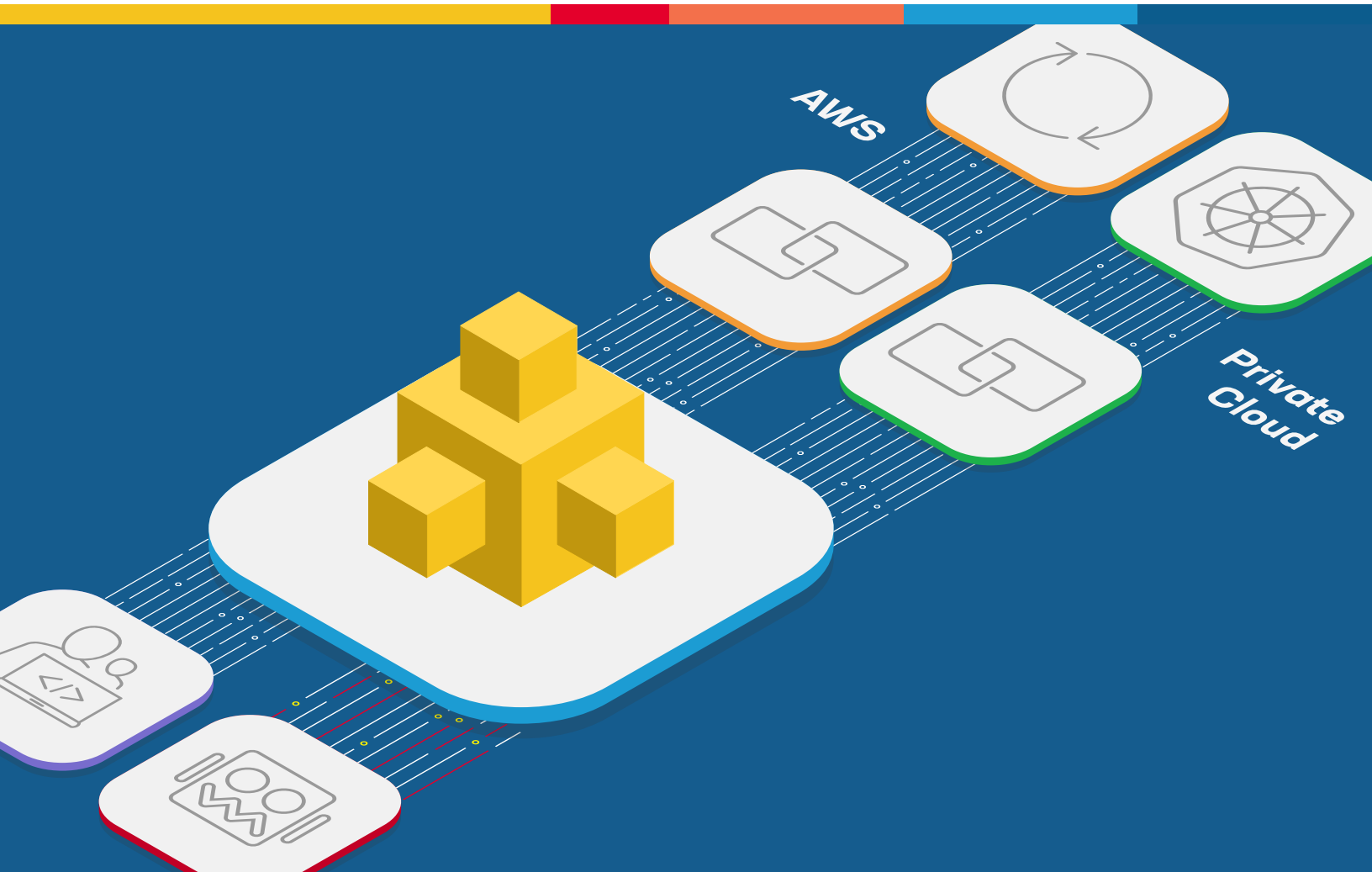
SOLUTION OVERVIEW

Distributed Cloud DDoS Mitigation

F5 Distributed Cloud DDoS Mitigation delivers DDoS and advanced security services to protect against L3-L7 attacks on enterprises and hosting and service providers.



KEY BENEFITS

Maximize uptime
Ensure the availability of critical applications and infrastructure against sophisticated volumetric and distributed attacks by leveraging F5's global network and support.

Reduce total cost of operations
Lower CapEx and OpEx by moving to cloud-based network perimeter security and reduce reliance on appliances and legacy architectures.

On-demand scalability
Dynamically expand capacity and deploy new services on demand without adding appliances or network capacity in your data centers.

Increase productivity
Empower your network and DevOps via a SaaS security platform and central pane of glass. Deliver more projects, new apps, and expanded capacity with existing resources.

The soaring volume and complexity of distributed denial of service (DDoS) attacks in the current decade warrant cause for concern, as well as finding the most sophisticated protection available. According to F5 Labs, DDoS attacks jumped by 55% in a 15-month period ending March 2021 and became increasingly more complex, with 54% of incidents leveraging multiple attack vectors.

The largest attack in that span measured 500 Gbps and used no fewer than five different attack vectors, according to the F5 report on DDoS attack trends. The technology sector was the most targeted, receiving 27% of all DDoS attacks over those 15 months.

Volumetric DDoS attacks, which attempt to consume critical network and application resources, accounted for 73% of all incidents.

But increasingly, threat actors also sought to exploit different layers of the network and application stack. Application attacks saw a sharp increase compared to previous years and were found in 16% of these DDoS attacks.

Today, DDoS mitigation is essential, and the quality and breadth of your solution matters. You need protection against attacks at multiple layers across your network and application ecosystem.

F5® Distributed Cloud DDoS Mitigation—a key offering in F5's SaaS-based Web Application and API Security (WAAP) solution—provides mitigation against a variety of denial-of-service attacks across L3-L7. It does this through multiple layers of protection, from custom DoS rules and edge firewalls prescreening traffic, to deep packet inspection with advanced scrubbing for enterprises, hosting, and service providers.

High-Capacity, Cloud-Based, and Hybrid DDoS Mitigation

To protect customers against DDoS attacks, F5 Distributed Cloud DDoS Mitigation leverages a globally secured network with points of presence (PoPs) deployed in Tier-1 IXCs interconnected across a dedicated, multi-terabit redundant private backbone. F5's PoPs provide robust, cloud network-based infrastructure protection including DDoS mitigation, L3 firewall, and anomaly detection.

INCREASINGLY, THREAT ACTORS SOUGHT TO EXPLOIT DIFFERENT LAYERS OF THE NETWORK AND APPLICATION STACK. APPLICATION ATTACKS SAW A SHARP INCREASE COMPARED TO PREVIOUS YEARS.

KEY FEATURES

Multi-layer global DDoS protection
DDoS mitigation systems are distributed across a spectrum of F5's PoPs worldwide to filter L3/L4 and advanced L7 attacks closest to the attack sources.

High-capacity defense
F5's secured backbone and scrubbing infrastructure is designed to handle today's largest and most complex DDoS attacks with more than 12+ Tbps of combined scrubbing capacity.

Centralized observability
F5 Distributed Cloud Console provides single-pane-of-glass management and is customizable for threat visibility and real-time mitigation data.

Support for all sized customers
F5 on-demand capacity supports the needs of customers of all sizes and scale, including direct BGP connections as well as GRE tunnels.

Continuous attack monitoring/ mitigation
F5's Technical Assistance Center operates 24x7, with high business-continuity dependability when under attack.

Cloud-Based DDoS Mitigation

Distributed Cloud DDoS Mitigation safeguards companies and service providers against DDoS for both their network infrastructure and their web application services. F5® Distributed Cloud Mesh—running in F5's PoPs—provides an intelligent mitigation solution for both network and application traffic, and is deployed upstream from customers' Internet access. It autonomously protects against public-access DDoS attacks.

Thanks to F5's globally deployed and largescale network infrastructure, Distributed Cloud Mesh supports direct Border Gateway Protocol (BGP) connections in addition to Generic Routing Encapsulation (GRE) tunnels. The DDoS mitigation systems are distributed across a spectrum of F5's PoPs worldwide to filter L3/L4 and advanced L7 attacks (via on-demand or always-on service) closest to the attack sources.

Hybrid DDoS Mitigations

Combining on-premises defense with F5's cloud-based DDoS mitigation gives customers the control to defeat targeted network and application-layer attacks. This approach is logical in cases of operating multiple IP transit providers and massive DDoS attack protection when the on-premises appliance cannot handle the full attack volume.

In the event of a volumetric attack overwhelming the capacity of the on-premises appliance or Internet link, DDoS mitigation is activated by an administrator with an API call or directly in the F5® Distributed Cloud Console. The IP prefix under attack is then announced by F5 and mitigated. The scrubbed traffic is received from F5 Distributed Cloud Services either through direct BGP peering or GRE tunneling.

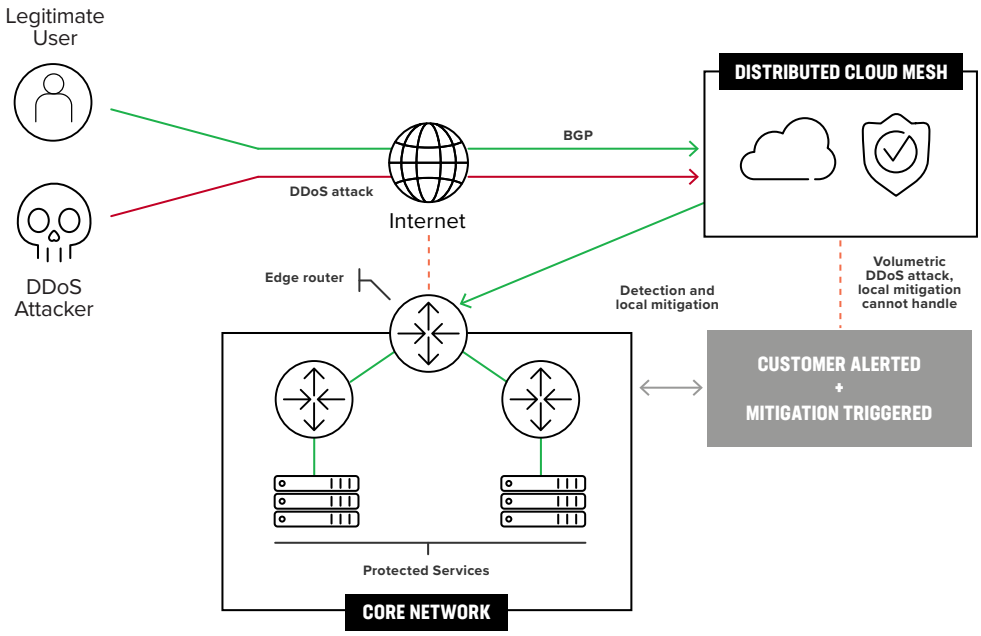


Figure 1: Hybrid DDoS protection: cloud mitigation

F5'S DDOS MITIGATION SYSTEMS ARE DISTRIBUTED ACROSS A SPECTRUM OF F5'S POPS WORLDWIDE TO FILTER L3/L4 AND ADVANCED L7 ATTACKS CLOSEST TO THE ATTACK SOURCES.

Conclusion

F5 Distributed Cloud's secured backbone is designed to handle today's largest and most complex DDoS attacks of more than 3 Tbps. When the attack begins, Distributed Cloud Mesh performs the following actions:

1. Cloud Detection

F5's cloud detection equipment and software detect the attack. Detection is based on a combination of static rules, such as volumetric attacks, and personalized rules per customer:

- Distributed Cloud Mesh routers send NetFlow information to Distributed Cloud NetFlow collectors and analyzers.
- NetFlow allows cloud detection to not miss any alert, with real-time polling and information collection (e.g., source |destination ASN, IP address, next-hop IP | ASN).

2. Customer Alerting

When an attack is detected, our 24/7/365 SecOps Team (Security Operations Center) is alerted and will either notify you to trigger the mitigation or trigger the mitigation on your behalf.

3. Cloud-Based DDoS Scrubbing

Customers can use a variety of service and connectivity options depending on the location of apps, level of service, and protection needed. This includes always-on or always-available scrubbing options and includes several routing choices for scrubbing—such as BGP or DNS-based redirection or via direct connections or peering.

You change your BGP announcements to have transit directed through Distributed Cloud Mesh instead of the other transit providers. Distributed Cloud Services steers the traffic using BGP and our scrubbing centers to block the attack, allowing only legitimate traffic to go through.

For more information about F5 Distributed Cloud DDoS Mitigation and the Distributed Cloud WAAP services, visit f5.com. Contact sales@f5.com to learn more or to schedule a demo.