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

Method: Packet or Flow Flood

Resource Attacked: Network Bandwidth

Volumetric

- 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

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

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

Set proper thresholds for load

Use Web Application Firewall flow definition for application logic DOS

Set proper protocol protection

Set proper timeouts

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"

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)

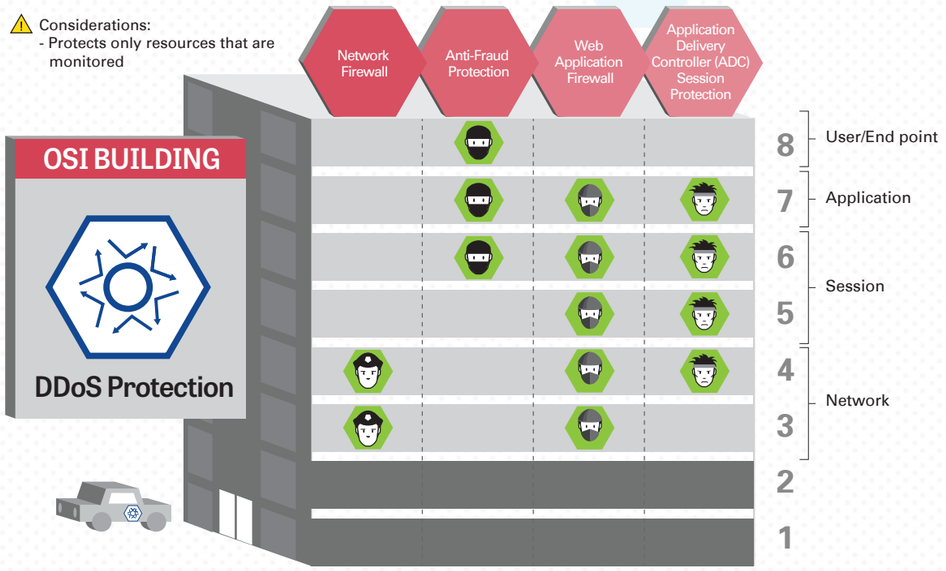
Reputation List (L3-L7)

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

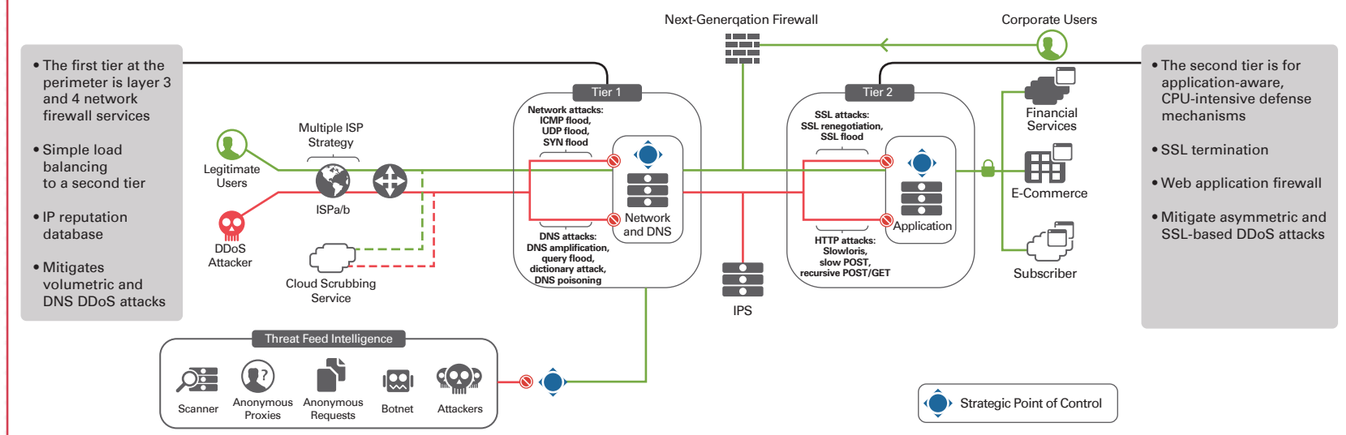
Considerations:
- Does work against many volumetric network attacks (spoofed source addresses)

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