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).

**DDoS Protection Reference Architecture**

- **The first tier at the perimeter is layer 2 and 4 network firewal services:**
  - Simple load balancing to a second tier
  - IP reputation database
  - Mitigates volumetric and DNS DDoS attacks

- **The second tier is for application-aware, CPU-intensive defense mechanisms:**
  - SSL termination
  - Web application firewall
  - Mitigate asymmetric and SSL-based DDoS attacks

**Detected and Mitigated DDoS**

- **Informed by Threat Feed Intelligence**
- **Abuse of legacy, untrusted and compromised services**
- **After identifying the attack vectors:**
  - Use profile definitions and resource monitoring
  - Use profile definitions and resource monitoring
  - Use profile definitions and resource monitoring
  - Use profile definitions and resource monitoring
  - Use profile definitions and resource monitoring
- **Use Web Application Firewall heuristic detection**
- **Use Web Application Firewall heuristic detection**
- **Use Web Application Firewall heuristic detection**
- **Use Web Application Firewall heuristic detection**
- **Use Web Application Firewall heuristic detection**

**Volumetric**

- **Packet or Flow Flood**
  - UDP Packet Floods
  - ARP/ICMP Floods
  - DNS Reflection Attack
  - HTTP Flood

**Stateful Asymmetric**

- **SYN Floods**
  - Fragmentation Attacks
  - Slow-Low/Pat, Slow-Post/GET
  - FFS Ephe_temporal Operations
  - Slow File dawned

**Computational Asymmetric**

- **SSL Re-encryption**
  - Heavy URL’s
  - XML, DTD, XML external entity logs (e.g., Ask where are the closest ATMs?)

**Signature Based**

- **- Ease of hardware implementation**
  - Fast determinants
  - False positive rate

**Heuristic Flow Analysis**

- **- Good at “Good” vs. “Bad”**
  - Pro-actively finds anomalies

**Vulnerability/Exploit**

- **- LAND Attack**
  - Bad TCP Options/Size
  - Apache killer, PostOfDoom
  - Apache Struts

**Server Resource Monitoring**

- **- Based on attack’s target (not specific to attack mechanism)**
  - Low false positives/negative rate
  - Feedback-driven security appliance self-defense mechanism

**Security Appliance Resource Monitoring**

- **- Based on attack’s target (not specific to attack mechanism)**
  - Low false positives/negative rate
  - Feedback-driven security appliance self-defense mechanism

**Server Resource Monitoring**

- **- Based on attack’s target (not specific to attack mechanism)**
  - Low false positives/negative rate
  - Feedback-driven security appliance self-defense mechanism

**User/End point**

- **Network**
  - Firewall
  - Anti-Fraud Protection
  - Web Application Firewall
  - Application Delivery Controller (L7)
  - Session Protection

**OSI BUILDING**

- **DDoS Protection**
  - Network
  - Application
  - Session
  - User/End point

**Sources:** FS Security Forums