Solution Overview

F5 Distributed Cloud DNS–DDoS Security Capabilities

As part of the F5 Distributed Cloud platform, F5 Distributed Cloud DNS delivers and protects apps, addressing web app security by providing a robust and scalable solution to handle diverse DDoS-style attacks.

Key Benefits

Assess health and availability
Chart traffic patterns across your network from the F5 Distributed Cloud DNS console to identify and log suspicious traffic dynamics.

Leverage attack alerts and insights
A DDoS attack creates a security event observable from the Distributed Cloud dashboard, enabling you to identify the origin of the attack, respond quickly, and harden defenses for the future.

Build resiliency into your network
Seamless failover to F5 Distributed Cloud DNS means your applications have resiliency built in—no matter the traffic demands they face.

Security may not be the first topic that comes to mind when considering how a DNS solution will fit into your application environment. It would be a mistake, however, to think of a DNS service as anything less than a linchpin in the stability and reliability of your network and app delivery operations. As a cornerstone of the digital ecosystem, it presents a tempting target for Distributed Denial of Service (DDoS) attacks.

DDoS attacks are designed to overwhelm and incapacitate critical services. Often orchestrated by malicious individuals, they leverage a coordinated botnet of compromised, networked computer devices. While a single compromised device may inflict only minimal disruption by most processing throughput standards, a sophisticated multipronged attack from a large botnet can reach throughput levels that many enterprise networks cannot withstand.

So, what might these attacks look like? Here are three examples:

1. **Stateless Attacks:** These are popular because they require minimal resources and work with source IP address spoofing. The TCP SYN flood attack is one instance. Attackers send a barrage of SYN requests to a target server but never complete the handshake by sending the final ACK. This leaves the server with half-open connections, consuming resources and eventually overwhelming its capacity to handle legitimate traffic. Flooding the server with incomplete connections can bring a service to a crawl or make it unavailable, disrupting business operations and user access.
2. **Stateful Attacks:** These are generally more successful and harder to stop. They mimic the behavior of legitimate users to create a sizable amount of traffic using a significant number of attackers. The attacks prevail when the victim cannot consume or process all the requests, or when the service's internet connection reaches capacity. Because the traffic is crafted to emulate the behavior of normal users, it is extremely difficult to detect and differentiate malicious traffic from legitimate.
3. **Amplification Attacks:** These attacks can be particularly harmful because the response from the server is often excessively greater than the original request. The attacks leverage the distributed nature of a botnet and the amplification potential of DNS servers. The overwhelming flood of amplified data can quickly saturate the target's network bandwidth, causing severe disruption or a complete outage of services.

We often focus our attention on the more conspicuous threats highlighted in the OWASP top 10, fortifying our networks with advanced web application firewalls and robust API protection mechanisms. So, it's easy to overlook DNS as a security component as it facilitates zone transfers, directs traffic, scales to meet demand, and enhances performance.

Key Features

Scale for surges and keep DNS online
Distributed Cloud DNS is built on F5's Anycast network, which provides heightened scalability in the event of a traffic surge—including DDoS attacks—without compromising performance or security.

Avoid outages by deploying automatic failover
Keep apps and sites online and available in the event of a data center outage or degradation with automatic failover.

Achieve 99.99% availability
The combination of F5's Anycast network and expertise in DNS with BIG-IP empowers users to leverage a service that delivers industry-leading availability and app uptime.

But overlooking the ways in which DNS factors into your overall security posture is akin to a knight charging into battle with a shield, but no armor. Put simply: Without DNS services, your business may have a difficult time existing online at all.

The challenges that DNS faces, particularly in the context of DDoS attacks, are multifaceted:

- Tools developed to safeguard DNS must possess not only an intimate understanding of DNS traffic patterns but also ensure that the end-user experience remains seamless and uninterrupted.
- Detection of anomalous traffic that may signify the onset of a DDoS attack must be both rapid and continuous to prevent the attack from gaining strength and momentum.
- Mitigation strategies must be precise enough to filter out malicious traffic without derailing legitimate queries, all while maintaining the ability to process an immense volume of DNS packets.

So, how can a DNS service help secure every DNS zone and service from malicious attacks across an expanding threat landscape?

F5 Distributed Cloud DNS, Delivered via the F5 SaaS Platform, Comes With Critical Security Capabilities to Assist in the Protection of Infrastructure and Apps

It's widely understood that bad actors will target networks any way they can. Mitigating diverse threats requires teams to deploy an equally varied set of tools to safeguard their applications and networks.

Here are four key tools that F5® Distributed Cloud DNS provides:

Not considering the ways in which DNS factors into your overall security posture is akin to a knight charging into battle with a shield, but no armor.

1. **Security-First Deployment:** Distributed Cloud DNS comes with automatic defense capabilities to defend against and mitigate the impact of DDoS attacks—attempts by bad actors to overwhelm network infrastructure with a flood of traffic—from the moment it is deployed and configured.
2. **Scalability:** With Points of Presence in dozens of locations around the world, the global footprint of F5's Distributed Cloud network enables it to absorb the high traffic volumes typical of DDoS attacks. The infrastructure scales up resources to handle unexpected surges in traffic, providing a stellar defense against these types of attacks.
3. **Traffic Visibility:** Enhanced dashboards provide multi-angle visibility into network traffic, allowing teams to identify and respond to a potential attack quickly and decisively. They also empower more complete post-mortems, so teams can better prepare for the next attack.

When bad actors attempt to take down your network from every public point, it pays to be ready with a solution that can address threats from every angle.

4. **Multi-Vector Protection:** DDoS attacks against DNS services don't always occur in one form. Bad actors use various methods or avenues to launch such attacks. Addressing them requires a simultaneous, multi-vector attack mitigation strategy. Some of the vectors that Distributed Cloud DNS safeguards against include:
   - DNS amplification and reflection attacks
   - NXDOMAIN (non-existent domain) attacks
   - Random subdomain attacks
   - DNS floods

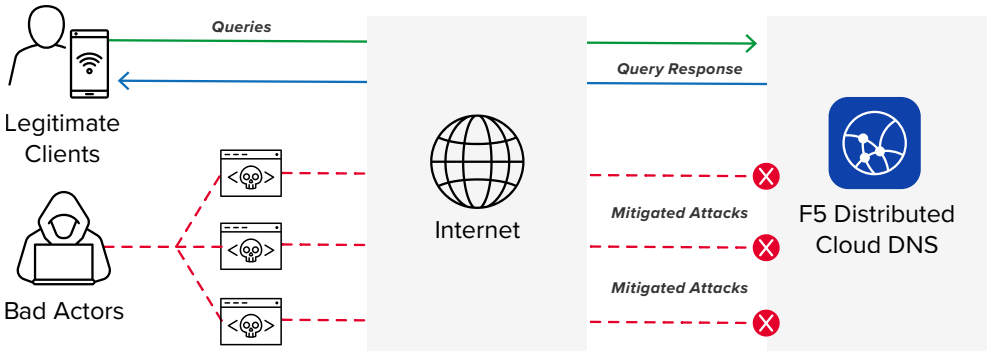

Figure 1: F5 Distributed Cloud DNS blocks malicious traffic in addition to scaling to absorb DNS traffic spikes.

Distributed Cloud DNS: Full Circle Security

Protecting DNS zones is a critical step to a robust network security posture. And so, when bad actors attempt to take down your entire network from any or all public DNS points, it pays to be ready with a solution that can address threats from every angle.

The capabilities that Distributed Cloud DNS brings are part of a comprehensive approach to security built into the solution at a foundational level. They work together to not only keep services operating and performing well, but also to defend against and respond to potential security threats with an ability to scale, boost availability, and build resiliency into a network.

If you want to know more about how these features are implemented and how they can be configured to meet particular security requirements, contact F5 today.

To learn more or get a Distributed Cloud DNS trial, please contact your F5 account manager or F5 sales today.