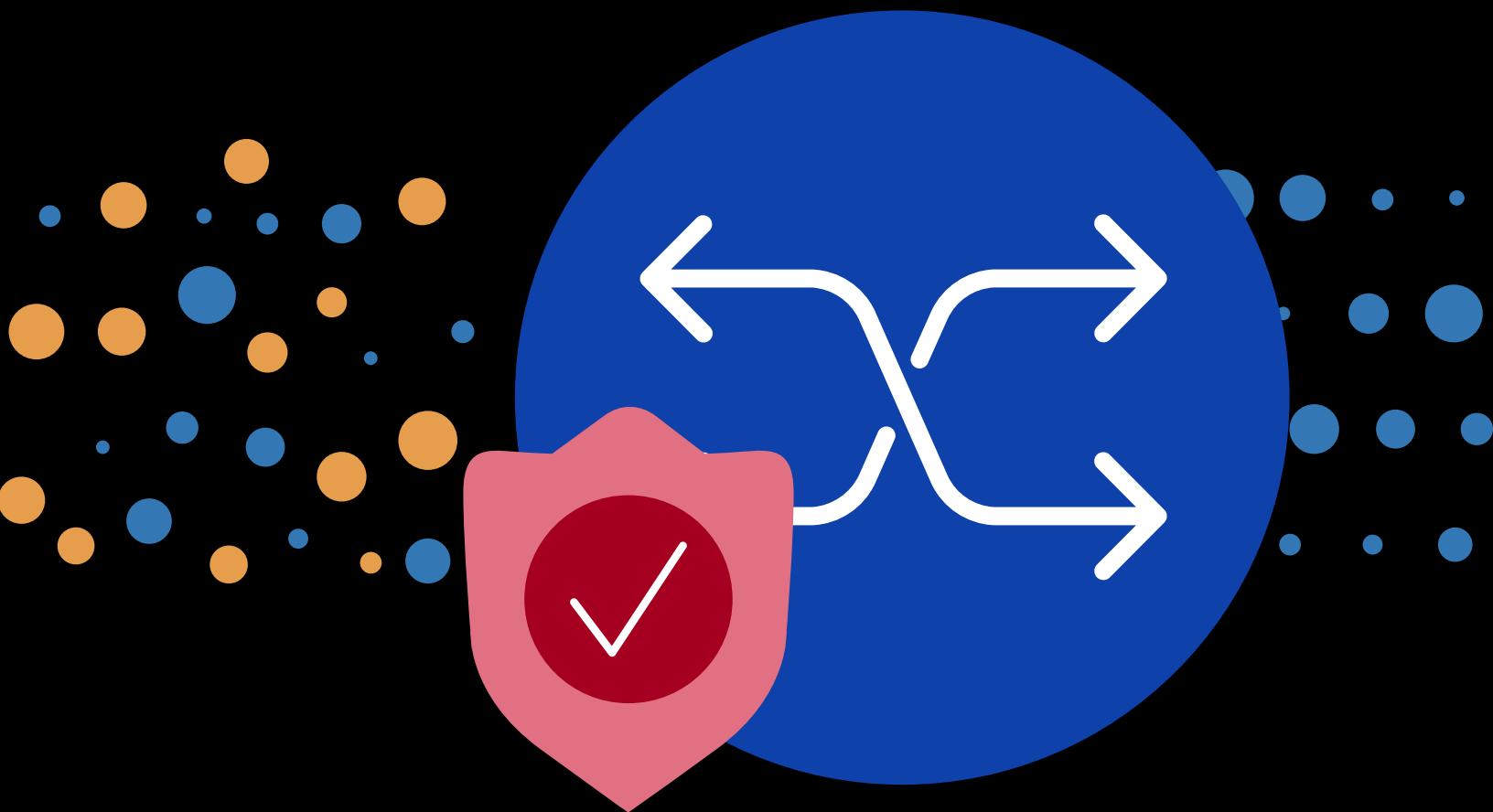# F5 BIG-IP Local Traffic Manager: beyond load balancing

F5® BIG-IP Local Traffic Manager enables client IP visibility to help your organization improve application performance and reliability.

Key benefits

Optimized routing
Unlock client IP visibility to enable traffic steering that directs users to the ideal app instance.

Seamless integration
Deploy into existing infrastructures with SNAT and iRules toolsets—no backend changes required.

Transparent, reliable traffic flow
Maintain proper responses and flow integrity between clients, CDNs, and backend servers while preserving performance and visibility.

Accurate data and analytics
Ensure client IP preservation—even through NAT, SSL termination, or load balancing—so downstream services receive accurate user data.

Stronger security
Expose real client IPs to WAFs, rate limiters, and access policies to strengthen threat detection, bot defense, and IP-based access controls.

The importance of client IP visibility in modern applications

Accurate logging of client IP addresses plays a critical role in today's application environments. Whether for security monitoring, analytics, compliance, or troubleshooting, capturing the original source IP of users accessing web applications is essential. However, organizations that rely on content delivery networks (CDNs) to optimize performance and distribute content often encounter unique challenges in maintaining visibility into client IPs. Many CDNs act as intermediaries between users and application infrastructure, masking the original source IP as traffic flows through edge servers.

Organizations with legacy infrastructure like older web servers can find this challenge to be particularly complex. Backend servers may lack the capability to parse HTTP headers like X-Forwarded-For (XFF), where the original client IP is typically delivered by CDNs. As a result, the logging infrastructure at the server layer only captures the IP of the intermediary CDN, limiting the organization's ability to trace user activity accurately.

To solve this problem, organizations need a solution that can seamlessly integrate client IP logging into an existing legacy environment—without requiring disruptive changes to the backend infrastructure.

Enable accurate IP logging with F5 BIG-IP Local Traffic Manager

Through Secure Network Address Translation (SNAT) and custom iRules, F5® BIG-IP Local Traffic Manager (LTM) enables organizations to maintain IP visibility, even when they're using CDNs or legacy infrastructure. To demonstrate how it's possible without backend changes, let's examine the case of how a large financial services and insurance organization uses BIG-IP LTM for client IP visibility.

The company's CDN delivers original client IPs via the XFF HTTP header. This presented a challenge because the legacy web servers could not parse or log the information. Instead, the servers only logged the source IP of incoming traffic—the CDN itself—and not the original client IP address.

The organization implemented a BIG-IP LTM solution leveraging SNAT and a custom iRule to address the issue. The iRule extracts the client's original IP from the XFF header provided by the CDN. BIG-IP LTM then translates the source IP of traffic forwarded to the backend servers to match the original client IP. Configuring BIG-IP LTM as the default gateway for the servers allows return traffic to flow back seamlessly, maintaining proper routing and flow integrity.

Key features

Custom traffic manipulation
Use iRules to direct traffic based on IP addresses, headers, instance-routing, or virtually anything else in the payload.

Source IP translation
Use a single SNAT object to map multiple original addresses to a single translation address or map all node addresses on a network to a single public IP address.

The solution cleanly integrated with existing CDN workflows and upstream infrastructure, enabling secure, high-performance application delivery with minimal architectural disruption.

Through this solution, the organization has preserved client IP visibility end to end without requiring changes to legacy web servers. The result is precise logging and policy enforcement based on true source IPs while maintaining deterministic traffic behavior and session integrity across the environment. The solution cleanly integrated with existing CDN workflows and upstream infrastructure, enabling secure, high-performance application delivery with minimal architectural disruption.

Next steps

Start a trial
See how BIG-IP LTM works for yourself. Start today.

Contact us
Learn how F5 products and solutions can enable you to achieve your goals. Contact F5.

Find a reseller
Explore partners that can help move your business forward. Browse now.