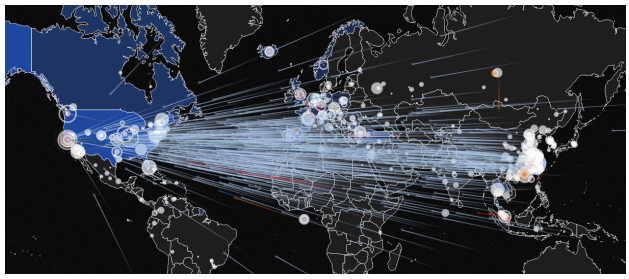
Security Trends in 2016: Defending DDoS Attacks

John Wagnon, 2017-09-02



Distributed Denial of Service (DDoS) attacks were huge in 2016, and they will likely be a tough nemesis again in 2017…and beyond! With all the excitement and trepidation surrounding these attacks, it's important to know how to defend against them. It's also important to know what to do if you get attacked. Because, honestly, it's not *IF* you get attacked but *WHEN*.

The best place to start when discussing DDoS defense is to study a known DDoS-resilient architecture. If you don't know of one, F5 provides a great multi-tiered example for you to consider. The idea behind the multi-tiered architecture is to mitigate various types of DDoS attack vectors at different strategic points while also providing flexibility in the way you defend against those attacks.

The first tier of DDoS defense should be a cloud-based scrubbing service that can protect against things like volumetric attacks. A good scrubbing service will also have a dedicated team of professionals who are experts at defending DDoS attacks. You can leverage this expertise from your scrubbing service because, most likely, you don't have the resources to employ your own dedicated DDoS defense team.

The next tier should focus on DNS and lower-layer attacks like SYN Floods, ICMP Floods, etc.

Then, the last tier can focus on mitigating upper-layer attacks like Slowloris, SSL Renegotiation, RUDY, etc.

Multi-tiered architecture also allows each tier to scale independently of the other. So, if you are experiencing a big attack at Layer 7 and you need more Web Application Firewall power, you can add appliances at that tier and not have to worry about scaling up the other tiers as well. Also, different tiers allow for different platform types at each tier, software versions, etc. The bottomline with a multi-tiered architecture is that it allows for the flexibility you will most likely need in order to defend against an attack.

Having a strong architecture to defend DDoS attacks is critical, but it's also important to know some of the detailed mitigation techniques to employ as well. Some of the more common defense actions include (but are certainly not limited to):

- Use protocol validation for DNS attacks
- Over-provision DNS services to withstand DNS query attacks
- Use multiple DNS providers to serve addresses for your critical applicatoins
- Implement DNSSEC
- Configure and verify logging capabilities
- Configure your network firewall to withstand Layer 4 attacks (BIG-IP AFM DoS Protection Profile excels at this)
- Throttle connections based on request-per-second metrics

While it is a good thing to put all these plans in place to withstand a DDoS attack, it's also very important to have a plan to execute when you actually get attacked. F5's own David Holmes is seriously one of the leading experts in this stuff, and he published a DDoS Playbook that outlines "Ten Steps for Combating DDoS in Real Time." Those steps are:

1. Verify the attack
2. Contact team leads

3. Triage applications
4. Identify the attack
5. Protect remote users and partners
6. Evaluate source address mitigation options
7. Mitigate specific application attacks
8. Increase application-level security postures
9. Constrain resources
10. Manage public relations

Using a resilient architecture, implementing best practices for DDoS mitigation, and executing a well-defined plan will help you defend against and respond to any DDoS attack you will face.

Related Resources:

- F5 DDoS Protection
- F5 Silverline Cloud Scrubbing Service
- BIG-IP DNS Services
- BIG-IP Web Application Firewall
- BIG-IP Layer 3/4 Firewall

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com