



Optimize DNS, Secure and Ensure Availability, and Monetize Usage

What's Inside

- 2 Increasing Services Demand
- 2 F5 DNS Services in Service Provider Networks
- 9 Simple Management and Programmability
- 11 Network Integration
- 13 Architecture
- 14 BIG-IP DNS Platforms
- 14 DNS Query RPS Maximum Performance
- 15 F5 Global Services
- 16 More Information

To achieve increased ARPU and decreased subscriber churn, communications service providers (CSPs) are focusing on delivering a high subscriber quality of experience (QoE). DNS is a key element in the service provider network that delivers content and services to the user, while ensuring high availability and fast response times. DNS is often the target of disruptive DDoS attacks that affect the security, reliability, and scalability of the DNS infrastructure and ultimately prevent you from providing high QoE.

F5® BIG-IP® DNS (formerly BIG-IP® Global Traffic Manager™) secures your DNS infrastructure through high-performance DNS services; hyperscales DNS responses geographically to survive volume increases and DNS DDoS attacks; and ensures high availability of your global applications and services. In addition, BIG-IP DNS distributes service requests based on business policies, POPs, network conditions, user location, and service performance—and delivers high-performance DNS services with visibility, reporting, and analysis.

Key benefits

Optimize DNS infrastructure and hyperscale responses

With an optimized DNS infrastructure, BIG-IP DNS provides scalability and delivery offload to your LDNS infrastructure, while delivering high-speed DNS by hyper-scaling responses to up to 40 million query responses per second. You can reduce latency up to 80 percent, resulting in higher service delivery and increased subscriber QoE.

Secure DNS and take control of your network

The BIG-IP system is an ICSA Labs–certified network firewall that can defend your DNS infrastructure, while ensuring service availability that mitigates high-volume attacks. In addition, it mitigates DNS threats by blocking access to malicious IP domains.

Ensure DNS and service availability

BIG-IP DNS helps you improve availability by ensuring that subscribers are receiving fast query responses from data centers and POPs.

Monetize with improved network performance

BIG-IP DNS delivers faster response times for content being accessed by fixed and mobile devices, leading to increased revenues from higher data usage and lower subscriber churn. Network performance is also improved by F5's mobile core capabilities—ensuring packet gateway availability and automated monitoring.

Increasing Services Demand

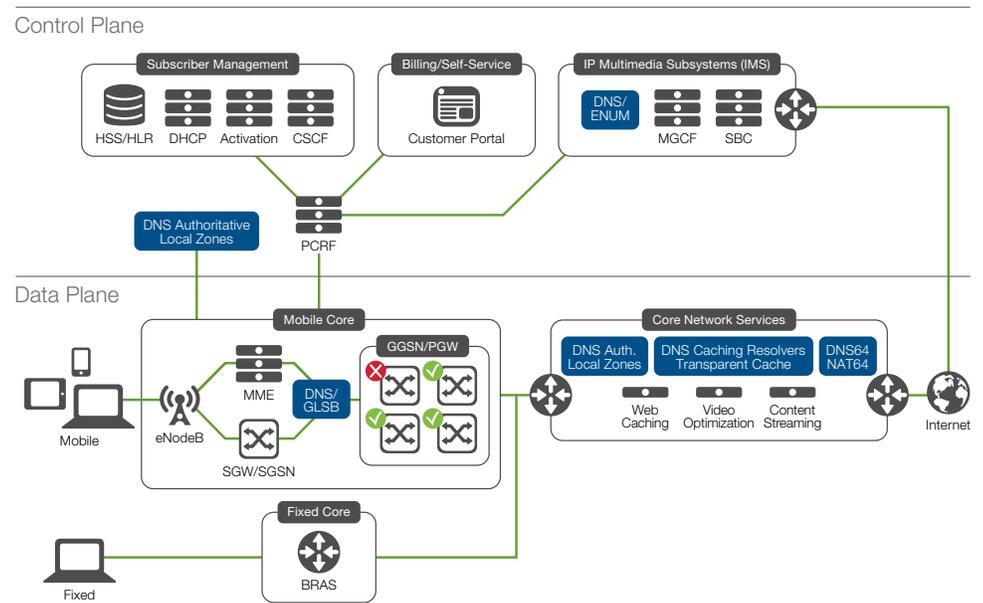
With the increased demand for services and apps, CSPs need to scale to provide availability to subscribers. [Kissmetrics research](#) reports that most mobile users in their survey would wait 6–10 seconds for a site to load on their smartphone before leaving the site.

At the same time, there is little point in having faster data speeds with a 4G/LTE rollout if DNS latency reduction and increased throughput aren't in place to allow the user to experience higher QoE. With lower packet latency (sometimes below 30 milliseconds of round-trip time) and very high wireless bandwidth (above 40 megabits per second [Mbps]), DNS lookups for service selection and web app rendering is an exchange-to-exchange critical path to meet subscriber requirements. Cisco research reports that global mobile data with 4G/LTE is driving the need for fast, available DNS with up to 2.6 GB average usage a month.

In addition, DNS distributed denial-of-service (DDoS) attacks and DNS outages are more prevalent in the news. Not only do these attacks affect enterprises trying to keep their sites and apps available, CSPs are affected when services for subscribers that rely on external DNS and applications are unavailable. In addition, your subscribers' mobile devices could be used in DNS DDoS from remote attackers attempting service delivery disruption. To maximize monetization, DNS must be optimized and secured to deliver increased data usage and reduced subscriber churn.

F5 DNS Services in Service Provider Networks

When service providers look to enhance their mobile core networks for the best services delivery, BIG-IP DNS can provide scalable, secure DNS and global service delivery in both the control and data planes with authoritative infrastructure and LDNS resolver networks offloaded to BIG-IP DNS for a higher subscriber QoE.



BIG-IP DNS with DNS Services scales mobile core network performance and secures DNS in both the data plane and control plane with authoritative DNS, infrastructure DNS, and LDNS resolver services.

F5 DNS Services in BIG-IP DNS are built on an intelligent services framework incorporating naming services across the entire service provider network. BIG-IP DNS works to manage DNS and to guarantee service availability to all users.

BIG-IP DNS provides the following name services:

- Authoritative DNS scalability, handling up to 20 million global name requests per second
- DNS optimization and security for all internal and external services
- Pinpoint service delivery with topology load balancing service
- Single point of control for management of all global and local name services
- Load balancing support for both inline and recursive DNS and ENUM systems
- Support for Name Authority Pointer (NAPTR) and SRV records used in mobile core, IP Multimedia Subsystem (IMS), and Voice over LTE (VoLTE) DNS resolutions, plus caching ENUM requests
- Transparent health monitors to evaluate service health before directing users
- Additional BIG-IP intelligent services such as application delivery, policy enforcement, NAT64 and DNS64 translation, F5 iRules®, and health monitors

Unmatched DNS performance

BIG-IP DNS delivers DNS performance that can handle even the busiest services. This helps you provide the best quality of service for your subscribers while eliminating poor performance.

When your services have DNS query volumes spikes due to legitimate requests or DDoS attacks, BIG-IP DNS manages requests with multicore processing and DNS Express™, dramatically increasing DNS performance to up to 20 million responses per second (RPS) to quickly answer all queries. DNS Express improves standard DNS server functions by offloading DNS functions as a secondary DNS server. BIG-IP DNS zone transfers DNS records from the principal DNS server and answers DNS queries authoritatively—delivering exponential performance improvements that optimize DNS infrastructures, and scaling to protect against DNS outage.

Benefits and features of multicore processing and DNS Express include:

- High-speed response and outage protection with in-memory DNS
- Replicate authoritative DNS in multiple BIG-IP or DNS service deployments for faster responses
- Authoritative DNS and DNSSEC in virtual clouds for disaster recovery and fast, secure responses
- Scalable DNS performance for quality of app and service experience
- Ability to consolidate DNS servers and increase ROI

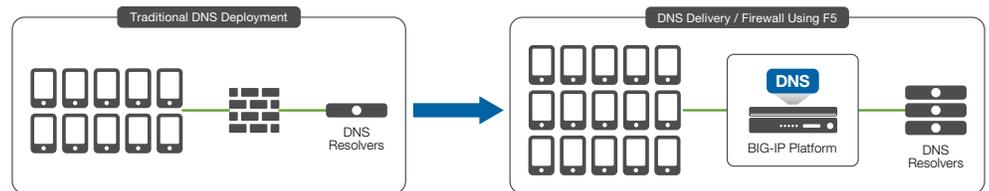
In cases of very high volumes for apps and services or a DNS DDoS attack, BIG-IP DNS hyperscales in Rapid Response Mode (RRM) up to 40 million RPS. It extends availability with unmatched performance and security—absorbing and responding to queries at up to 200 percent of the normal limits. See page 15 for performance metrics and details.

Authoritative DNS for scalable portals and service access

You offer your customers various account services that utilize DNS, including online billing access and the ability to change their plan and view account activity. DNS Express makes it easy to consolidate these functions inside the BIG-IP platform. The administrator may maintain their own management zone, such as Infoblox, BlueCat, Nominum, or other servers such as BIND or Active Directory. Using F5 as an authoritative DNS server, you can zone transfer to BIG-IP DNS with DNS Express for high-performance DNS responses without affecting your management policies and procedures for zone management.

Optimize local DNS

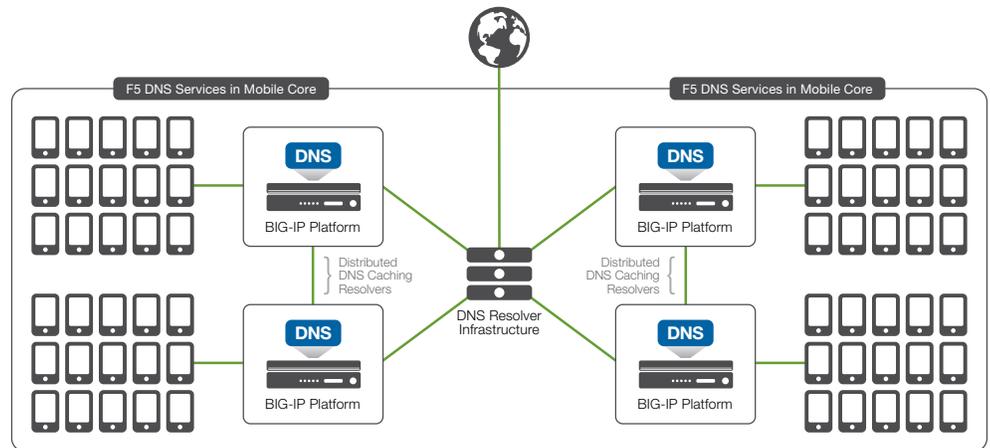
When looking for ways to optimize their DNS deployments, many service providers add more DNS servers to accommodate growth. To manage the increased DNS traffic effectively, they also implement a load balancing solution for maximum performance. F5 BIG-IP DNS with DNS Services and traffic management solutions help manage increased DNS traffic, as well as replace any firewalls and combine security and DNS services to reduce CapEx and OpEx. An integrated, scalable, and secure solution enables DNS optimization by efficiently routing network traffic to the optimal DNS service, which increases response reliability.



Service providers can move from one DNS to multiple DNS servers, while exposing a single IP. BIG-IP DNS also allows you to replace your firewall and combine functions, thus reducing CapEx and OpEx.

Transparent cache

With BIG-IP DNS, transparent caching offloads the LDNS resolver servers through a large cache for DNS optimization. Subscribers will now only ever reach the DNS resolver server if the DNS request they are making has expired or is for a name that has not been requested before. This high-performance cache allows existing DNS resolver servers to scale further as they are receiving fewer requests. This low-impact implementation means that the subscriber and server are unchanged in behavior, while the scalability of DNS increases, enabling more effective optimization.

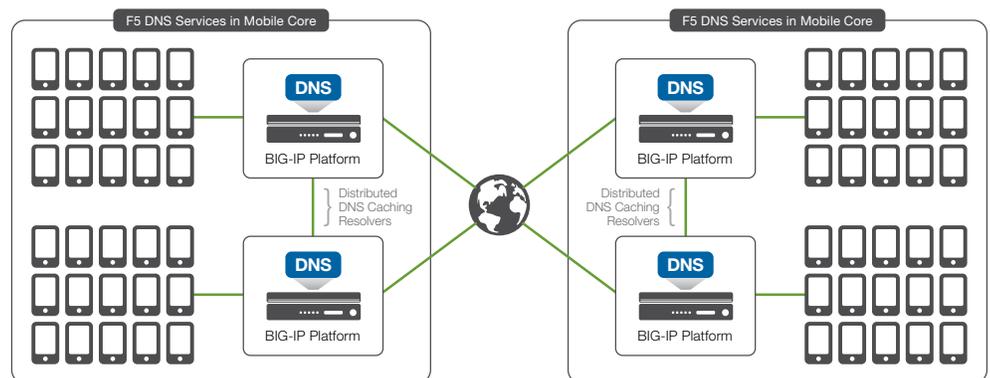


To decrease DNS latency and to offload DNS resolvers, service providers implement BIG-IP DNS with DNS caching close to the subscriber, and scale transparent caches as demand increases to ensure service availability.

BIG-IP DNS consolidates the cache and increases the cache hit rate. This dramatically decreases DNS latency by up to 80 percent, with DNS caching reducing the number of DNS queries for the same site within a short period of time. When used in hardware on the F5 VIPRION® platform, DNS caching hyperscales for ultimate query response performance. And, of course, this is combined with load balancing to the DNS servers on a purpose-designed ICSA-certified network firewall, consolidating resources while increasing security.

DNS caching and resolving

In addition to the DNS caching described above, adding resolver functions to BIG-IP DNS allows the device to do its own DNS resolving without requiring the use of an upstream DNS resolver. When you use BIG-IP DNS, there is no need for additional DNS resolver farms, and any prior LDNS devices are eliminated, leading to consolidation of DNS servers and a high ROI. This also simplifies management and delivers a complete view of DNS infrastructure. For example, you could deploy caching and resolving with the ability to co-locate the authoritative server using DNS Express for the zone that you own, enabling a consolidated and high-performance DNS solution.



With caching and resolving, BIG-IP DNS reduces the average DNS response time for mobile devices from an average of 300 milliseconds to as low as 15 milliseconds, and completes any DNS resolving required, consolidating services for lower CapEx and OpEx.

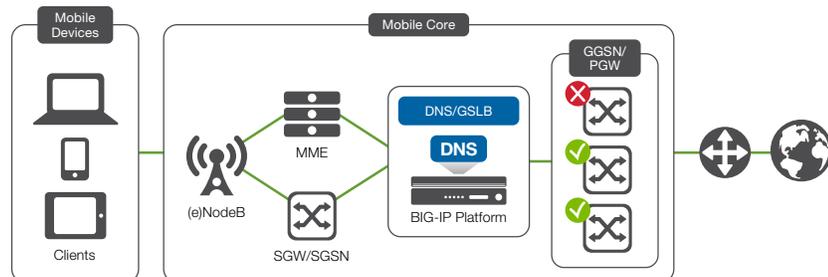
Caching profiles available to select for multiple caches include:

- Transparent cache
- Hot cache
- Caching resolver
- BIG-IP DNS in between client and DNS internal/external
- No cache response so that BIG-IP DNS sends out the request with the response coming back for resolving and caching
- Validating caching resolver so that BIG-IP DNS supports all common DNS deployments that are either authoritative or local resolver DNS

BIG-IP DNS supports all common DNS deployments that are either authoritative or local resolver DNS. Specific zone requests not cached are forwarded to name servers for faster DNS resolving, allowing users to receive expedient responses.

Gateway selection for service high availability

By using DNS and global server load balancing (GSLB) services for infrastructure deployments in the mobile core when subscribers need high-speed access to billing, support, and Internet services, you can realize additional value from BIG-IP DNS. With customizable monitors, you can use the GSLB function to allocate the best resources to DNS queries and respond with the best service experience. For example, the gateway selection process can be optimized by automatically monitoring the packet gateway devices and only providing answers to the DNS queries for gateways that are active and available. BIG-IP DNS adds real-time intelligence to the gateway GPRS support node (GGSN) and packet gateway selection process, which is critical for service delivery. In addition, you can automate service availability using GSLB intelligence with NAPTR and SRV records for optimal subscriber experience. BIG-IP DNS distributes the load intelligently across available GGSN and packet gateways, ensuring that the subscriber experience is optimal at all times.



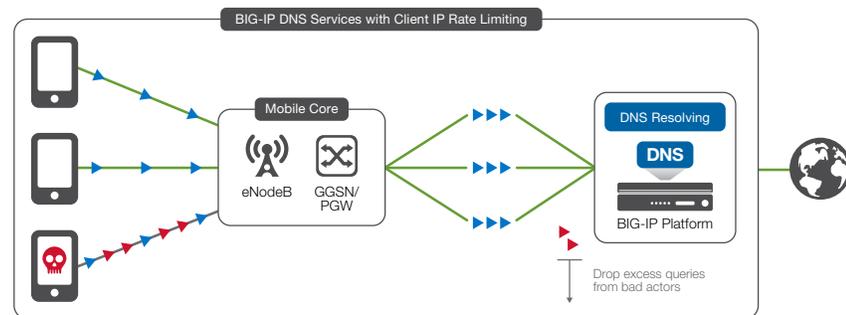
BIG-IP DNS automatically monitors each GGSN and packet gateway using the GSLB engine, and intelligently replies to DNS queries for the subscriber's Access Point Name (APN) with the most available GGSN/PGW for optimal service delivery.

Proactive DNS traffic management with DNS rate shaping

Service providers can proactively manage DNS traffic to ensure that the traffic patterns match the service levels for which the subscriber has opted. For example, a customer may have a 4G LTE service, which means, for typical usage, their DNS query rate should not exceed 200 responses per second (RPS). Using BIG-IP DNS with DNS Services and

a DNS iRule, the client IP rate can be shaped and DNS queries dropped or DNS service suspended should a subscriber be in breach of their permitted rate.

The reason administrators should consider such solutions is that they prevent situations where malware or bad actors affect service and disrupt service to other subscribers. Furthermore, with the sophistication of DNS-based DDoS attacks, these solutions prevent your infrastructure from being used as a significant contributor to such attacks.



Subscribers in your network can disrupt the DNS infrastructure with malicious behavior and unintentional DNS requests through bots and malware. Protect critical infrastructure from abuse with DNS Client IP rate limiting in BIG-IP DNS and ensure service availability for all subscribers.

DNS firewall

DNS DDoS, cache poisoning of LDNS, and other unwanted DNS attacks and volume spikes can cause DNS outage and lost availability. BIG-IP DNS delivers security, scale, performance, and control functionality that shields your DNS infrastructure from attacks and other undesired DNS queries as well as responses that reduce DNS performance.

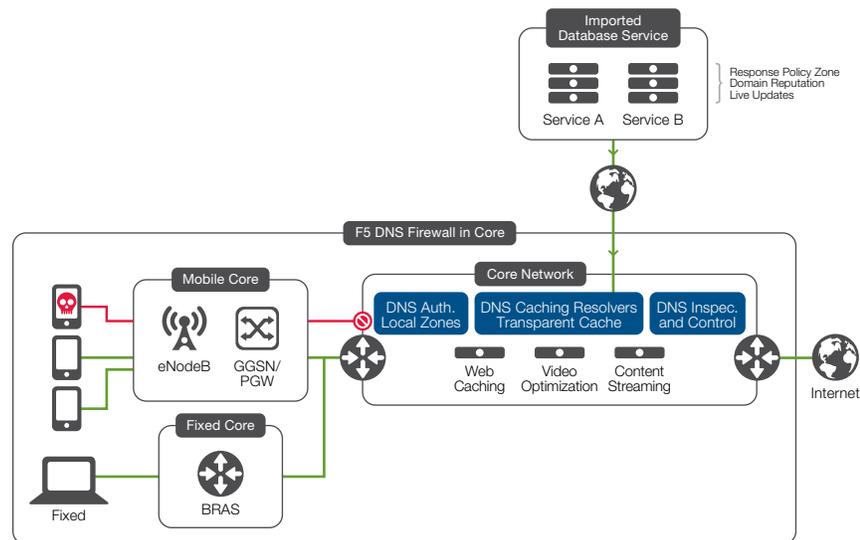
F5 DNS firewall services include:

- Protocol inspection and validation (in software or hyperscaled in hardware)
- DNS record type ACL*
- High-performance authoritative DNS scales responses, mitigating DDoS attacks
- DNS load balancing
- High-performance DNS cache (in software or hyperscaled in hardware)
- Stateful inspection (never accepts unsolicited responses)
- ICSA certified (can be deployed in the DMZ)
- Ability to scale across devices using IP Anycast
- Secure responses (DNSSEC signing)
- DNSSEC response rate limits
- Complete DNS control using DNS iRules
- DDoS threshold alerting*
- Threat mitigation by blocking access to malicious IP domains
- DNS logging and reporting
- Hardened F5 DNS code (not BIND protocol)

*Requires provisioning BIG-IP® Advanced Firewall Manager™ to access functionality.

In addition, you can mitigate complex DNS security threats by blocking access to malicious IP domains with Response Policy Zones. With BIG-IP DNS, you can install a third-party domain filtering service such as SURBL or Spamhaus—preventing client infection or intercepting infected responses to known sources of malware and viruses.

BIG-IP DNS offers built-in protocol validation in software to automatically drop high-volume UDP, DNS query, NXDOMAIN floods, and malformed packets. You can also use BIG-IP DNS in hardware to mitigate these high-volume attacks. F5 DNS firewall services reduce the costs of infection resolution and increase user productivity.



BIG-IP DNS with DNS firewall services lowers your risk of malware and virus communication and mitigates DNS threats by blocking access to malicious IP domains with a domain reputation service such as SURBL or Spamhaus.

DNSSEC signing

With BIG-IP DNS and DNSSEC real-time signing support server side, you can digitally sign and encrypt your DNS query responses. This enables the client-side resolver to determine the authenticity of the response, preventing DNS hijacking and cache poisoning of the LDNS. These signed DNS responses are used in conjunction with the BIG-IP intelligent DNS system so you receive all the benefits of global server load balancing while also securing your DNS query responses.

Centralized DNSSEC key management

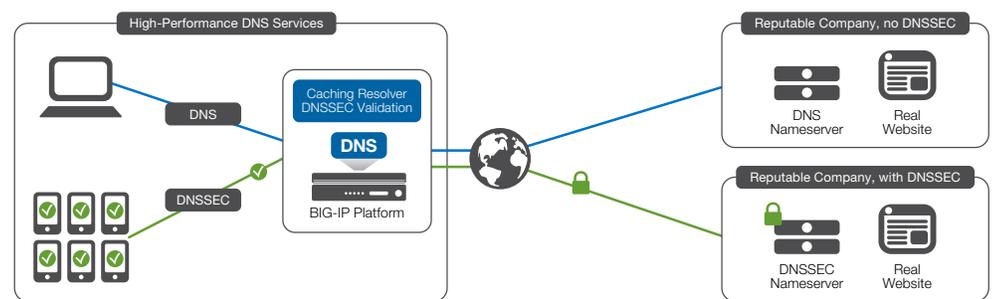
Many IT organizations have or want to standardize on FIPS-compliant devices and secure DNSSEC keys. You can use BIG-IP DNS with FIPS cards that provide 140-2 support for securing your keys. In addition, BIG-IP DNS integrates and uses hardware security modules (HSMs) from Thales for implementation, centralized management, and secure handling of DNSSEC keys, delivering lower OpEx, consolidation, and FIPS compliance. DNSSEC capabilities are now included with many of the latest platforms for fast implementation with Thales HSMs.

Top-level domain support for DNSSEC

For DNS administrators who want to delegate to other secure sub-domains, BIG-IP DNS allows easy management of DNSSEC as a top-level domain, becoming a parent zone.

DNSSEC validation

In most service provider networks, DNS resolvers manage DNSSEC record requests and crypto calculations to validate that the DNS response being received is correctly signed. DNSSEC responses coming into the network requires high CPU loads on DNS resolving servers. With BIG-IP DNS and DNSSEC validation, administrators can easily offload and validate DNSSEC on the client side using BIG-IP DNS for resolving. This results in superior DNS performance and a dramatic increase in the site response to subscribers.



With DNSSEC validation, administrators easily offload and validate DNSSEC on the client side using BIG-IP DNS for resolving. This results in superior DNS performance and a dramatic increase in the site response to subscribers.

Simple Management and Programmability

Managing your network from a single point is an enormous challenge. BIG-IP DNS provides tools that give you a global view of your infrastructure along with the means to manage the network and add policies to ensure the highest availability for your business-critical services.

iRules

Using F5's event-driven iRules, you can customize the dynamic distribution of global traffic. BIG-IP DNS looks deep inside packets to distribute application traffic to the desired data center, pool, or virtual server. This capability reduces latency, increases protection against malicious attacks, and improves service delivery for subscribers. Because iRules is based on an easy-to-use, TCL-based scripting language, administrative costs are nominal.

DNS iRules

You can easily manage DNS queries, responses, and actions for a fast, customized DNS infrastructure using DNS iRules. For instance, you can configure DNS iRules with filtering capabilities by using packet filters and query logging to enable protection and reporting of DNS. Because BIG-IP DNS can configure DNS iRules to manipulate DNS packets, administrators can add commands enabling dynamic DNS query and response management.

Customize traffic with QoS

Your DNS administrators can easily develop custom load balancing algorithms using quality of service (QoS) metrics in iRules. These allow you to use round-trip time, hops, hit ratio,

packet rate, bits per second, virtual server capacity, topology, virtual server score, and link capacity to specify unique and customized traffic requirements.

ZoneRunner

F5 ZoneRunner™ in BIG-IP DNS is an integrated zone file management tool that simplifies DNS zone file management and reduces the risk of misconfiguration. It provides a secure environment in which to manage your DNS infrastructure while validating and error-checking zone files.

Built on the latest version of BIND, ZoneRunner provides:

- Auto population of commonly used protocols
- Validation/error checking for zone file entries
- Rollback for the last transaction
- Command line versions of zone management
- Zone importation from an external server or a file
- Automatic reverse lookups
- Easy creation, editing, and searching of all records
- Easy management of Name Authority Pointer (NAPTR) records for LTE and 4G requirements

DNS health monitor

BIG-IP DNS deployed inline easily manages and load balances DNS servers. The DNS health monitor available in BIG-IP DNS and BIG-IP® Local Traffic Manager™ (LTM) monitors DNS server health and helps configure DNS based on reporting. The DNS health monitor detects whether the servers are operating at peak performance and helps reconfigure them for optimal responses. For example, when monitoring DNS responses, BIG-IP DNS receives a valid response from the DNS server sending an outbound query response. Or, in another example, if no devices answer a DNS request, the DNS monitor will check the path to see if the DNS infrastructure is working.

High-speed logging

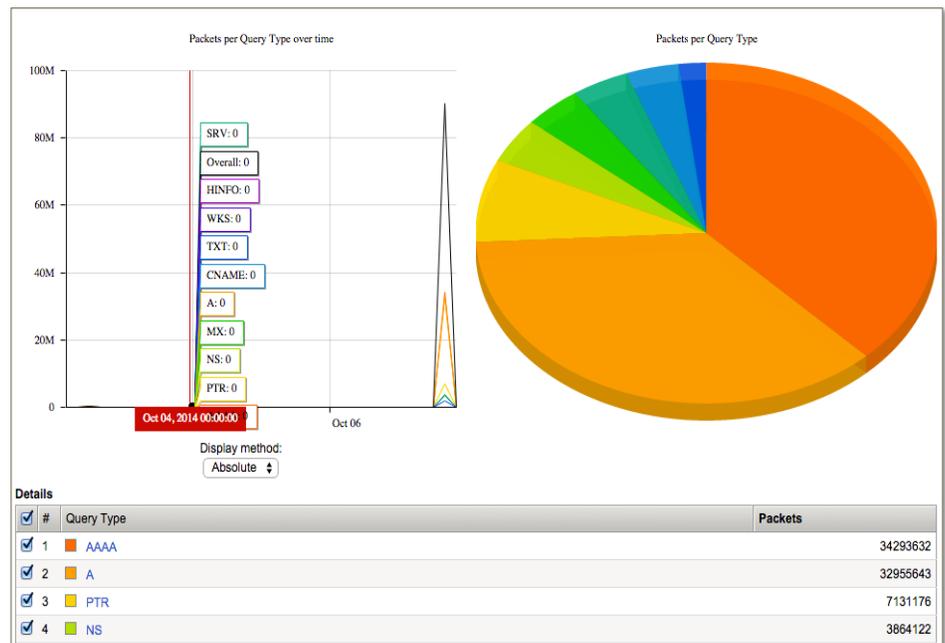
You can easily manage DNS and global application logging for fast network visibility and planning. By improving data information with high-speed logging of DNS queries and responses, syslog, and GSLB decision logs, high-speed logging enables fast network recognition with quick, deep search and display. For key network critical functions, there is centralized data recognition of all logs for destinations, formats, alerts, and more.

Enhanced DNS detailed statistics

BIG-IP DNS delivers advanced DNS statistics with detailed data for profiles such as query type counts (A, CNAME, NS, RRSIG, AAAA, SRV, and other types), along with requests, responses, and percentage counts. Statistics are per profile and per device global count for fast visibility and planning of DNS delivery infrastructure. You can view DNS detail statistics in DNS profile or in analytics reporting. GUI statistics show rated capacity of instances such as query RPS and object limits for DNS, delivering reporting such as A requests, AAAA requests, and DNS resolutions for use in capacity planning for DNS. On viewing current statistics, administrators can choose to purchase more capacity to deploy the exact capability they require.

Advanced DNS reporting and analytics

F5 Analytics provides advanced DNS reporting and analysis of applications, virtual servers, query names, query types, client IPs, top requested names, and more for business intelligence, capacity planning, ROI reporting, troubleshooting, performance metrics, and tuning, enabling maximum optimization of the DNS and global app infrastructure. Thresholds can be set for some of the statistics, and an alert can be delivered via syslog, SNMP, or email when the threshold is exceeded. You can export the data off-box to a third-party remote logging/reporting engine for enhanced analysis.



Service providers can easily manage DNS using analytics with advanced reporting and analysis of actions for fast visibility of DNS delivery and infrastructure.

Enterprise Manager

F5 Enterprise Manager™ can help you significantly reduce the cost and complexity of managing multiple F5 devices. You get a single-pane view of your entire application delivery infrastructure and the tools you need to reduce deployment times, eliminate redundant tasks, and efficiently scale your infrastructure to meet your business needs.

Network Integration

BIG-IP DNS is designed to fit into your current network as well as your plans for the future.

SNMP management application support

BIG-IP DNS integrates its Management Information Bases (MIBs) and an SNMP agent with DNS. This enables SNMP management applications to read statistical data about the current performance of BIG-IP DNS. SNMP management packages have an exact view of what BIG-IP DNS is doing, while keeping an eye on standard DNS information.

Third-party integration

BIG-IP DNS communicates and integrates with a broad array of network devices. This includes support for various types of remote hosts, including SNMP agents: UCD, snmpd, Solstice Enterprise, and the NT/4.0 SNMP agent. BIG-IP DNS also interacts with third-party caches, servers, routers, and load balancers to accurately diagnose the health of your network endpoints and provide a heterogeneous solution for global traffic management.

IPv6/IPv4 support

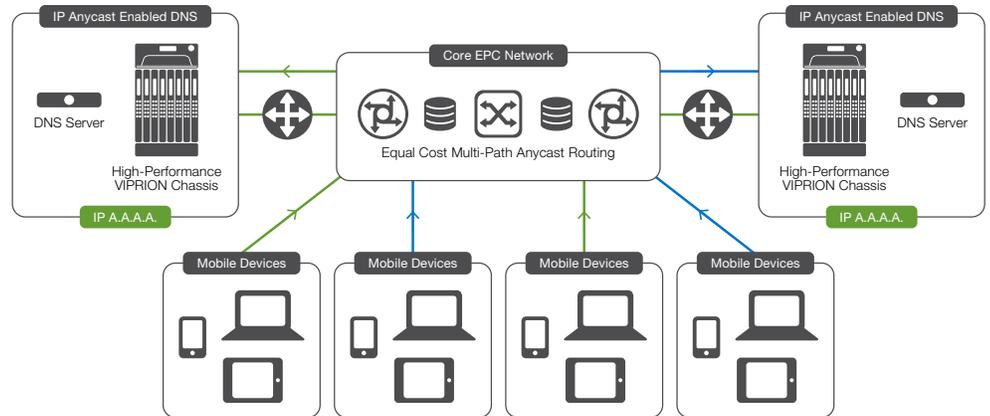
BIG-IP DNS supports next-generation IPv6 networks, resolving AAAA queries without requiring wholesale network and application upgrades. As IPv6 adoption grows, BIG-IP DNS eases the transition to IPv6 by bridging the gap between IPv6/IPv4 DNS. The DNS translation between IPv6 and IPv4 networks is seamless as BIG-IP DNS provides DNS gateway and translation services for hybrid IPv6 and IPv4 solutions, and manages IPv6 and IPv4 DNS servers in DNS64 environments. For AAAA queries from clients, BIG-IP® Carrier-Grade NAT (CGNAT) configured with NAT64 transforms IPv6 to IPv4 for those IPv4-only environments. The response data is sent to the client from NAT64 using IPv6. BIG-IP DNS enables the customer to run pure internal IPv6 and maintain connectivity to the IPv6/IPv4 Internet.

IP Anycast integration

BIG-IP DNS and IP Anycast integration increases DNS performance as more devices are added to support millions of DNS queries. DNS query volumes directed to one IP address—whether legitimate or during a DoS attack—are easily managed by distributing the load among multiple geographic BIG-IP DNS devices with an IP Anycast integration. You can scale DNS infrastructure up and out to manage DNS request load to one IP, increasing revenue by servicing more users and protecting your brand with trustworthy query response.

Network managers realize these benefits:

- Improved user performance and reliability
- Reduced network latency for DNS transactions
- Fewer queries routed to distant servers
- Lower rates of dropped query packets, reducing DNS timeouts/retries
- Fewer congested routers



BIG-IP DNS and IP Anycast integration distributes the DNS request load by directing single IP requests to multiple local devices.

DNS and GSLB services in virtual and cloud environments

Easily spin up new deployments of global server load balancing with BIG-IP DNS Virtual Edition (VE) standalone or BIG-IP DNS running on BIG-IP LTM VE. Provide flexible global application availability by routing users to applications in data centers, managing Internet Software as a Service (SaaS) and outsourced applications, or directing users to the most available cloud applications.

Architecture

The advanced architecture of BIG-IP DNS gives you total flexibility to control application delivery without creating traffic bottlenecks.

TMOS

At the heart of BIG-IP DNS is the F5 operating system, TMOS®, which provides a unified system for optimal application delivery, giving you total visibility, flexibility, and control across all services. TMOS empowers BIG-IP DNS to integrate with other F5 products and intelligently adapt to the diverse and evolving requirements of applications and networks.

Query and response performance and scalability

BIG-IP DNS query and response performance scales linearly on larger platforms and increases performance by integrating functions in TMOS. BIG-IP DNS is provisionable for platforms that support F5 Virtual Clustered Multiprocessing™ (vCMP).

ScaleN technology

Instead of adding more DNS servers and firewalls to scale and protect your infrastructure, consider consolidating DNS delivery into one intelligent services framework. With high-performance F5 ScaleN™ appliance technology, you get the robust capabilities required to enable multi-tenant solutions, elastic applications, and infrastructure for any environment. Just select one platform for high-performance DNS delivery management and add capacity as needed without growing overhead. With optimized and secure DNS services from F5, you can focus on monetizing subscribers and reducing subscriber churn with higher data usages, faster web browsing, and better QoE.

BIG-IP DNS Platforms

F5 Software-Defined Application Services™ are delivered via both hardware and software to flexibly support your specific environments—physical, virtualized, or cloud.

Hardware includes BIG-IP appliances or the F5 VIPRION® modular chassis and blade system designed specifically for application delivery, security, and high performance. VIPRION uses [ScaleN](#) technologies to provide on-demand linear scalability by enabling you to add blades without re-configuration. BIG-IP® virtual edition (VE) software runs on commodity servers and provides agility and fast deployment of services in cloud environments. See the [BIG-IP System Hardware](#), [VIPRION](#), and [Virtual Edition](#) data sheets for details. For information about specific module support for each platform, see the latest release notes on [AskF5](#). For the full list of supported hypervisors, refer to the [VE Supported Hypervisors Matrix](#).

F5 solutions can be centrally managed through [F5 BIG-IQ®](#), an intelligent platform for managing and orchestrating F5 devices and the services they deliver.



BIG-IP Appliance



VIPRION Chassis



Virtual Edition

DNS on-demand scaling

Administrators have the option to add DNS and GSLB on-demand scaling with rate-limit and object-limit capacity to BIG-IP DNS or LTM appliances. This option supports requirements for exact traffic performance, resulting in lower CapEx and OpEx. On-demand scaling includes the following services: DNS, GSLB, and DNSSEC. User interface statistics show rated capacity of instances, such as query RPS and object limits, which deliver fast traffic detail for easy capacity planning. Contact your regional F5 sales representative or reseller for more information.

DNS Query RPS Maximum Performance

BIG-IP DNS delivers DNS query response per second (RPS) with high-performance scalability. The table below lists many BIG-IP platforms with DNS Express enabled for authoritative DNS query response with maximum capabilities per platform.

Platform	Max Query RPS
Virtual Edition	250,000*
2000s	210,000
2200s	350,000
4000s	420,000
4200v	720,000
5050s	760,000
5250v	1,300,000
7050s/7055s	770,000
7200v/7250v/7255v	1,400,000
10050s/10055s	1,100,000
10200v/10250v/10255v	1,800,000
11050(N)	2,200,000
VIPRION 2200 Full Chassis (2 blades) VIPRION 2400 Full Chassis (4 blades)	
VIPRION B2150 Blade	790,000
VIPRION B2250 Blade	2,100,000
VIPRION 4480 Full Chassis (4 blades) VIPRION 4800 Full Chassis (8 blades)	
VIPRION B4300 Blade	2,200,000

*Virtual Edition is available in increments of 250,000 RPS.

For 5050s and above, Rapid Response Mode (RRM—see page 3) delivers up to 200 percent of normal max query RPS when turned on. [See F5 Sales or Reseller for details.](#)

F5 Global Services

F5 Global Services offers world-class support, training, and consulting to help you get the most from your F5 investment. Whether it's providing fast answers to questions, training internal teams, or handling entire implementations from design to deployment, F5 Global Services can help you achieve IT agility. For more information about F5 Global Services, contact consulting@f5.com or visit f5.com/support.

More Information

To learn more about DNS Solutions and BIG-IP DNS, use the search function on f5.com to find these and other resources.

Blog

[Mitigating Unwanted Communication on Your Service Network](#)

[F5 Intelligent DNS - Optimizing the Mobile Core](#)

Data sheets

[BIG-IP System Hardware Data Sheet](#)

[BIG-IP Virtual Editions Data Sheet](#)

[VIPRIION Chassis Hardware Data Sheet](#)

Solution profiles

[Scaling DNS Services with BIG-IP DNS](#)

Reference architecture

[Intelligent DNS For Service Provider Reference Architecture](#)

White papers

[The Dynamic DNS Infrastructure](#)

[Mitigating DDoS Attacks with F5 Technology](#)

Video

[Intelligent DNS for the Evolved Packet Core](#)

[Threats to Mobile Carrier Networks](#)

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

Americas
info@f5.com

Asia-Pacific
apacinfo@f5.com

Europe/Middle-East/Africa
emeainfo@f5.com

Japan
f5j-info@f5.com

Solutions for
an application world.

