Building a DDoS Protection Architecture

Distributed denial-of-service (DDoS) attacks are constantly changing. While the objective is still to cause a service outage, attacks and attackers are becoming more sophisticated. Motivations for attacks are increasingly financial or political—with more serious consequences for the targeted victims.

In the past, DDoS attacks focused on layers 3-4, and network firewalls were able to provide a basic line of defense. In response to that defense, attackers are moving up the stack and focusing on using SSL and application-layer attacks to overwhelm resources.

Conventional network firewalls have failed to keep up with the volume and intelligence of these attacks. These firewalls have no contextual understanding of the traffic they handle, and so they are powerless to defend against multi-layered attacks.

Cloud-based scrubbing services have emerged as a useful tool against large-scale volumetric attacks. However, they can't provide comprehensive protection against all forms of DDoS attacks. Strong on-premises security is necessary to mitigate attacks targeted at application servers (such as business logic attacks) and DNS servers, as well as attacks hidden in SSL-encrypted communications.

F5 Multi-Tier Architecture: Protection at All Layers

Faced with the prospect of crippling DDoS attacks, large financial customers and enterprises have been redesigning their networks to include DDoS mitigation. Working with these customers, F5 has developed a DDoS protection architecture that includes F5 security products across two tiers. Tier 1 provides DDoS protection for DNS and layers 3 and 4. Freed from the noise of the network attacks, tier 2 can use its CPU resources to protect the higher-layer application protocols. This strategy is already providing benefits at several F5 customer data centers.

This multi-tier architecture enables the application layer at tier 2 to scale independently of tier 1. It also allows different code versions, platforms, and even security policies to exist within the two tiers. For example, a new policy in F5's web application firewall can be deployed to a single standalone unit at tier 2. Tier 1 can then direct one percent of traffic to it until the new policy is validated.

At the other end of the scale, smaller organizations are looking to maximize the value of every IT dollar. These customers are consolidating on a single, integrated security platform. For these organizations, F5 provides a cost-efficient, one-tier solution that includes complete DDoS resistance from layers 3 through 7, including DNS and SSL.

Key features

- **Scale and performance**—Handle up to 576 million concurrent connections, 640 Gbps of throughput, and 8 million connections per second.
- **Intelligence and context**—Monitor incoming connections for anomalous latency to distinguish attackers from valid users.
- **Protect all layers**—Get DDoS security at all layers: network, DNS, SSL, and application. Protect not only protocols (including UDP, TCP, SIP, DNS, HTTP, and SSL) but also applications.
- **Dynamic threat mitigation**—Use F5 iRules to create a zero-day dynamic security context.

Key benefits

- **Protect network infrastructure**—Mitigate attacks before they reach your network with dedicated hardware and purpose-built, full-proxy architecture.
- **Safeguard your brand reputation**—Ensure customers can always conduct business through your web applications.
- **Defend against targeted attacks**—Protect against a breadth of DDoS attack vectors and mitigate crafted attacks.
- **Save money**—Consolidate your DDoS protection services onto your existing F5 platform and save OpEx costs.

Solution

The components of the F5 DDoS solution support high-scale, high-performance architectures, with full-proxy, deep application fluency. They provide an intrinsic security because they are inline and already inspecting every single user connection instead of sampling or watching traffic off a mirrored port. This is what has enabled F5 customers around the world to combat DDoS every single day for more than 10 years. In many cases, F5 is the only solution in a position to combat a DDoS attack and guarantee availability.

The F5 DDoS protection solution comes from the intrinsic security built into each of the following intelligent and scalable components of the F5 security portfolio:

- High-performance **network firewall capabilities** defend against network-layer DDoS attacks such as SYN floods and ICMP floods.
- An industry-leading **web application firewall** uses deep application fluency to detect and mitigate HTTP-based attacks.
- **Full-proxy DNS architecture** mitigates DNS DDoS floods while validating every DNS request and providing every DNS response.
- The F5 **application delivery controller** protects SSL resources by absorbing SSL DDoS attacks with high-performance, high-capacity cryptographic offload hardware.
- F5 has a long history of defending against zero-day attacks with the **rich, data-plane programming** of the iRules® scripting language.

Learn more

For more information about F5 DDoS protection solutions, please see the following resources or use the search function on f5.com.

Solution pages

F5 DDoS Protection

Product pages

BIG-IP Advanced Firewall Manager

BIG-IP Application Security Manager

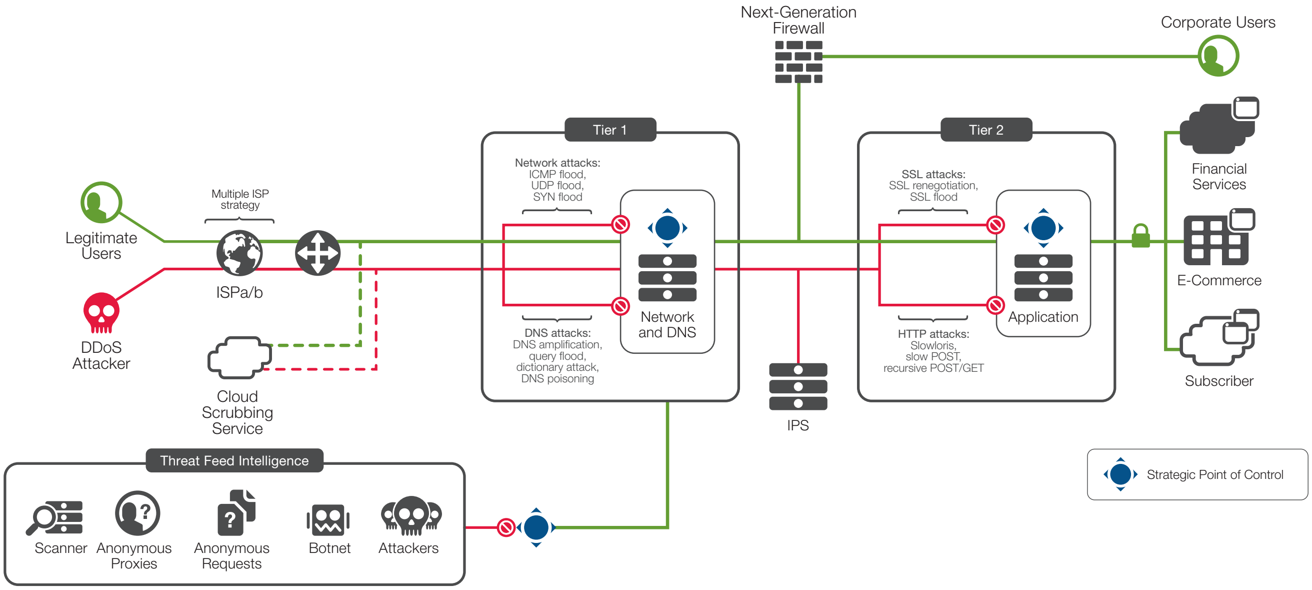
BIG-IP Global Traffic Manager

BIG-IP Local Traffic Manager

White papers

The DDoS Threat Spectrum

Mitigating DDoS Attacks with F5 Technology



A two-tier DDoS protection architecture provides greater efficiency and flexibility in scaling security components.

F5 Networks, Inc. 401 Elliott Avenue West, Seattle, WA 98119 888-882-4447 www.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

Solutions for an application world.