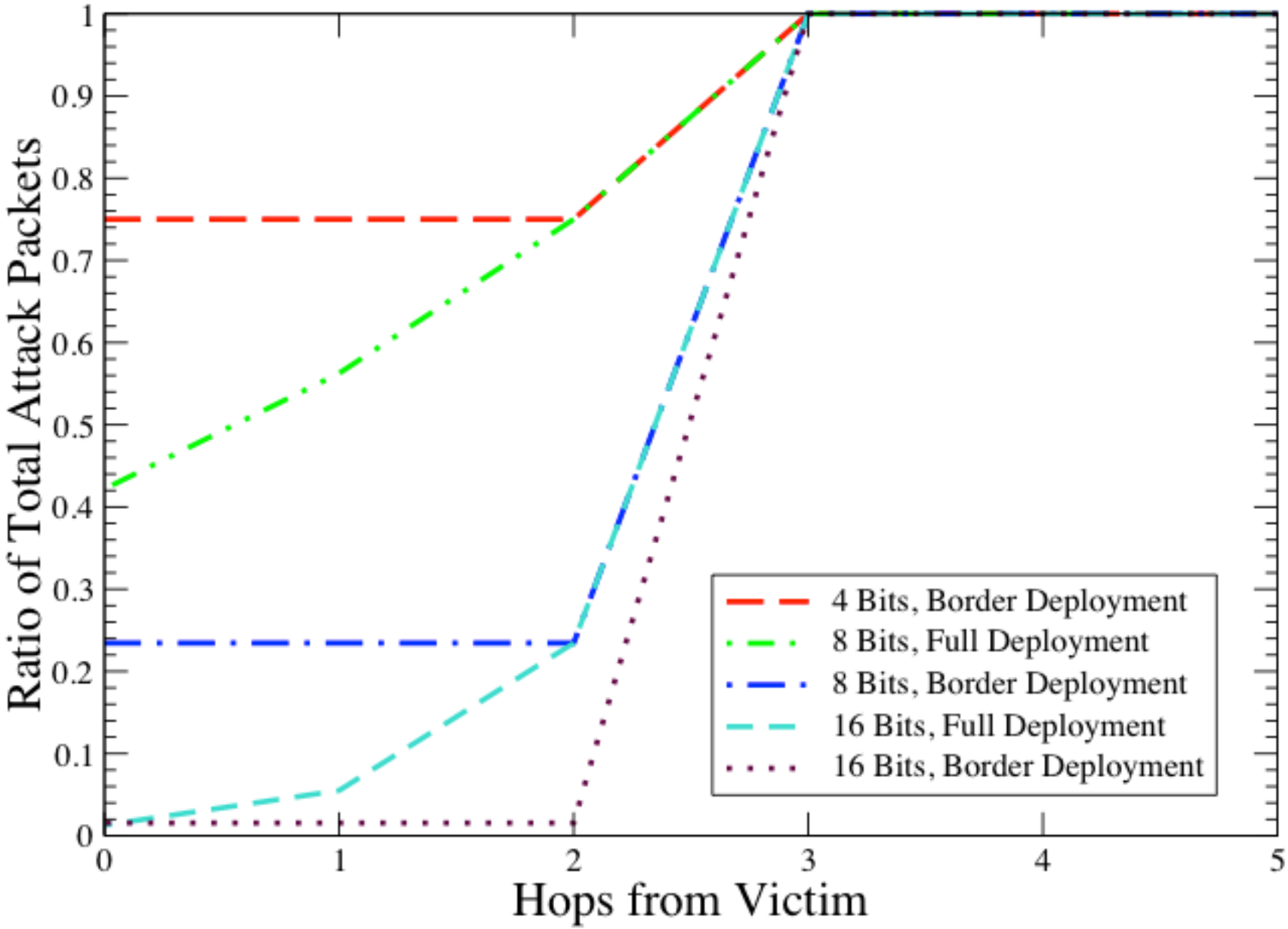

Ratio of Total Attack Packets
Hops from Victim
0
0.1
0.2
0.3
0.4
0.5
0.6
0.7
0.8
0.9
1
0
1
2
3
4
5
4 Bits, Border Deployment
8 Bits, Full Deployment
8 Bits, Border Deployment
16 Bits, Full Deployment
16 Bits, Border Deployment

The probability that the client can connect after k tries is:

$$\begin{aligned} &P(\text{ connect after k tries}) \\ &\quad = 1 - (1 - P(\text{connect after 1 try}))^k \\ &\quad = 1 - (1 - (1 - \epsilon_i)^i)^k \end{aligned}$$

the required number of connection attempts is:

$$k = \frac{\log(1 - P(connect))}{\log(1 - (1 - \epsilon_i)^i)}$$

A nice feature of this formula is that the expected number of connection attempts depends logarithmically on the connection probability, which indicates that even for large ϵ_i, a determined client can get a connection after a moderate waiting time.

Mitigating Multiple DDoS Attack Vectors

By recognizing the four main categories of attack, security professionals can mitigate even previously unknown vectors:

1. **Volumetric**: Flooding
2. **Computational Asymmetric:** Consuming CPU cycles
3. **Stateful Asymmetric:** Abusing memory
4. **Vulnerability-based**: Exploiting software vulnerabilities
5. **Blended DDoS**: Combination of multiple attack vectors

Security professionals need to understand how to plug the security gap from Layers 3 to 7, and protect against multi-layer attacks, with a full proxy security architecture. It's time to rethink and refine the enterprise security architecture, so organizations can remain agile and resilient against future threats.
The following mindmap shows the detection methods (left) for DDoS attack categories (middle) and the mitigations (right).

DETECTION

Signature Based

Strengths:
- Ease of hardware implementation
- Fast deterministic
- False positive rate

Considerations:
- Reactive
- Some may not be able to distinguish volumetric "Good" vs. "Bad"

Heuristic Flow Analysis

Strengths:
- Good at "Good" vs."Bad"
- Pro-actively finds anomalies

Considerations:
- May require "baseline-ing"

Security Appliance Resource Monitoring

Strengths:
- Based on attack's target (not specific to attack mechanism)
- Low false positive/negative rate
- Feedback-driven security appliance self-defense mechanism

Considerations:
- Protects only resources that are monitored
- Not server-aware; doesn't directly protect server

Server Resource Monitoring

Strengths:
- Based on attack's target (not specific to attack mechanism)
- Low false positive/negative rate
- Server-centric
- Feedback-driven

Considerations:
- Protects only resources that are monitored

Use Web Application Firewall heuristic latency based detection

Use Web Application Firewall heuristic Transaction Per Second (TPS) based detection

Use profile definitions and resource monitoring

Volumetric

Method: Packet or Flow Flood

Resource Attacked: Network Bandwidth

- UDP Packet Floods
- ARP/ICMP Floods
- DNS Reflection Attack
- HTTP flood

Vulnerability/Exploit

- LAND Attack
- Bad TCP Options/Size
- Invalid DNS Opcode
- Apache killer, PostOfDoom
- Apache Struts

Method: Create malformed/ crafted requests & packets targeting software security holes

Resource Attacked: Software stack of security and server infrastructure

Stateful Asymmetric

Method: Create packets/requests requiring security and server infrastructure under attack to maintain state

Resource Attacked: Memory of security and server infrastructure

- SYN Floods
- Fragmentation Attacks
- Slow-Loris/Post, Slow Post/GET
- FTP Ephemeral Opens,
- Slow file download

Computational Asymmetric

- SSL Renegotiation
- Heavy URL's
- XML DND, XML external entity logic (e.g.: Ask where are the closest ATMs?)

Method: Create requests that have large computational cost on security and server infrastructure under attack

Resource Attacked: Compute Resources of security and server infrastructure (Middleware/DB) of Server

Use custom scripts for zero day attack and other vulnerability exploits protection

MITIGATION

Rate Limiting (L3-L7)

Strengths:
- Fast, easy for hardware implementation
- Deterministic/ predictable

Considerations:
- Dependent on 5-tuple/header info to distinguish "Good" vs. "Bad"

Set proper thresholds for load

Client Challenge (L7-L8)

Strengths:
- Use client response to lower false-pos/neg. rate
- Weed out botnets to protect server resources
- Computational challenge can limit per-attacker rate

Considerations:
- May not work with all listener types (Forwarding, BigTCP)

Reputation List (L3-L7)

Strengths:
- Detect in Layer 7 and block in Layer 3
- Real-time updates

Considerations:
- Does work against many volumetric network attacks (spoofed source addresses)

Use Web Application Firewall flow definition for application logic DOS

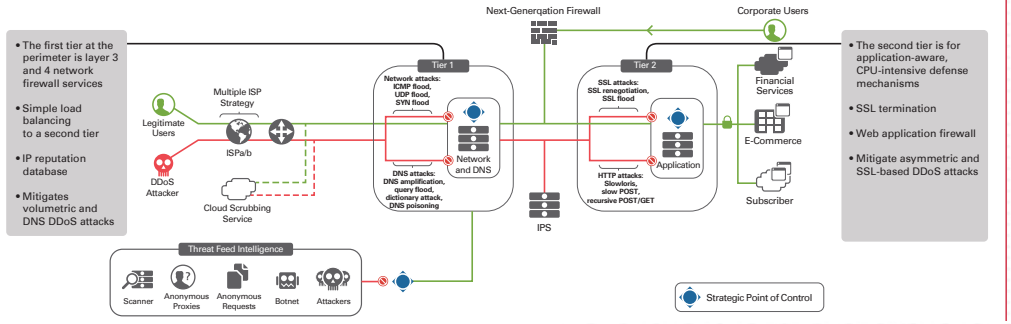
Set proper protocol protection

Set proper timeouts

Full Proxy Architecture (L3-L8)

Strengths:
- Manipulate packages
- Programmability
- Flexibility

DDoS Protection Reference Architecture



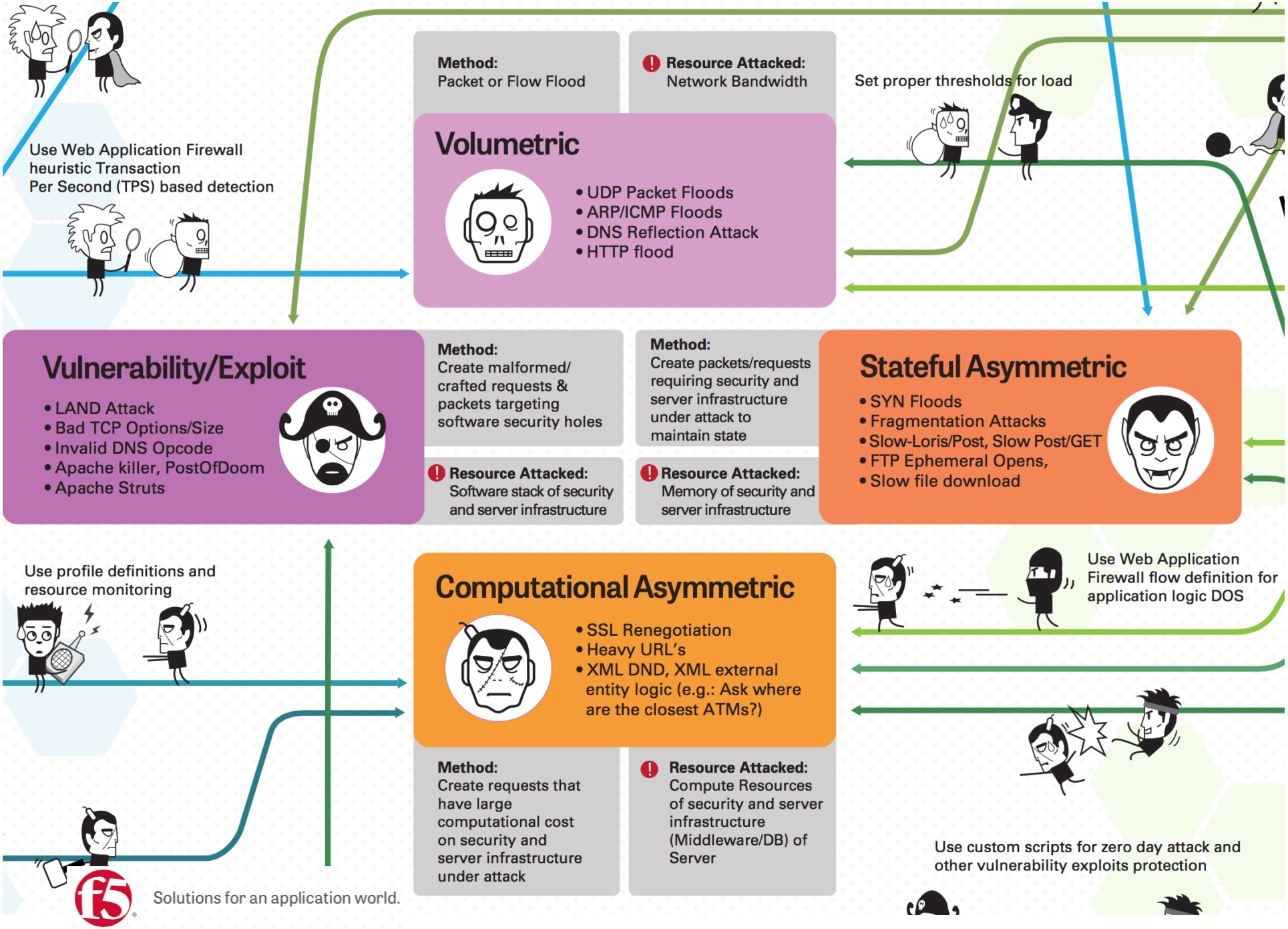
Get the DDoS Protection Exclusive Resources!

http://delivr.com/2wgtk

Sources : F5 Security Forums

http://resources.idgenterprise.com/original/AST-0127081_Mitigating_Multiple_DDoSAttack_Vectors_Infographic.PDF

Solutions for an application world.


Use Web Application Firewall
heuristic Transaction
Per Second (TPS) based detection
Method:
Packet or Flow Flood
Resource Attacked:
Network Bandwidth
Volumetric
• UDP Packet Floods
• ARP/ICMP Floods
• DNS Reflection Attack
• HTTP flood
Set proper thresholds for load
Vulnerability/Exploit
• LAND Attack
• Bad TCP Options/Size
• Invalid DNS Opcode
• Apache killer, PostOfDoom
• Apache Struts
Method:
Create malformed/
crafted requests &
packets targeting
software security holes
Resource Attacked:
Software stack of security
and server infrastructure
Method:
Create packets/requests
requiring security and
server infrastructure
under attack to
maintain state
Resource Attacked:
Memory of security and
server infrastructure
Stateful Asymmetric
• SYN Floods
• Fragmentation Attacks
• Slow-Loris/Post, Slow Post/GET
• FTP Ephemeral Opens,
• Slow file download
Use profile definitions and
resource monitoring
Computational Asymmetric
• SSL Renegotiation
• Heavy URL's
• XML DND, XML external
entity logic (e.g.: Ask where
are the closest ATMs?)
Use Web Application
Firewall flow definition for
application logic DOS
Method:
Create requests that
have large
computational cost
on security and
server infrastructure
under attack
Resource Attacked:
Compute Resources
of security and server
infrastructure
(Middleware/DB) of
Server
Use custom scripts for zero day attack and
other vulnerability exploits protection
f5
Solutions for an application world.

DETECTION

Signature Based

Strengths:
- Ease of hardware implementation
- Fast deterministic
- False positive rate

Considerations:
- Reactive
- Some may not be able to distinguish volumetric "Good" vs. "Bad"

Heuristic Flow Analysis

Strengths:
- Good at "Good" vs."Bad"
- Pro-actively finds anomalies

Considerations:
- May require "baseline-ing"

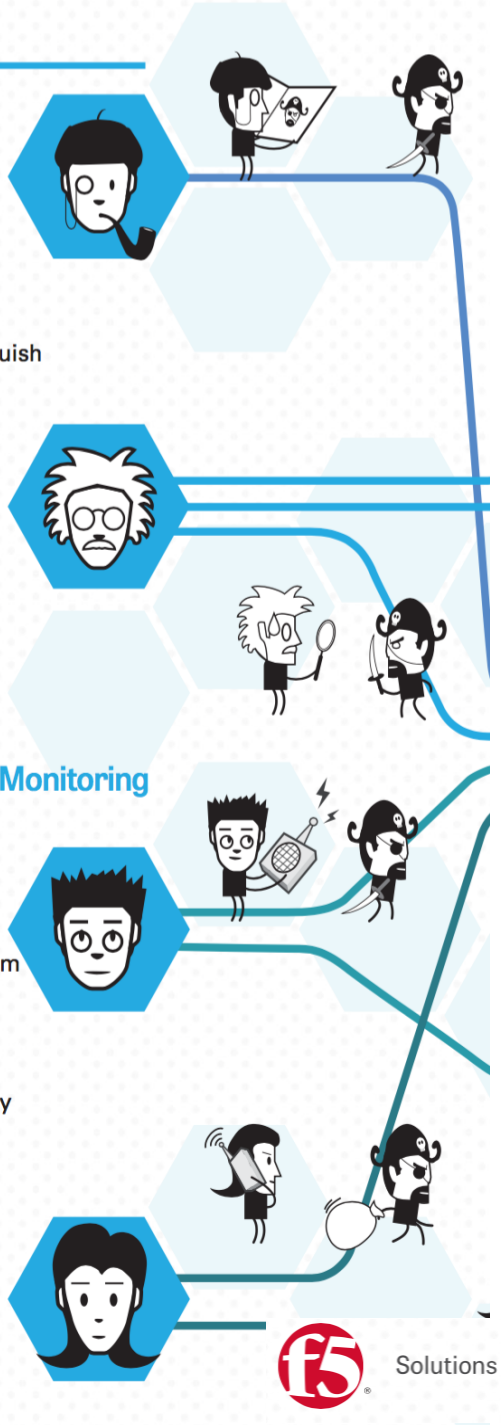
Security Appliance Resource Monitoring

Strengths:
- Based on attack's target (not specific to attack mechanism)
- Low false positive/negative rate
- Feedback-driven security appliance self-defense mechanism

Considerations:
- Protects only resources that are monitored
- Not server-aware; doesn't directly protect server

Server Resource Monitoring

Strengths:
- Based on attack's target (not specific to attack mechanism)
- Low false positive/negative rate
- Server-centric
- Feedback-driven



MITIGATION

Rate Limiting (L3-L7)

Strengths:
- Fast, easy for hardware implementation
- Deterministic/ predictable

Considerations:
- Dependent on 5-tuple/header info to distinguish "Good" vs. "Bad"

Client Challenge (L7-L8)

Strengths:
- Use client response to lower false-pos/neg. rate
- Weed out botnets to protect server resources
- Computational challenge can limit per-attacker rate

Considerations:
- May not work with all listener types (Forwarding, BigTCP)

Reputation List (L3-L7)

Strengths:
- Detect in Layer 7 and block in Layer 3
- Real-time updates

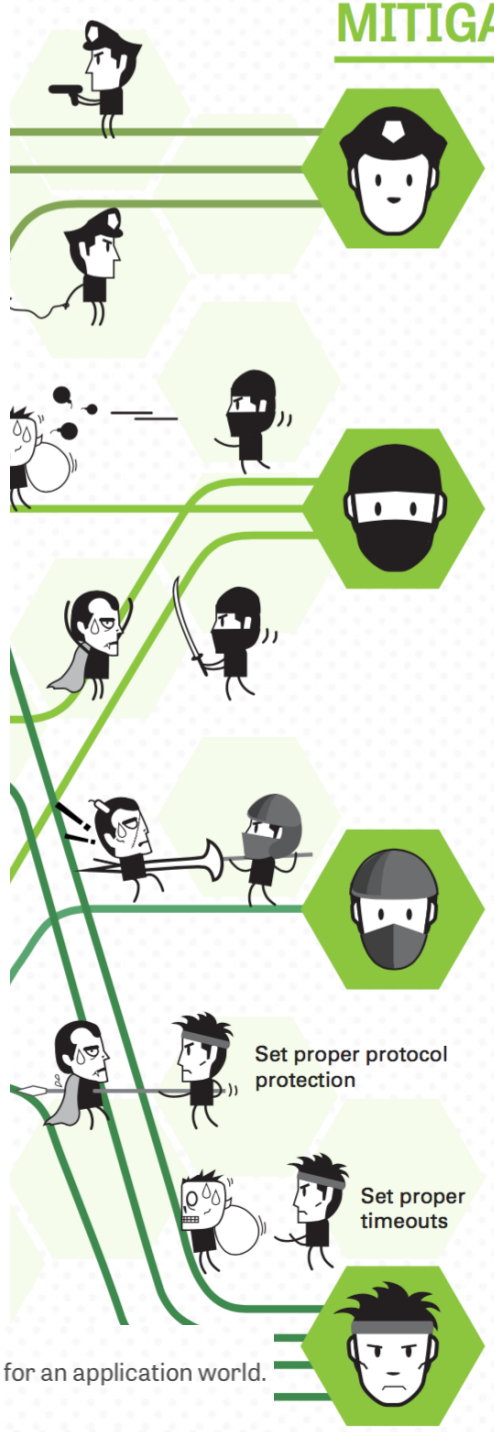
Considerations:
- Does work against many volumetric network attacks (spoofed source addresses)

Set proper protocol protection

Set proper timeouts

Full Proxy Architecture (L3-L8)

Strengths:
- Manipulate packages
- Programmability
- Flexibility



f5

Solutions for an application world.

Attack Mitigation Techniques

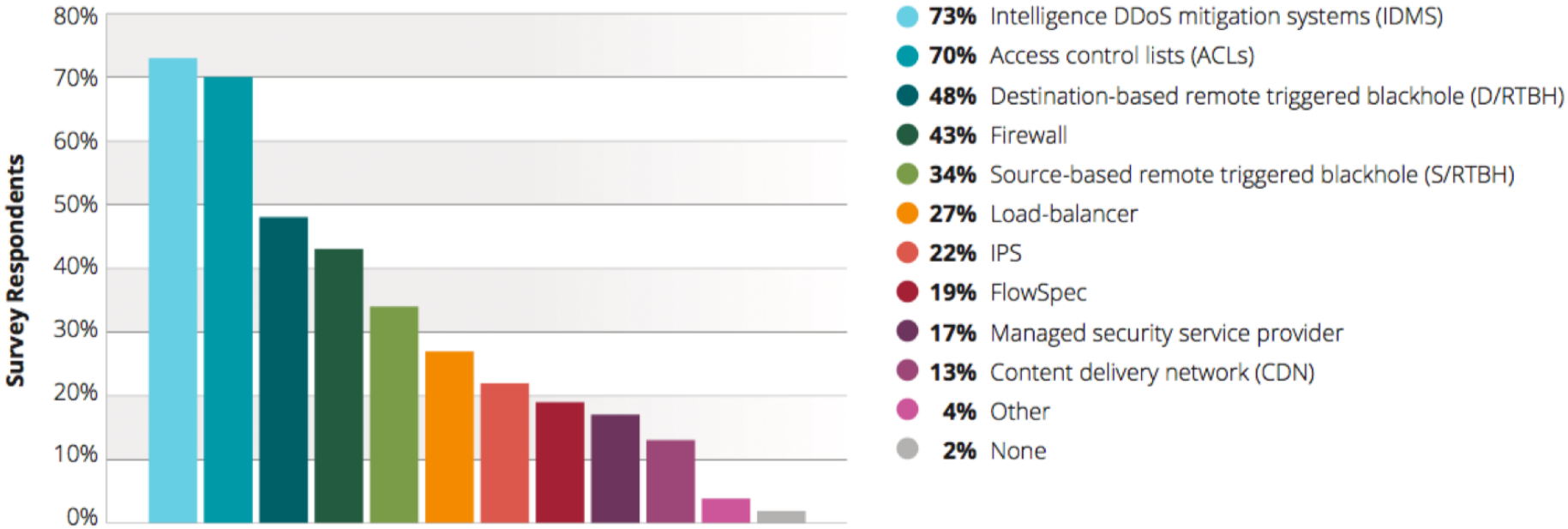
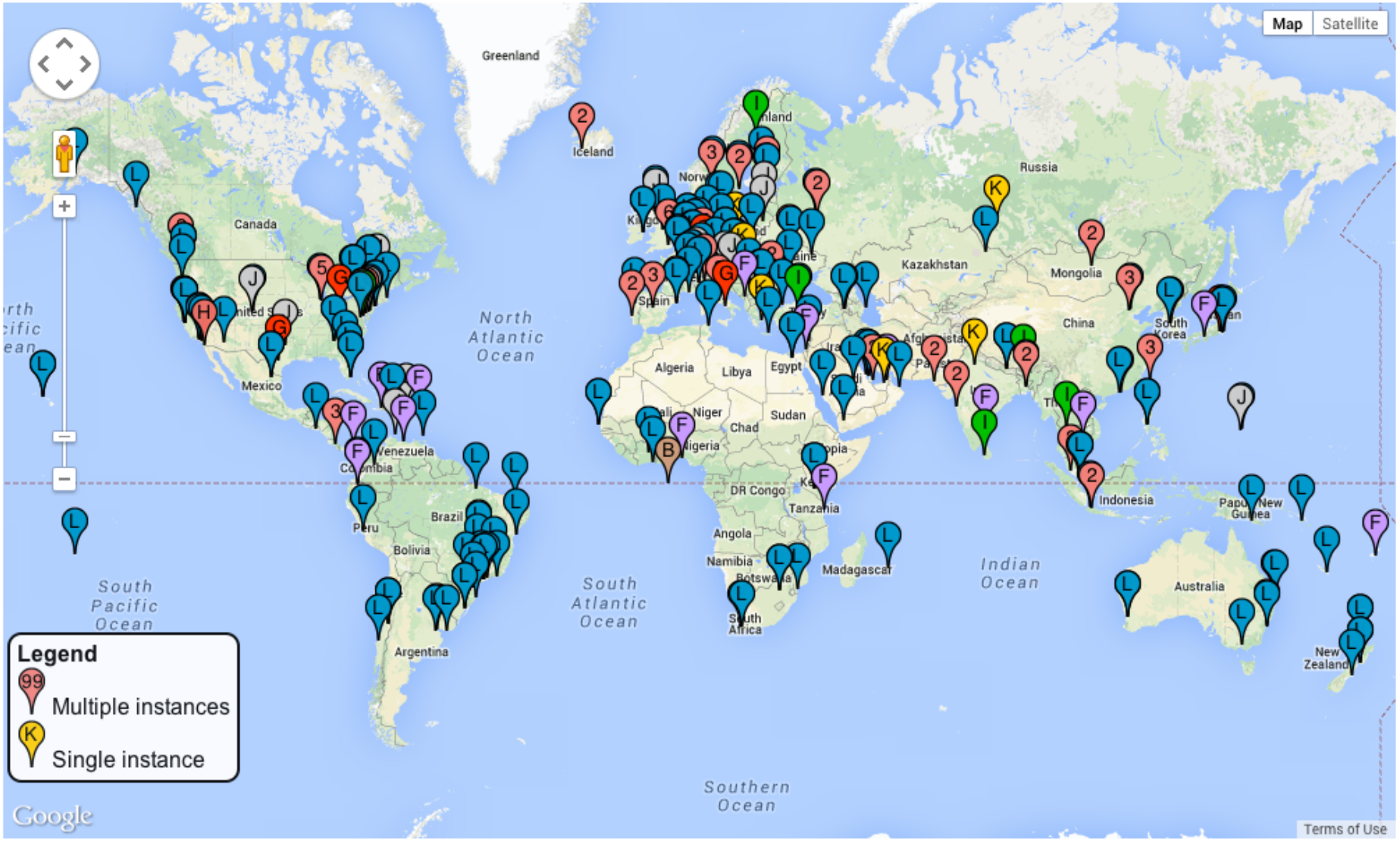
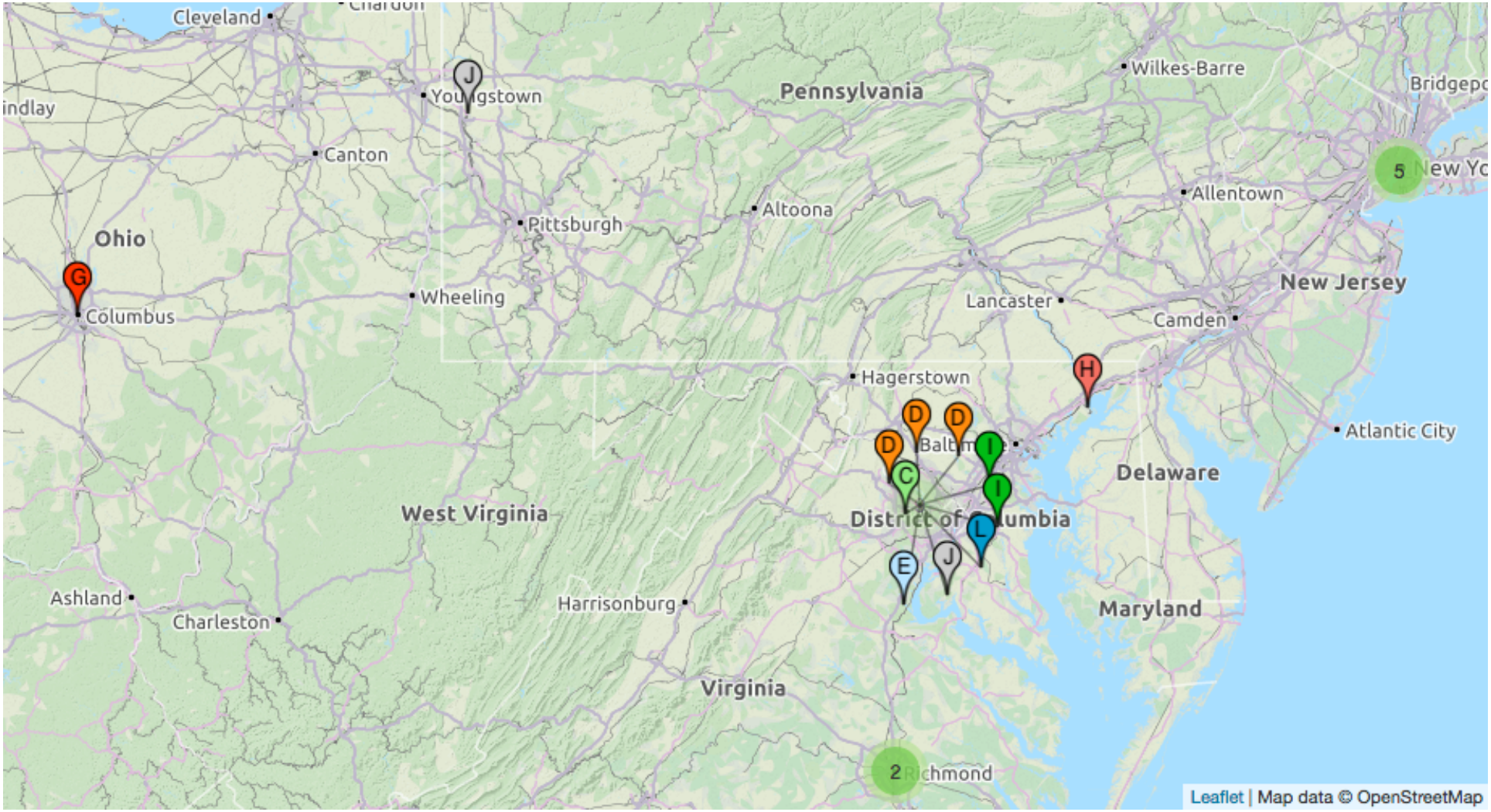


Figure 27 *Source: Arbor Networks, Inc.*



Server	Operator	Locations	IP Addresses	AS Number
A	Verisign, Inc.	**Sites: 4** Global: 4 Local: 0 **Los Angeles, CA, US *; New York, NY, US *; Frankfurt, DE *; Hong Kong, HK ***	IPv4: 198.41.0.4 IPv6: 2001:503:BA3E::2:30	19836


Cleveland
Youngstown
Pennsylvania
Wilkes-Barre
Canton
Pittsburgh
Altoona
Allentown
Ohio
Columbus
Wheeling
New Jersey
Lancaster
Camden
Hagerstown
Atlantic City
Delaware
West Virginia
District of Columbia
Ashland
Charleston
Harrisonburg
Maryland
Virginia
Richmond
5
2
Leaflet | Map data © OpenStreetMap

Root Servers

Archives

A B C D E F G H I J K L M

Operator: Netnod — Homepage | Peering Policy | Contact Email

Locations:

Sites: 50

Amsterdam, NL | Ankara, TR | Ashburn, US | Bangkok, TH | Beijing, CN | Belgrade, RS | Brussels, BE | Bucharest, RO | Chicago, US | Doha, QA | Dubai, AE | Frankfurt, DE | Geneva, CH | Helsinki, FI | HongKong, CN | Jakarta, ID | Johannesburg, ZA | Karachi, PK | Kathmandu, NP | Kiev, UA | Kigali, RW | Kuala Lumpur, MY | London, UK | Lulea, SE | Luxembourg City, LU | Manama, BH | Manila, PH | Miami, US | Milan, IT | Mumbai, IN | Oslo, NO | Paris, FR | Perth, AU | Port Vila, VU | Porto Alegre, BR | San Francisco, US | Singapore, SG | St Petersburg, RU | Stockholm, SE | Taipei, TW | Tallinn, EE | Thimphu, BT | Tokyo, JP | Ulaanbaatar, MN | Washington DC, US | Wellington, NZ | Wien, AT | Yerevan, AM

IPs:

IPv4: 192.36.148.17
IPv6: 2001:7fe::53

ASN: 29216