Guide

The F5 Handbook for Service Providers

VERSION 2, REVISED 2018

Table of Contents

Optimize, Secure, and Monetize Your Network

Mobile consumers are growing accustomed to anytime/anywhere access to resource-intensive content, such as streaming video and high-bandwidth applications from their mobile devices. Mass-market consumption of smartphones and other connected mobile devices, along with advanced 4G LTE network deployments, have led to massive and sustained growth in data usage. As a result, operating costs are rising while average revenue per user (ARPU) has trended flat to negative.

To remain profitable, service providers must find new ways to support increased demands on their networks with more efficient resource utilization, while maintaining the ability to support rapid rollout of new revenue-generating services.

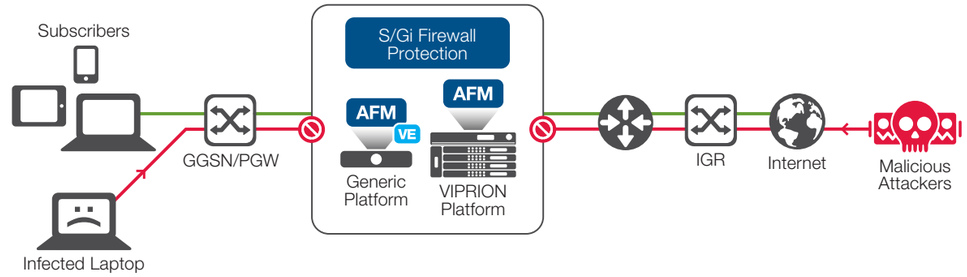
F5 offers solutions for fixed and mobile service providers to achieve maximum optimization, security, and monetization of their networks. The sections on the following pages feature use cases that illustrate how you can maintain top network performance and profitability.

SECURITY SOLUTIONS

S/Gi Firewall

THE CHALLENGE

As mobile network operators and other service providers migrate to all-IP-based networks, such as 4G LTE, network intrusions and attacks are far more likely to occur. Service providers must constantly defend against security threats to ensure the availability of their most precious resource—the network. This increases costs and operational complexity, while having a negative effect on both network performance and subscriber experience.



A high-performance, full-proxy firewall protects your core infrastructure.

THE SOLUTION

F5® BIG-IP® Advanced Firewall Manager™ (AFM) defends mobility infrastructure and mobile subscribers from attacks, regardless of their source. This includes mitigation of large-scale DDoS attacks such as network floods, port scans and sweeps, or connection floods. By detecting and stopping these types of attacks, BIG-IP AFM can prevent congestion and overloading of the control and bearer planes of the radio access network. BIG-IP AFM protection against DDoS attack vectors continues to increase with each version released and with many BIG-IP platforms, DDoS protection functions are accelerated using specialized hardware. Furthermore, Gi Firewall supports CGNAT with NAT44 and NAT64.

As an ICSA Labs Certified firewall solution, BIG-IP AFM offers the protection of a full-proxy firewall, fully terminating and inspecting incoming client connections for threats, ensuring network availability and an improved subscriber experience.

F5 HELPS YOU:

- Protect the core infrastructure with a high-performance, highly scalable firewall.
- Defend against DDoS attacks across all layers.
- Transition from IPv4 to IPv6 with NAT44, NAT64, 464XLAT.

SECURITY SOLUTIONS

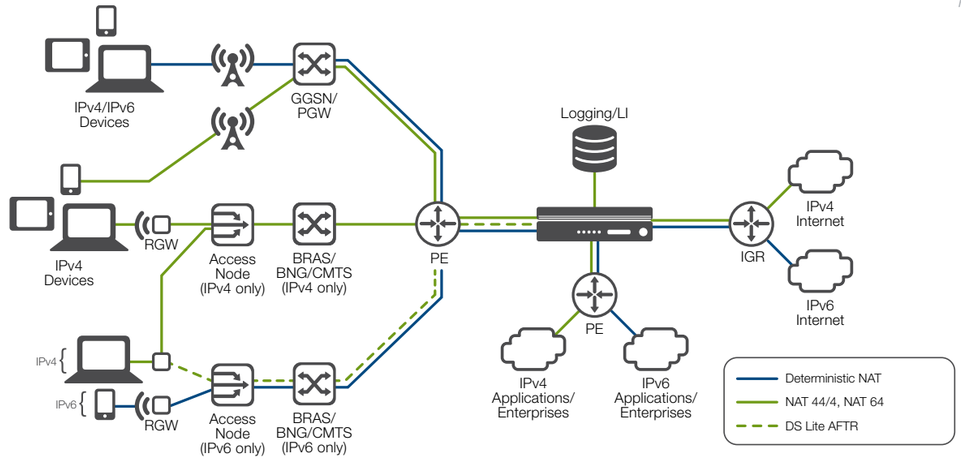
Carrier-Grade NAT

THE CHALLENGE

Worldwide proliferation of wireless and Internet-enabled devices has rapidly depleted IPv4 addresses. Asia, Europe, North America, and Latin America have already exhausted their IPv4 allotments, and Africa is expected to exhaust its allotment by the end of 2018. 61 percent of all fixed and mobile network devices will be IPv6-capable by 2021, up from 30 percent in 2016 (The Zettabyte Era: Trends and Analysis, Cisco June 2017).

Service Providers are being challenged to support and manage existing IPv4 devices and content in the network while they transition to support newer IPv6 devices and applications. And because IPv6 devices and content are not backward compatible with IPv4, any IPv6 migration strategy needs to support the coexistence of IPv4 and IPv6 during transition.

5G READY



Ensure seamless connectivity and a smooth migration to IPv6 with BIG-IP CGNAT.

THE SOLUTION

F5 BIG-IP Carrier-Grade NAT (CGNAT) offers a broad set of high-performance, highly scalable tools that enable service providers to successfully migrate to IPv6 while continuing to support and interoperate with IPv4 devices and content. In addition, BIG-IP CGNAT provides extensive, flexible, high-speed logging capabilities along with support for IPFIX, which compresses NAT logging, therefore reducing the amount of data per log entry and minimizing overall costs.

With tunneling solutions, including Dual-Stack Lite (DS Lite) capabilities, BIG-IP CGNAT supports legacy IPv4 endpoints in the IPv6 network. DS Lite capabilities consist of endpoint IPv4 packets being encapsulated in an IPv6 tunnel and sent to an external IPv4 destination through the network. Another tunneling service, called IPv6 rapid deployment (6rd), enables networks on IPv4 to communicate with IPv6 addresses without upgrading hardware.

BIG-IP CGNAT also provides network address translation (NAT) functionality, enabling continued delivery of IPv4 connectivity while handling high numbers of concurrent sessions as service providers manage IPv4 address depletion and plan for a seamless migration to IPv6. NAT functionality includes NAT44, to primarily focus on extending the use of IPv4 addresses in the network, as well as NAT64, enabling IPv6 endpoints to seamlessly and transparently access IPv4 content and destinations. BIG-IP CGNAT also supports DNS64, which uses DNS AAAA records so IPv6 hosts can see IPv4 destinations as IPv6 addresses.

F5 HELPS YOU:

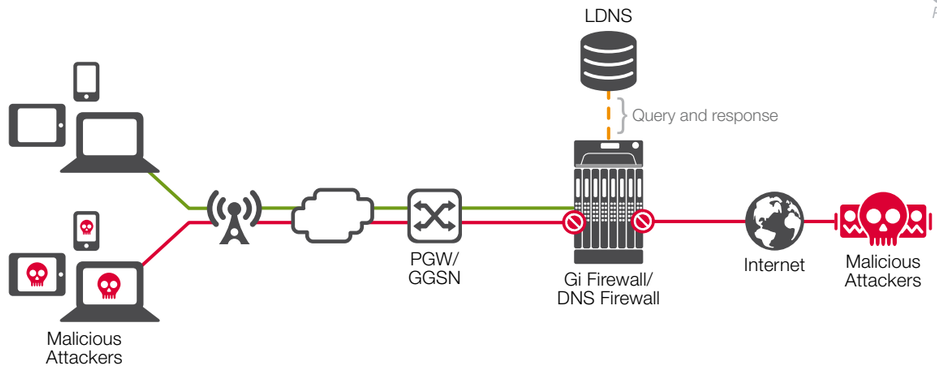
- Manage address depletion and IPv6 migration with flexible deployment options.
- Optimize the network with carrier-grade performance and scalability.
- Reduce server quantities and management costs.

SECURITY SOLUTIONS

Secure DNS

THE CHALLENGE

Service providers are tasked with delivering highly secure, scalable, and available Domain Name System (DNS) services to an exponentially growing number of devices, driven by mobile and IoT. They rely on DNS to enable subscriber access to critical services and web applications. But if DNS is unavailable, services will fail to function properly, leading to network and service degradation or failures. And while service providers need to optimize and secure the DNS infrastructure to best serve mobile users, such an infrastructure requires a tremendous amount of real-time management and stability. Scaling DNS rapidly becomes critical when dealing with millions of service names and IP addresses. As service providers scale their control planes, they also need the capacity and control to withstand attacks such as DNS DDoS attacks, DNS reflection and amplification attacks, DNS water torture attacks, and DNS tunneling for circumventing service limits.



BIG-IP DNS protects the network and mitigates DDoS attacks while providing hyper-scale DNS services.

THE SOLUTION

F5 BIG-IP DNS helps Service Providers optimize, secure, and monetize their DNS infrastructures. The solution provides carrier-grade, high-performance LDNS caching and resolving, and is a hyper-scale authoritative DNS solution with DNS firewall security services for mitigating DNS DDoS attacks. BIG-IP DNS delivers an intelligent and scalable DNS infrastructure for faster access and service response for mobile users. In addition, it can load balance local and recursive DNS services. Service providers use customizable monitors and global server load balancing (GSLB) services to allocate the best resources to DNS queries and respond with the best service experience. BIG-IP DNS also enables a DNS64 environment, creating a fault tolerant architecture—optimizing network traffic and increasing quality of experience (QoE) for users, thus protecting service providers' brands.

In addition, it shields the DNS infrastructure from malicious attacks via infected subscribers and from undesired DNS queries and responses that reduce DNS and service performance. The F5 intelligent DNS firewall inspects and validates protocols while dropping invalid requests or refusing to accept unsolicited responses. BIG-IP DNS is an ICSA Labs Certified network firewall with DDoS threshold alerting that hyper-scales across many devices using IP Anycast for DDoS absorption. It mitigates threats by blocking access to malicious IP domains.

BIG-IP DNS also offers enhanced, detailed statistics with high-speed DNS logging and reporting, along with advanced analytics and performance metrics to deliver business intelligence for service and capacity planning, optimization, and monetization, as well as security troubleshooting.

F5 HELPS YOU:

- Optimize DNS infrastructure and hyper-scale service delivery.
- Monetize with improved network performance and lower churn.
- Secure your network and mitigate DNS attacks and circumvention.
- Ensure service experience and extend service availability.

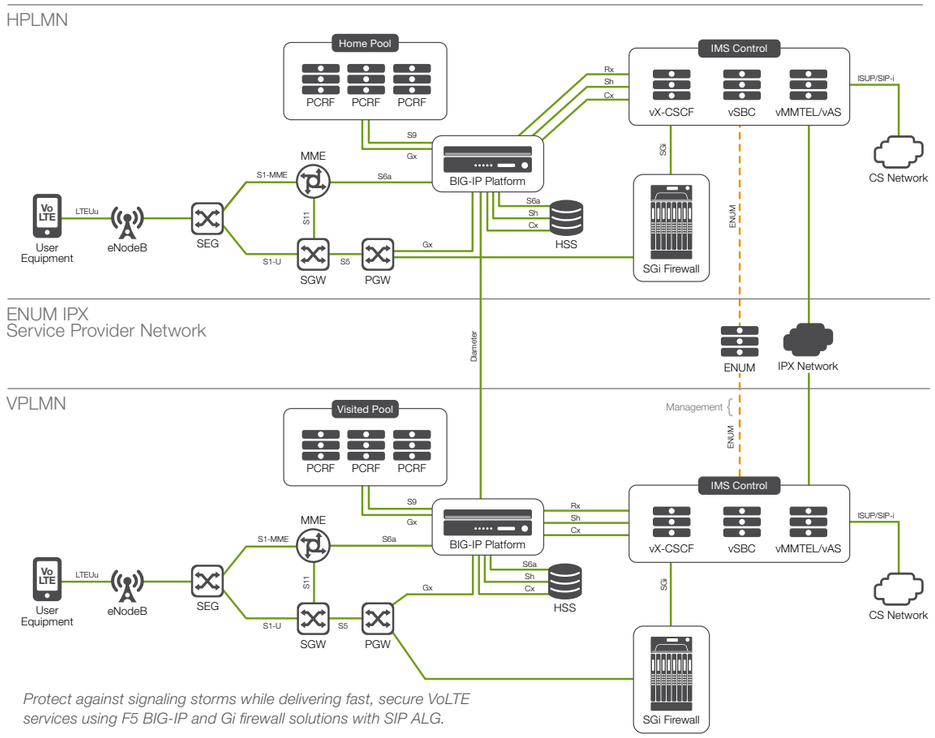
SECURITY SOLUTIONS

VoLTE and IMS Security

THE CHALLENGE

VoLTE is crucial for service providers, consolidating voice traffic from circuit switch networks to all-IP LTE networks, thereby reducing overall network operation costs. As the rate of VoLTE adoption rapidly increases, attacks against the signaling resources used to provide services—including real-time signaling protocols—will also increase. As a result, VoLTE security which focuses on protecting and controlling signaling protocols, including Diameter and SIP, is becoming more critical.

With more and more devices coming to market with support only for IPv6, the ability to manage and control potential signaling spikes caused by these IPv6 devices is equally important. When a SIP signaling storm occurs due to unintended actions, other node outages in the network, or malicious attacks, it is important to rate-limit SIP requests to the P-CSCF so it is not overwhelmed. Plus, the increase in the types and numbers of new devices means massive and continued changes in traffic and usage characteristics. To handle all these changes, operators will require solutions capable of very high connection rates and increasing concurrency.



Protect against signaling storms while delivering fast, secure VoLTE services using F5 BIG-IP and Gi firewall solutions with SIP ALG.

THE SOLUTION

The BIG-IP platform helps ensure VoLTE service continuity and protects against unauthorized access, unexpected traffic peaks, signaling storms, session spoofing, and privacy attacks.

The F5 firewall solution with SIP ALG capabilities monitors SIP messages and only permits RTP streams when it validates the SIP control channel, providing security for user traffic in the network. By combining firewall, traffic management, DDoS protection, and rich protocol support (SIP, Diameter, HTTP, DNS, and others), the BIP-IP platform can enforce controls on the S/Gi LAN, directly in front of the P-CSCF and other application servers, and on Roaming interconnect points. F5 solutions can secure and distribute traffic, regardless of whether that traffic is from IPv4 or IPv6 devices. By doing so, F5 solutions combine security and availability functionalities to maintain network service during times of unexpected stress. Additionally, these solutions enable service delivery with the highest possible protection, connection rates, and concurrency levels in the industry—more than a terabit of throughput and up to 1.2 billion concurrent connections.

F5 HELPS YOU:

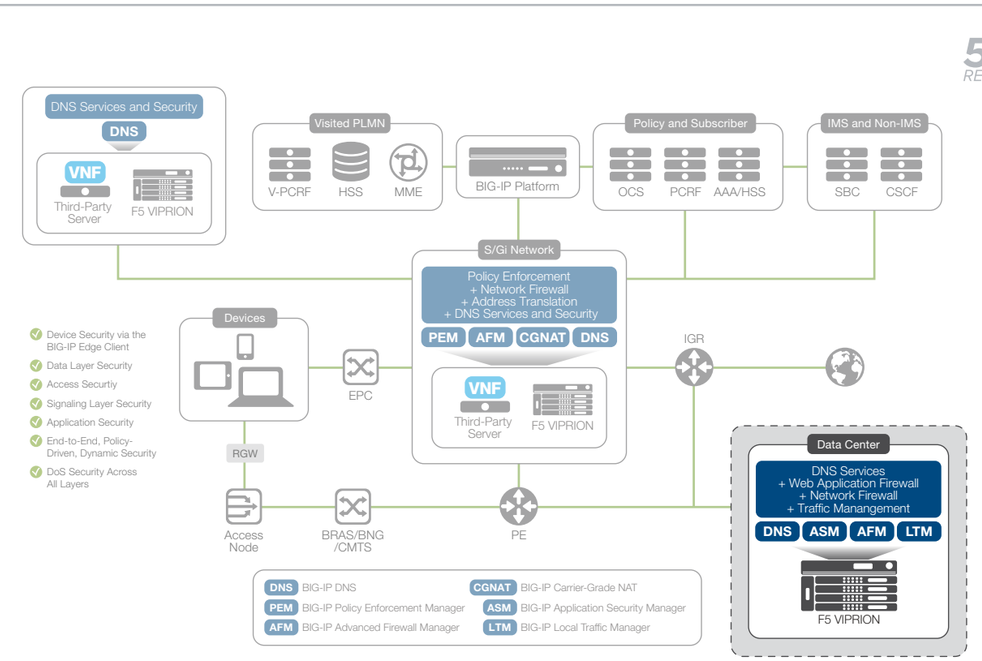
- Deliver fast and secure VoLTE and IMS services.
- Provide the highest possible security protection.
- Support high connection rates and a high level of concurrency.
- Protect the brand and maximize subscriber QoE.

SECURITY SOLUTIONS

Data Center Firewall

THE CHALLENGE

Networks continue to grow to adopt 4G and 5G technologies, rapidly deploy new services based in the data center, and host applications such as video and content streaming. These changes can threaten the quality of service for users, increase capital and operational expenses, and strain the security architecture's ability to handle a rapidly changing threat landscape. Service providers need a way to support network growth while ensuring reliable and scalable security.



F5 solutions deliver comprehensive network protection—from the data center to DNS infrastructures.

THE SOLUTION

F5 delivers a full range of solutions that simplify service providers' security architectures while mitigating threats. The full proxy architecture of F5 solutions also allows service providers to attain extensive visibility and control throughout layers 4 through 7. This enables granular control of all connections, more extensive security functionality, and comprehensive end-to-end protection against DDoS and other attacks. F5 solutions protect targeted network elements, the DNS infrastructure, devices, and applications with features that include application health monitoring, a robust web application firewall, web access controls, TCP optimization, web acceleration, L7 DDoS protection, and broad SSL support, including SSL inspection and offload.

A leading T-1 service provider implemented F5 data center firewall solutions and reduced its hardware footprint by a factor of 20—a big improvement for scalability. Typical data center footprints can be reduced even more dramatically with F5 solutions for securing DNS. Ultimately, these solutions help simplify operations and lower total cost of ownership while securing the network and protecting the service provider's business and brand.

F5 HELPS YOU:

- Rapidly deploy new, revenue-generating services and applications based in the data center.
- Increase connection rates and concurrency.
- Reduce space, power consumption, and TCO.
- Improve quality of service for users.

SECURITY SOLUTIONS

DDoS Mitigation

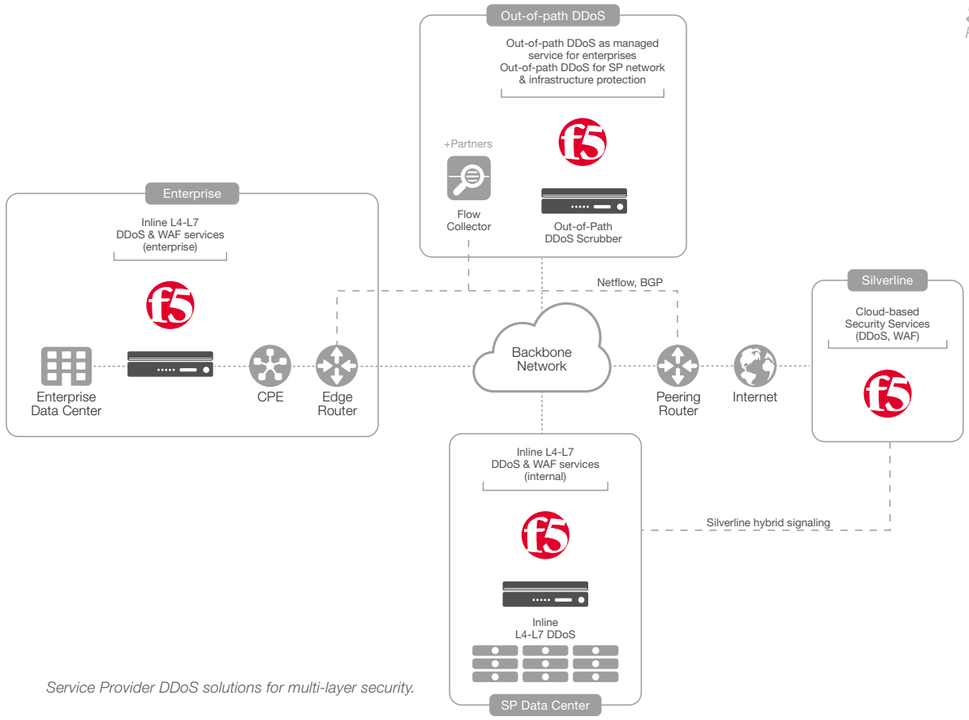
THE CHALLENGE

DDoS attacks range from pranksters having fun to targeted acts of retaliation, protest, theft, and extortion. Depending on their skills, attackers may use readily available DDoS tools or launch customized, sophisticated attacks. Ultimately, all DDoS attacks have one objective: to disrupt service availability and have a significant impact on businesses. Suddenly, applications aren't available and businesses can't connect with customers.

There are four main types of attacks, often used in some combination:

- Volumetric—Flood-based attacks at layer 3, 4, or 7.
- Asymmetric—Invoking timeouts or session-state changes.
- Computational—Consuming CPU and memory.
- Vulnerability-based—Exploiting application software vulnerabilities.

The most damaging DDoS attacks mix volumetric attacks with targeted, application-specific attacks.



Service Provider DDoS solutions for multi-layer security.

THE SOLUTION

Combined or "blended" DDoS attacks are becoming more difficult to defend against and are often an indicator of more advanced, persistent threats to come. Quickly discovering and stopping these threats is key to ensuring service continuity and limiting damage.

F5 offers the most comprehensive layer 3–7 DDoS mitigation, combining on-premises and cloud DDoS scrubbing to mitigate network, application, and volumetric attacks.

F5 HELPS YOU:

- Defend against the full spectrum of DDoS attacks with multi-layered, hybrid defense.
- Support flexible deployment options with inline and out-of-band mode to keep applications available.
- Detect and mitigate targeted multi-vector, bursty DDoS.
- Seamlessly integrate on-premises and native cloud-based protection by signaling F5 Silverline cloud-based scrubbing.

SECURITY SOLUTIONS

GTP Security

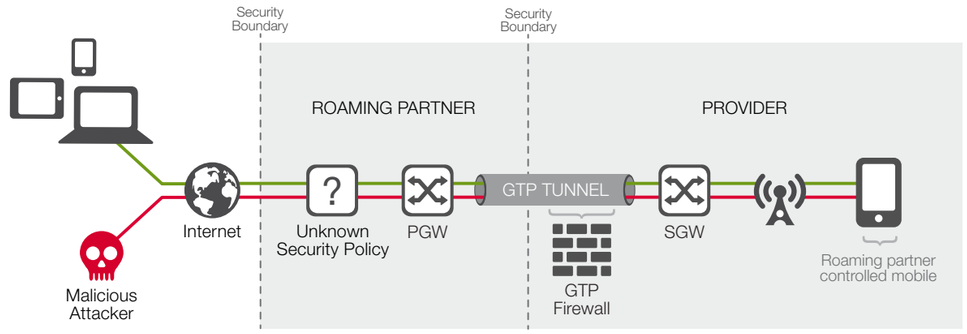
THE CHALLENGE

Highly scalable and secure roaming services depend on the GTP protocol to provide signaling and transport between an increasing number of partners. While many roaming partners implement strong security controls, risks still exist and providers are ultimately responsible for the security of their own infrastructure. Protecting the GTP protocol from abuse and vulnerabilities not only prevents unwanted activity, it ensures roamers have a high quality, predictable experience.

With 4G data roaming increasing, shifts to VoLTE, and fundamental changes in the European Union's roaming regulations, providers are expecting a significant increase in GTP traffic volume. Service providers need to scale and secure the GTP traffic today and prepare to evolve to a 5G network where GTP still plays an important role.

In parallel to the strong increase in GTP traffic, there has been a trend in GSMA to make mobile operators (and related GRX/IPX carriers and other international parties) aware of the GTP security vulnerabilities and how to deal with them. Various protocols have been investigated by GSMA, mainly driven by the GSMA Fraud Security group. These include SS7, Diameter, and GTP. The result of this GSMA activity is an FS.20 document, *GTP Security*, which acts as guideline for GSMA members to be aware of known GTP security issues and how to prevent/resolve them as the native GTP protocol has no strong, built-in security mechanisms.

5G READY



Protect the control and data planes at scale by mitigating the risk from roaming traffic.

THE SOLUTION

F5 offers GTP Security solutions that scale and protect both control and data plane traffic while implementing FS.20 protections on roaming traffic. Protections include the ability to filter many aspects of the GTP control protocol per roaming partner, such as APNs, information elements, and message types. Invalid and malformed messages can be blocked or reported, and tunnels with an unknown TEID can be blocked. Combined with the flexibility and scale that F5 is known for, the GTP Security solution can protect the most demanding service provider roaming infrastructures.

F5 HELPS YOU:

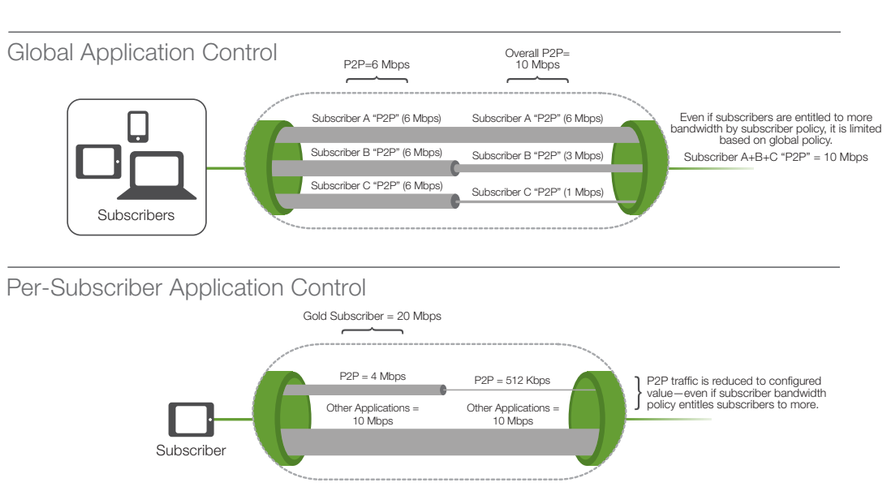
- Scale and protect control and data plane traffic.
- Scale and protect roaming traffic.

DATA TRAFFIC MANAGEMENT SOLUTIONS

Subscriber, Application, and Policy Aware Bandwidth Control

THE CHALLENGE

During peak times, heavily congested broadband networks can cause difficulty for subscribers, whether they're streaming high-bandwidth video or low-bandwidth web applications. This causes significant deterioration in subscriber QoE. Service providers must deliver a high quality of service (QoS) to subscribers at all times, even during periods of heavy network congestion.



Bandwidth control limits can be applied at the application level or at a per-subscriber, per-application level.

THE SOLUTION

BIG-IP Policy Enforcement Manager™ (PEM) delivers subscriber insight and effectively manages network traffic via a wide range of subscriber-aware policies, like identifying subscriber usage and subscriber plans.

Traffic classification (also called application awareness) is a key feature of BIG-IP PEM. It identifies which applications, services, and protocols are being used to help you create application-specific plans, like controlling how much bandwidth is being allocated for specific applications and rate-limiting P2P applications during peak network congestion levels. BIG-IP PEM classifies traffic into several categories of applications and protocols including P2P, VoIP, web, and streaming applications.

The policies can be obtained via various methods, with the most common in mobile networks being Gx (PCRF).

BIG-IP PEM effectively manages network traffic to optimize performance or enforce controls on traffic via subscriber- and application-aware policies. BIG-IP PEM provides subscriber- and/or application-aware bandwidth-controlling mechanisms via rate limiting, DSCP marking, and layer 2 QoS marking. These limits can be applied to a group of subscribers, to all subscribers, at the application level, or per subscriber per application level.

These capabilities help service providers establish tiered services and manage incremental revenue generating plans based on subscribers' actual data and application usage patterns. They also help with implementing fair-usage policies, allowing subscribers to consume bandwidth fairly and with proportional distribution across the subscriber base.

F5 HELPS YOU:

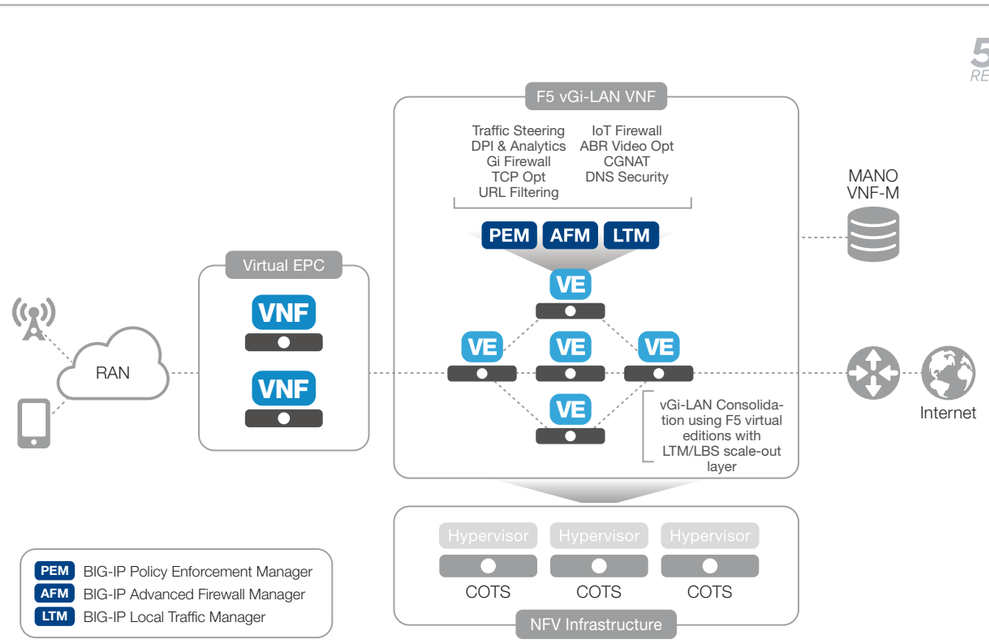
- Optimize network performance.
- Increase ARPU with new services.
- Reduce churn and gain additional brand loyalty.

DATA TRAFFIC MANAGEMENT SOLUTIONS

Charging and Quota Management

THE CHALLENGE

In mobile networks, subscribers sign up for specific quotas based on their service tiers, and the operator charges them appropriately and allows a refresh of quotas. Service providers need to provide consistent QoE to ensure that subscribers receive the service they have signed up for.



Mobile access virtual SGi-LAN deployments. Highly scalable network function virtualization.

THE SOLUTION

Leveraging BIG-IP PEM, operators can integrate with the online charging system (3GPP) and define quotas which are tracked per subscriber/application. This allows service providers to bill the subscribers appropriately and charge them for quota renewals.

F5 HELPS YOU:

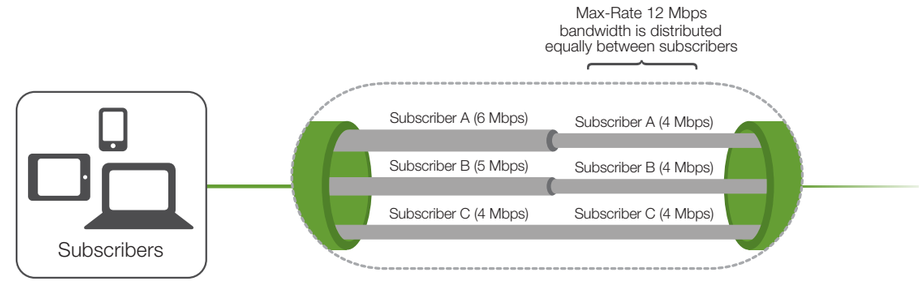
- Assign quotas to subscribers depending on their service plan.
- Provide high QoE to subscribers.
- Reduce churn.

DATA TRAFFIC MANAGEMENT SOLUTIONS

Fair Usage Policy

THE CHALLENGE

While Service Providers need to provide consistent QoE, many networks have a small percentage of heavy data users who continuously download and stream large amounts of content. Not only does this significantly strain the network, it also inhibits other users from getting the network speeds they have paid for.



Ensure higher QoE by evenly distributing bandwidth between subscribers.

THE SOLUTION

BIG-IP PEM detects heavy data users and the type of applications they are using. Subscriber- and application-awareness functionality, along with quota management and charging capabilities, help control rates on a per-subscriber and per-application basis, according to the existing rate plan. Evenly distributing and fairly allocating bandwidth between subscribers ensures higher QoE while efficiently managing network resources.

F5 HELPS YOU:

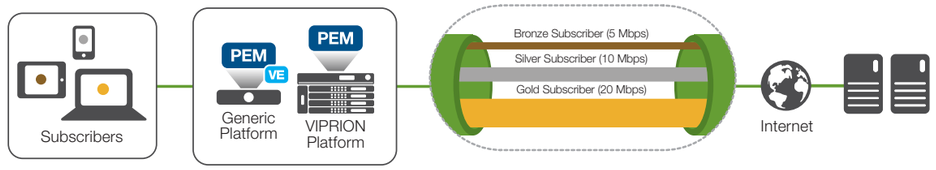
- Decrease network congestion.
- Provide high QoE to subscribers.
- Reduce churn.

DATA TRAFFIC MANAGEMENT SOLUTIONS

Tiered Service Plans

THE CHALLENGE

Service providers want new services that will help drive revenue while providing a high QoE to their subscribers. However, they cater to diverse subscriber bases with different expectations in the amount of bandwidth they require, and how much they are willing to pay.



Offer rate plans based on subscriber preferences and their bandwidth requirements.

THE SOLUTION

Tiered service plans offer specific rate plans based on subscriber preferences and their requirements for bandwidth and broadband speed. Some users may require the highest speeds possible while others only need content with best effort. The ability to offer tiered service plans with quota management ensures a high QoE for the subscriber base and increased revenues from those who use the network the most. For example, providers can implement a bronze, silver, or gold plan. Bronze and silver subscribers would be capped at a certain data limit and best-effort data speeds, whereas gold subscribers would get unlimited data and guaranteed class of service. Service plans can also be application specific or based on time of day.

F5 HELPS YOU:

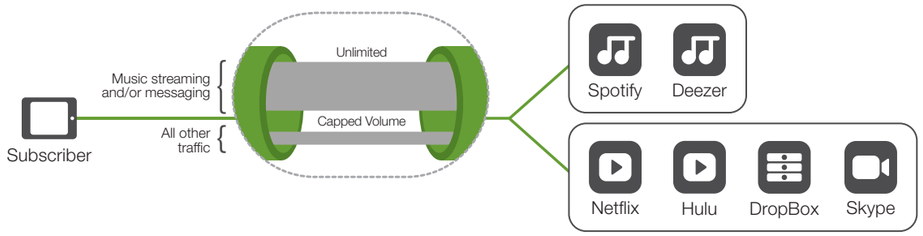
- Gain more revenue from high usage subscribers.
- Increase brand loyalty.
- Achieve greater optimization of the network.

DATA TRAFFIC MANAGEMENT SOLUTIONS

Over-the-Top (OTT) Monetization

THE CHALLENGE

Over-the-top (OTT) providers put pressure on service providers by offering bandwidth-intensive applications that drive networks to full capacity, while providing minimal or no revenue to the Service Providers.



Develop joint partnerships with OTT providers to offer services to your subscribers.

THE SOLUTION

With BIG-IP PEM, service providers can detect and classify specific applications and implement unique policies, such as applying a higher QoS to specific applications or excluding applications from a subscriber's data cap. For example, they can identify a video streaming application and determine that a subscriber has paid for the premium package. The subscriber then receives guaranteed QoS at all times for that application, while other applications are delivered based on best effort. In addition, specific OTT applications can be identified and excluded from a subscriber's data usage. For instance, subscribers using Facebook could be zero-rated, whereas other applications would count against their data cap. Both scenarios offer opportunities to form business partnerships with OTT providers, leading to monetization for these services. Another key use case is identifying ABR Video and applying throttles to it in a way that subscriber QoE is not impacted and the operator gains resource savings.

F5 HELPS YOU:

- Achieve higher QoE for subscribers.
- Increase revenue.

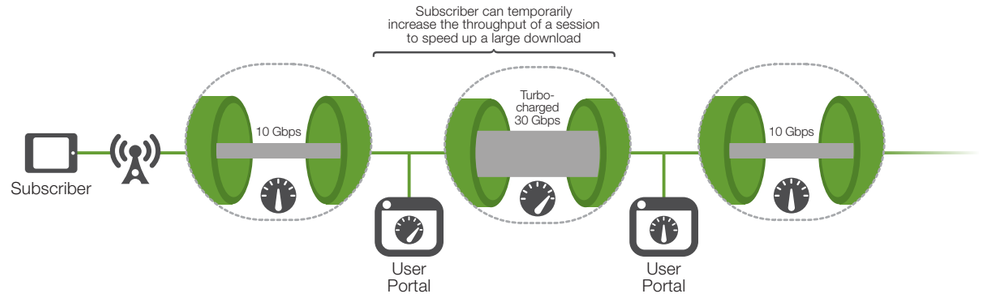
DATA TRAFFIC MANAGEMENT SOLUTIONS

Bandwidth On-Demand

THE CHALLENGE

Increased demand for bandwidth requires service providers to expand networks and add capacity to accommodate subscribers. However, peak traffic only happens at certain times of the day, while other times, network components sit idle, resulting in potential lost revenue.

5G READY



Provide your subscribers with a boost in bandwidth based on the time of day.

THE SOLUTION

Service providers can further differentiate their offerings by adapting to subscribers' real-time bandwidth requirements and quota management. A subscriber may only want a boost in bandwidth for a certain amount of time each day (either on- or off-peak hours). This provides an opportunity to generate incremental revenue by charging a premium to the subscriber for that period. Providers can also monitor the network for low utilization during off-peak hours, offering subscribers higher bandwidth speeds during these less-congested times, for an additional fee. In both cases, once the time period is over, the subscriber will resume normal broadband speeds.

F5 HELPS YOU:

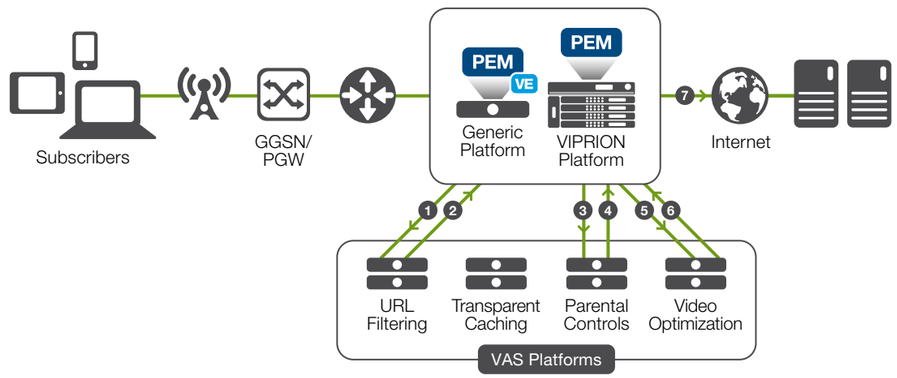
- Optimize network resources.
- Provide higher subscriber QoE.
- Increase revenue opportunities.

DATA TRAFFIC MANAGEMENT SOLUTIONS

Service Function Chaining/ Intelligent Traffic Steering

THE CHALLENGE

To support the growing number of services offered to subscribers, Service Providers have deployed multiple value-added service (VAS) platforms from a variety of different vendors. However, these platforms cause more network complexity, increased deployment and operating costs, and challenges in deploying new services. All data traffic is routed to these platforms via existing layer 3 and layer 4 equipment (including policy-based routers), regardless of relevance. As a result, all VAS platforms must inspect the traffic to determine whether to apply traffic policies or take specific action. This leads to additional VAS platforms needed to process all traffic, rather than just relevant traffic.



BIG-IP PEM with dynamic service chaining enables you to send traffic to multiple VAS platforms within a single call flow.

THE SOLUTION

BIG-IP PEM provides subscriber- and context-aware traffic management with the ability to perform layer 7 advanced steering to multiple VAS platforms (including web caching, video optimization, and parental control) based on parameters such as subscriber profile, device, content type, location, and network conditions. For example, BIG-IP PEM detects if a subscriber's mobile device is consuming video. If so, it can direct traffic from that device to a video optimization server. By steering traffic only to relevant servers, it reduces the burden on other servers, thereby reducing CapEx and OpEx. Intelligent traffic steering can decrease the traffic to VAS platforms by 50 to 75 percent, lowering the total cost of ownership.

To add more value for subscribers, the dynamic service chaining capabilities of BIG-IP PEM links multiple services together. Dynamic service chaining allows traffic to be sent to multiple value-added services within a single flow. For instance, BIG-IP PEM can send subscribers who want to watch a specific video clip to a URL filtering/parental control service before sending it to a video optimization server, ensuring that these subscribers are allowed to view the content. Dynamic service chaining creates differentiated services and provides opportunities to increase ARPU.

F5 HELPS YOU:

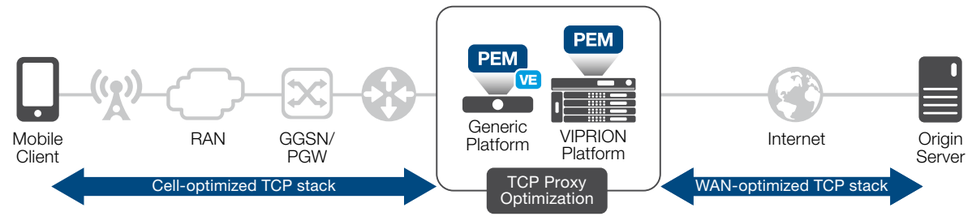
- Reduce deployment and operation costs.
- Simplify network architecture.
- Reduce time to deploy new services.
- Increase ARPU with innovative services.
- Create differentiated services.
- Improve QoE.

DATA TRAFFIC MANAGEMENT SOLUTIONS

IP Traffic Optimization

THE CHALLENGE

TCP has been the dominant traffic in operator networks. Within 3G/4G networks, mobile users are subject to the network connections based on the characteristics of the wireless access network—typically high latency, packet loss, and congestion. On the Internet side, the network has different performance characteristics including low latency, low packet loss, high bandwidth, and minimal congestion. To ensure the best customer experience, Service providers must implement a solution to optimize the TCP connection on both the Internet side and the wireless access network. In recent years, a dominant trend is the growth of non-TCP traffic mostly UDP/QUIC. Operators need the ability to handle the growing QUIC traffic.



Optimize TCP connections independently on both the Internet side and the wireless access network side.

THE SOLUTION

The BIG-IP system can optimize the TCP connections independently on both the Internet side and the wireless access network side. It is also possible to rate-pace UDP traffic similarly to TCP traffic via dynamic controls. This provides performance boost and improves subscriber QoE.

F5 HELPS YOU:

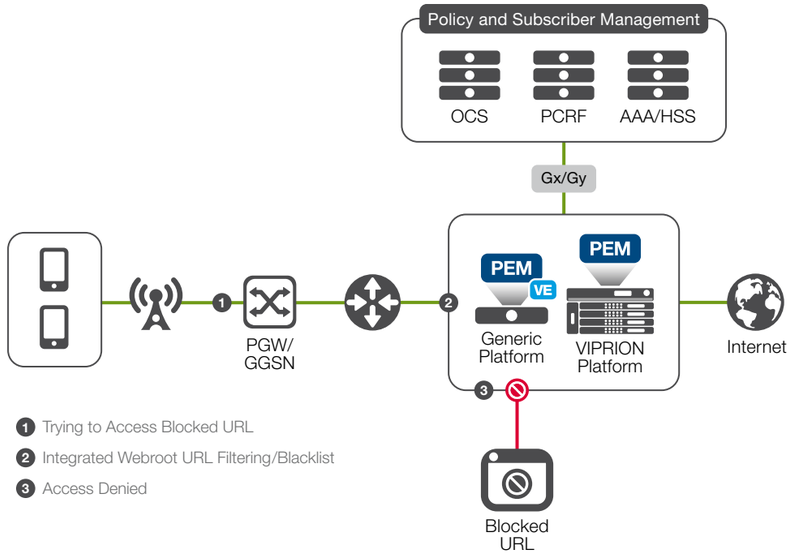
- Provide higher QoE to subscribers.
- Handle TCP and UDP traffic efficiently.
- Increase revenues with higher data usage.

DATA TRAFFIC MANAGEMENT SOLUTIONS

URL Filtering

THE CHALLENGE

The increasing percentage of young children and teenagers using devices to access the Internet can be a cause of concern for many parents, especially with inappropriate content so easily accessible and often unmonitored. Service providers need to develop solutions that give parents control over what sites their children can access. In addition, fixed and mobile service providers are required to comply with country regulations to block access to blacklisted content and provide a higher QoE for all subscribers.



BIG-IP PEM checks URL requests and blocks access to blacklisted sites as defined by subscribers or Service Providers.

THE SOLUTION

Service providers have an option to integrate URL filtering services within BIG-IP PEM. URL filtering implements parental control services by blocking traffic to specific websites based on specific URL categories. Parental controls allow for new revenue-generating services that provide greater QoE for subscribers.

In many countries, the service provider is responsible for URL filtering and content blocking to ensure that subscribers do not have access to potentially harmful content and that they adhere to cultural regulations. With built-in blacklisting capabilities, the F5 solution blocks access to a set of defined URLs or specific categories, such as gambling or child pornography, and allows access to specific content as defined by whitelists.

F5 HELPS YOU:

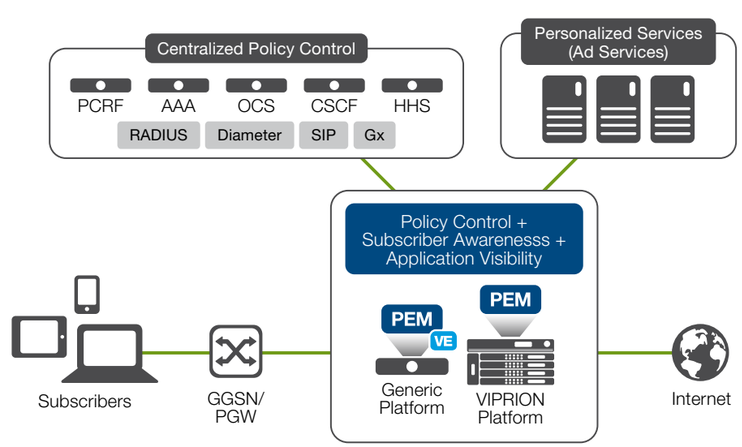
- Increase revenues.
- Maximize subscriber QoE.
- Comply with government regulations.

DATA TRAFFIC MANAGEMENT SOLUTIONS

Header Enrichment and Content Insertion

THE CHALLENGE

Service providers are continuously looking for ways to monetize and increase brand loyalty from subscribers. The devices used by mobile subscribers can provide a wealth of information, including subscriber location, applications used, and content viewed. When service providers can leverage this data, they can offer personalized services and insert content (such as ads and toolbars) within their devices, or enrich HTTP headers that immediately benefit subscribers.



Personalize the subscriber experience and increase revenue with content insertion.

THE SOLUTION

Personalized services offer a better subscriber experience while improving top-line revenue. The BIG-IP system helps providers gain subscriber- and context-awareness, as well as a deep understanding of subscribers' mobile preferences. BIG-IP PEM allows flexible enrichment of HTTP headers (for example, with MSISDN), allowing operators to tailor services appropriately. BIG-IP PEM also allows providers to insert targeted information into HTTP headers on mobile devices. This enables a variety of services like toolbar insertion, ad insertion, emergency alerts, etc. For example, a subscriber using a mobile device to look for a coffee shop could receive a discount ad for the nearest location. This type of service personalizes the subscriber experience while opening up additional business/revenue opportunities, like local retail stores paying to insert ads into HTTP headers.

F5 HELPS YOU:

- Offer new services and gain revenues.
- Increase subscriber brand loyalty.

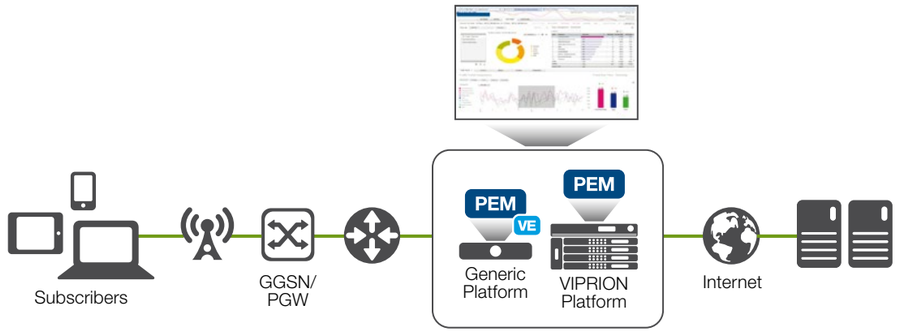
DATA TRAFFIC MANAGEMENT SOLUTIONS

Visibility, Reporting, and Analytics

THE CHALLENGE

Understanding traffic patterns and growth in the core network and Gi LAN for management, security, and analytics provides insight on network usage trends of their subscribers, their preferred applications, new applications that are becoming prevalent on operator networks, etc. This in turn helps them offer new and innovative services to cater more closely to subscriber needs and preferences, rather than offer a one-size-fits-all model of generic services and rate plans.

5G READY



Analytics gives you new ways to provide innovative services for your subscribers.

THE SOLUTION

BIG-IP PEM classifies traffic based on application type, offering new ways to provide tailored services for subscribers, generate new revenue, and increase customer satisfaction. Application charging and quota management allow for customized service plans based on subscriber requirements. For example, if subscribers are interested in a VoIP package, they can opt into a plan with unlimited VoIP usage for an additional fee. Likewise, subscribers interested in a business package can pay a fee to access service-enabling business applications without affecting their data caps.

BIG-IP PEM can also collect and report information at different levels of granularity (session, flow, etc.), which can then be sent over HSL to 3P analytics vendors. BIG-IP PEM also offers an on-box analytics/visibility capability which displays certain visual reports. The right analytics help providers offer multiple types of services based on specific market demographics, resulting in increased revenues, improved user experience, and greater brand loyalty.

F5 HELPS YOU:

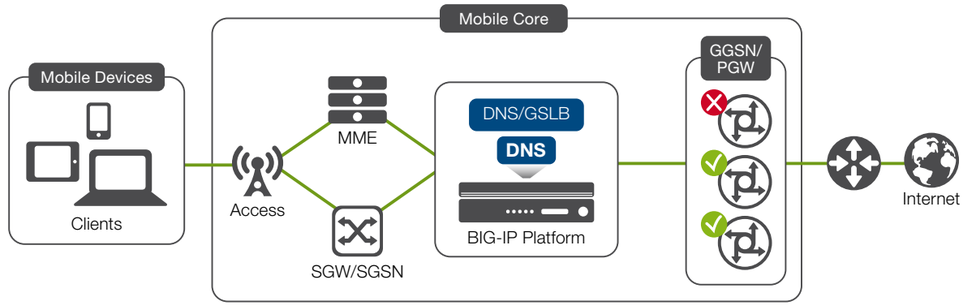
- Introduce innovative new services.
- Increase ARPU and brand loyalty.
- Enable application visibility, traffic detection function, charging/quota management, and reporting.

SIGNALING SOLUTIONS

Intelligent DNS for the Mobile Core

THE CHALLENGE

Today, most operators use a set of DNS solutions in the mobile core or Evolved Packet Core (EPC) to provide a static list of packet gateways or GGSNs (Gateway GPRS support node) for finding critical services. DNS provides the directory service by connecting service names to addresses. When a service request is initiated, DNS provides a static list of packet gateways. However, these gateways are not monitored, which makes the list non-deterministic (not based on monitoring or capacity). Overloading of a packet gateway can cause poor performance and service due to dropped connections and unanswered requests.



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.

THE SOLUTION

By using BIG-IP DNS and GSLB services for infrastructure deployments in the mobile core, the health and status of packet gateways or GGSNs can be monitored. BIG-IP DNS provides added value when subscribers need high-speed access to billing, support, and Internet services. Customizable monitors allow for the use of 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 packet gateway and GGSN selection process, which is critical for service delivery. BIG-IP DNS distributes the load intelligently across available GGSN and packet gateways, ensuring an optimal subscriber experience at all times.

F5 HELPS YOU:

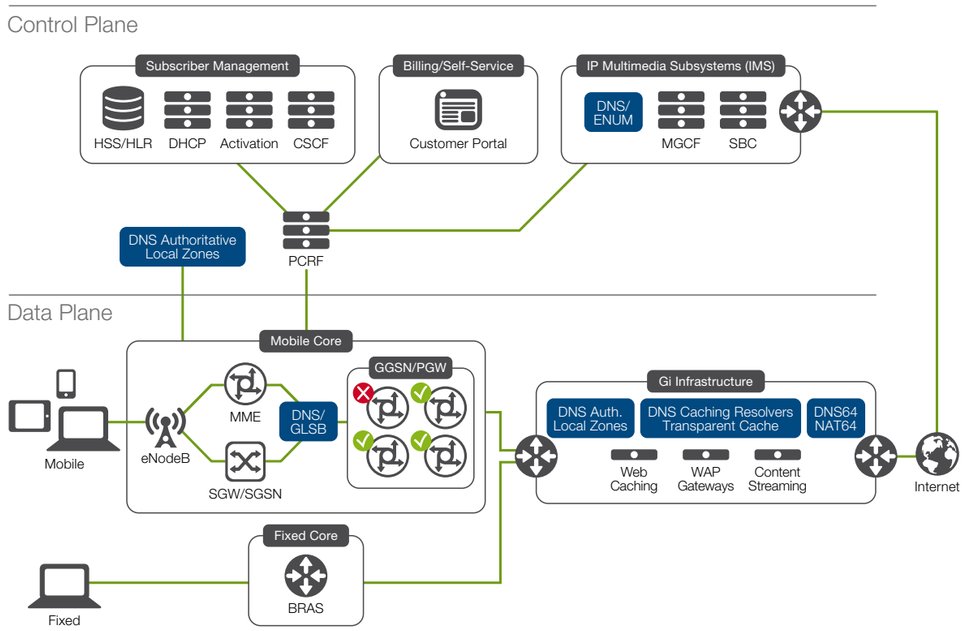
- Increase availability of services.
- Achieve closer mapping of capacity to required load.
- Reduce overhead through overprovisioning.
- Add or remove capacity automatically.

SIGNALING SOLUTIONS

Intelligent DNS Infrastructure

THE CHALLENGE

DNS is a core Internet technology and one of the most important components in a Service Provider's networking infrastructure, enabling users to access web applications and services. If DNS is unavailable, services will fail to function properly. Service Providers need to build an optimized and secure DNS infrastructure to better serve their users. However, creating this infrastructure requires a tremendous amount of real-time management, stability, and room to grow. Scaling DNS rapidly becomes a critical issue when dealing with millions of service names and IP addresses. As service providers scale their control plane, they also need to ensure the security of subscriber and billing data, as well as the capacity to withstand attacks, including DDoS, DNS amplification, and cache-poisoning.



BIG-IP DNS services optimize, secure, and monetize the operator's network.

THE SOLUTION

BIG-IP DNS makes it easy to optimize, secure, and monetize DNS infrastructures. It provides carrier-grade, high-performance LDNS caching and resolving, and is a hyperscale authoritative DNS solution that includes security service capabilities. BIG-IP DNS delivers an intelligent, scalable DNS infrastructure for faster access and web response to services for mobile users. In addition, it can load balance local and recursive DNS services. BIG-IP DNS also enables a DNS64 environment, creating a fault-tolerant architecture to optimize network traffic and increase QoE.

F5 HELPS YOU:

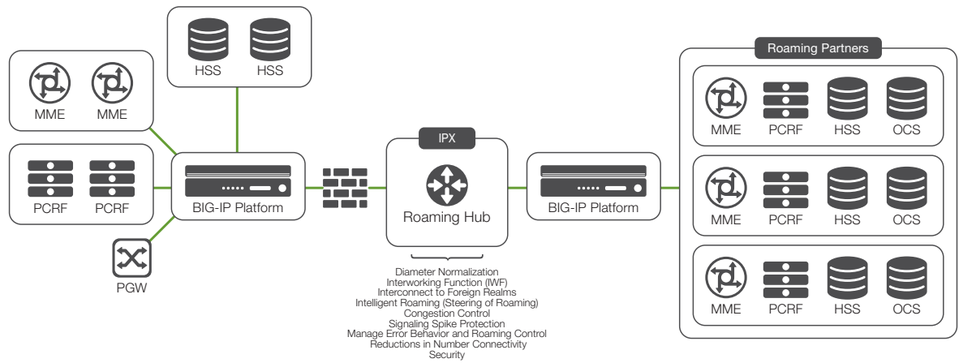
- Optimize network performance.
- Maximize subscriber QoE.
- Increase intelligence, flexibility, and automation.

SIGNALING SOLUTIONS

LTE Roaming

THE CHALLENGE

As service providers deploy LTE networks, they need to provide roaming services to LTE subscribers, including connectivity between LTE and 2.5G/3G roamers. This complex process requires addressing routing, scalability, and security issues while maintaining high QoS.



BIG-IP Diameter Traffic Management helps you seamlessly connect with roaming partners.

THE SOLUTION

BIG-IP Diameter Traffic Management fulfills technical requirements and generates revenue from roaming. To overcome the complexity resulting from connecting roamers using different technologies (e.g., 2G/3G versus 4G), BIG-IP Diameter Traffic Management provides connectivity, routing, translation capabilities, and extensive security, so users can connect quickly and safely with all other mobile networks, wholesale roaming providers, and IP eXchange (IPX) carriers.

F5 HELPS YOU:

- Achieve faster time to market with new roaming partners.
- Introduce new services.
- Grow your network and profits.

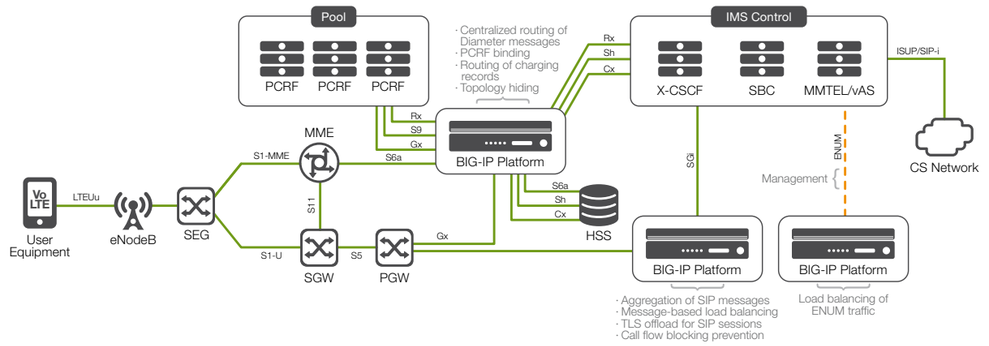
SIGNALING SOLUTIONS

SIP/IMS

THE CHALLENGE

With LTE, service providers can deliver higher broadband speeds, rich multimedia communication services, and VoLTE. To accomplish this, service providers have implemented IMS architectures, with SIP being one of the primary signaling protocols required to enable innovative applications and services. However, migrating to an all-IP-based network has its challenges, including security concerns. Specifically, the open-standard nature of the protocols make IP networks and services prone to attacks, including DoS, DDoS, stealth floods, and botnets, as well as malformed or unroutable SIP requests. In addition, migration to all-IP-based networks can pose challenges in managing capacity and performance as subscriber usage continues to increase over time, and, most importantly, in ensuring the availability of all-IP-based services.

5G READY



F5 delivers SIP solutions as part of a highly available, scalable, and secure IMS network infrastructure.

THE SOLUTION

The BIG-IP platform delivers SIP solutions as part of a highly available, scalable, and secure system for the IMS network infrastructure, including devices such as X-CSCF servers and session border controllers (SBC).

BIG-IP devices or virtual editions are positioned in front of SIP infrastructure and application servers where they manage SIP traffic and ensure service availability by continuously monitoring the SIP servers and applications at layer 7 while managing sessions between the different servers. Each new SIP session is forwarded to the most appropriate server, based on health and load. In addition, the BIG-IP platform can perform advanced health checks on SIP devices and route SIP clients away from unstable servers, providing increased reliability to existing SIP solutions. BIG-IP instances ensure there are no interoperability issues between IMS services by transforming the SIP requests and responses as necessary between multiple devices within the IMS architecture.

The BIG-IP platform enhances security by detecting and automatically dropping SIP communications that are malformed or contain errors. In addition, BIG-IP instances can log and report any unusual increase in SIP requests, including content that is malformed, contains errors, or otherwise appears to rapidly increase the threat of attacks.

F5 HELPS YOU:

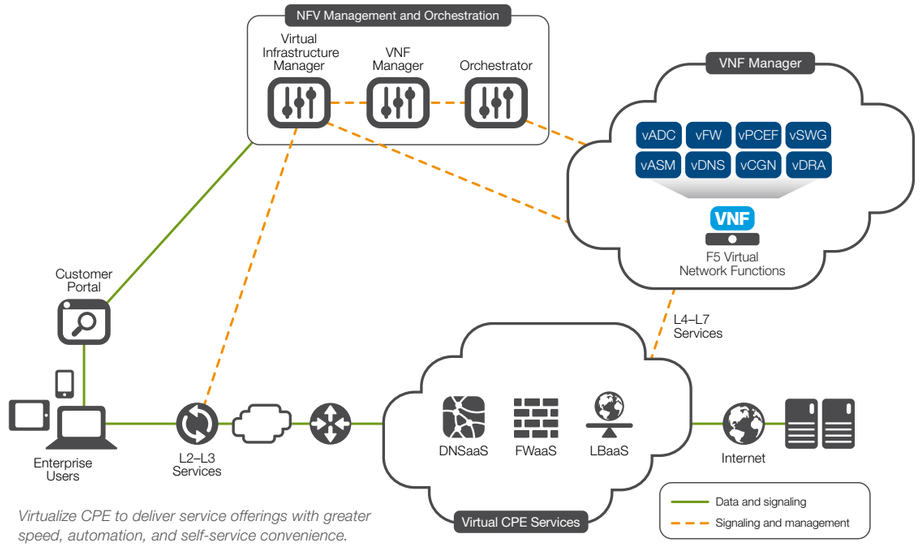
- Ensure interoperability of SIP requests and responses throughout IP infrastructure.
- Scale to handle millions of subscriber calls simultaneously.
- Enhance reliability at carrier-grade levels, including session synchronization and full failover capabilities with no connection loss.

NETWORK FUNCTIONS VIRTUALIZATION

Virtual CPE

THE CHALLENGE

Launching and deploying new services to enterprise customers can significantly challenge service providers. Service providers with rigid, inflexible network infrastructures incur higher CapEx and OpEx costs to physically install and provision services and customer premises equipment (CPE) in each customer location. In addition, when customers want to change a service or add capacity, the service provider needs to go on-site again to reconfigure, update, or swap out the device. From the enterprise perspective, any change requires them to schedule time and wait for the service to be turned on, causing significant delays and loss to their business, which in turn can lead to lost revenues for the service provider, as well as lower customer satisfaction.



Virtualize CPE to deliver service offerings with greater speed, automation, and self-service convenience.

THE SOLUTION

Virtual CPE helps service providers take advantage of common network functions virtualization (NFV) infrastructure for services deployed in the cloud and in the network. With NFV, where multiple core network functionalities are offered, virtual CPE enables service providers to adopt a cloud model. This cloud model enables you to share a common pool of resources and dynamically allocate physical compute and network resources to virtual network functions (VNF). You can deploy individual instances of virtualized network functions and offer them as services on customer premises.

Enterprise customers can spin up or spin down instances of network functions or order new services that can be dynamically provisioned in a single location or multiple global locations. Services can be ordered and provisioned via a self-service web portal offered by the service provider. This self-service enables service providers and enterprises alike to move from the complexities, costs, and long delivery cycles associated with deploying physical devices to a cloud-centric, automated, and agile model of service delivery, as and wherever needed.

All F5 VNFs can be deployed as a service, including load balancing as a service (LBaaS), firewall as a service (FWaaS), and DNS as a service (DNSaaS). By taking advantage of virtual CPE, service providers can achieve faster deployments in the network, faster recognition, higher revenues from service monetization, and a higher return on investment (ROI).

F5 HELPS YOU:

- Quickly introduce and deploy new network services.
- Reduce CapEx and OpEx for delivery of services on customer premises.
- Achieve end-to-end service automation and orchestration.
- Dynamically spin up and spin down services.
- Improve customer satisfaction and retention.

NETWORK FUNCTIONS VIRTUALIZATION

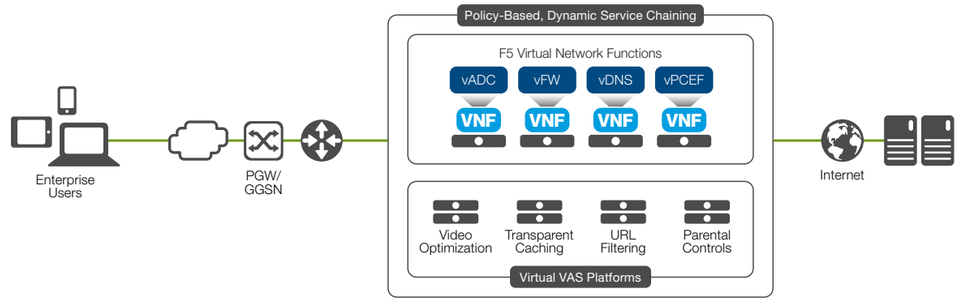
Virtual Gi LAN

THE CHALLENGE

The increases in mobile traffic, applications, and video streaming are placing a significant strain on the mobile network, including the Gi LAN. Within the Gi LAN are services including network address translation (NAT), firewall, policy management, traffic steering, and URL filtering, as well as TCP and video optimization. Service Providers are able to intelligently steer traffic, including video traffic, to optimization platforms or apply intelligent policy management actions based on subscriber and application awareness.

As mobile traffic increases, service providers need to scale out the Gi LAN, which in many cases consists of solutions from multiple vendors. For that reason, adding new services to the network can result in increased CapEx and OpEx while introducing additional complexities and increased points of failure into the network. As a result, delivery of new services to subscribers becomes more complex, with major delays, leading to loss of new revenue streams and lowered subscriber QoE.

5G READY



Simplify the network and speed time to market with a virtual Gi LAN.

THE SOLUTION

A virtualized Gi LAN solution from F5 enables service providers to build a cost-effective model, allowing for faster time to market for new services while reducing network complexity. F5 VNFs are a core component within an efficient virtual Gi LAN, providing solutions such as virtual policy enforcement, virtual firewall, and virtual Application Delivery Controller (ADC) services. These virtual solutions enable intelligent traffic steering to VAS components. Providers can dynamically chain together services based on real-time subscriber and application awareness, as well as secure the Gi LAN. By deploying a common, shared set of commercial, off-the-shelf (COTS) hardware to run various functions—network functions as well as software—hardware costs can be reduced while multiple services are deployed dynamically. This cloud-like model means service functions are delivered based on real-time network conditions and improve network resource utilization. Service providers also achieve greater service agility, as they can launch new services without any network downtime. A virtual Gi LAN allows for innovation, improved subscriber QoE, and lowered costs.

F5 HELPS YOU:

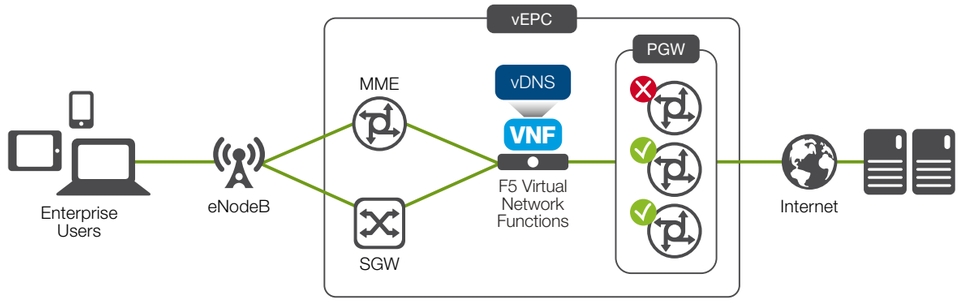
- Reduce CapEx and OpEx with COTS hardware.
- Increase service agility with faster build, test, and deploy cycles.
- Simplify the network architecture with software-based network functions.
- Dynamically manage and orchestrate services.
- Tailor innovative services to subscriber preference and usage.

NETWORK FUNCTIONS VIRTUALIZATION

Virtual EPC

THE CHALLENGE

Given increases in mobile data usage, and more notably, exponential growth in video traffic and growth in VoLTE, service providers need to architect their evolved packet cores (EPCs) to not only support the growth in traffic, but also to ensure that they can deliver a superior QoS at all times. As the market evolves, so must the EPC, including the ability to dynamically scale up to meet traffic demands during peak congestion hours and the flexibility to instantiate new services based on real-time network conditions. At the same time, service providers must ensure service availability and meet real-time performance requirements.



A virtual EPC reduces TCO and enables fast spin up and spin down of new services.

THE SOLUTION

Virtualizing the EPC allows service providers to quickly realize significant TCO savings and speed time to market for new services. In addition, service providers can reduce OpEx by dynamically spinning up and spinning down various network resources based on network demand and capacity.

F5 solutions using BIG-IP VEs include virtualized GTP load balancers, policy management, and Diameter signaling solutions. F5 virtual ADCs—based on BIG-IP LTM Virtual Edition—help perform GTP load balancing among a group of PGWs/SGWs. And by taking advantage of the global server load balancing (GSLB) and dynamic gateway selection functionality of BIG-IP DNS, service providers can monitor virtual packet gateways and only provide answers to the DNS queries for gateways that are active and available. If a packet gateway goes down, BIG-IP DNS will distribute the traffic load intelligently across only the available packet gateways, ensuring the best subscriber experience.

F5's NFV solutions rely on open REST-based APIs that are interoperable with leading management and orchestration systems, providing a complete NFV ecosystem. These solutions deliver a flexible, agile, and scalable network that helps deliver services to market faster, improve network efficiency, and reduce CapEx and OpEx.

F5 HELPS YOU:

- Reduce network costs.
- Improve network architecture flexibility.
- Speed service velocity.
- Increase automation.

F5 Solutions for Service Providers

F5 solutions for service providers allow network operators to optimize, secure, and monetize their networks. The solutions use a common, shared platform to reduce operational overhead and improve service provisioning velocity while addressing key security concerns across the network. F5 solutions for service providers help providers scale in three dimensions—the control, data, and application planes—supporting the highest connection rates and concurrency levels in the industry.

Control Plane

The control plane is the heart of a service provider's network. Tasked with managing subscriber use and ensuring appropriate services are applied to traffic, it can easily become overwhelmed by signaling storms due to spikes in activations, for example, an Internet-wide gaming trend causing millions of concurrent players to join in. The control plane is driven predominantly by Diameter and SIP signaling protocols. F5 traffic management and signaling solutions include BIG-IP Policy Enforcement Manager (PEM) and support for Diameter and SIP to help network operators scale the control plane while creating new control plane services. This enables service providers to deliver secure, Service Level Agreement (SLA)-based services to users.

Data Plane

The service provider data plane serves as the backbone between the network and the Internet, supporting millions of consumer requests for applications. Bandwidth-hungry applications like video can be problematic for the data plane, degrading performance to the point subscribers seek a new provider. F5 solutions for service providers include a high-performance services fabric composed of hardware or virtual network functions (VNFs) in any combination. F5 chassis-based VIPRION offerings support up to 1.2 billion concurrent connections and greater than one terabit (1TB) of throughput, while F5 VNFs and BIG-IP virtual editions (VEs) support L4 throughput up to 70 Gbps.

The F5 high-performance services fabric is built on a common, shared, and optimized platform on which key service provider functions can be consolidated. By doing so in the Gi network on a single platform, providers can eliminate the operational overhead incurred by the need to manage multiple point products, including Carrier-Grade NAT (CGNAT) and firewalls.

Application Plane

Value-added services (VAS) are a key differentiator and key revenue opportunity for service providers, but can be the source of poor performance due to the requirement to route all data traffic through all services, regardless of applicability. Sending text through a video optimization service or video through an ad insertion service does not add value; rather, it consumes resources and time, impacting the overall subscriber experience. F5 solutions for service providers work with virtual machine provisioning systems to help service providers move toward network functions virtualization (NFV)-based architectures. Intelligent monitoring of value-added services, combined with awareness of load and demand, enable service providers to ensure their VAS platforms can be scaled up and down individually, resulting in significant cost savings across the VAS infrastructure. With F5 solutions, network operators can simplify their Gi networks and combine physical, virtual, and cloud-based deployments to form a unified, elastic, high-performance services fabric. This enables more efficient network architectures while laying the foundation for rapid service creation and deployment.

F5 enables fixed and mobile service providers to leverage next-generation networks to provide a superior customer experience. Intelligent L4–L7 network devices play a primary role in the F5 approach to solution design, allowing service providers to maintain high network performance while expanding customized products and services for specific audiences.

Diameter Signaling Management

Diameter signaling messages serve as an excellent source of information on network operations and subscribers. When extrapolated, this information can help differentiate service offerings and improve the customer experience. BIG-IP solutions are capable of manipulating, load-balancing, rate-limiting, and adding security within a Diameter network.

Intelligent Traffic Management and Policy Enforcement

F5 offers intelligent traffic management solutions on a unified platform, simplifying delivery of network services such as dynamic service chaining. Using context- and subscriber-aware technology, BIG-IP PEM offers a full-proxy architecture and rich IP capabilities for critical traffic visibility and analytics, as well as sophisticated traffic-steering capabilities—including the ability to inspect and route traffic based on data type and subscribers' profiles.

DNS Services to Manage Network Growth

F5's comprehensive control and data plane solutions optimize, intelligently scale, and securely manage messaging interfaces such as RADIUS, DNS, and SIP. BIG-IP DNS allows service providers to optimize their LDNS, authoritative DNS, and infrastructure DNS, delivering a high subscriber QoE, which in turn increases revenues and reduces churn.

Carrier-Grade Network Firewall Security

F5 provides integrated, high-performance ICSA Labs Certified security solutions. F5 carrier-class network firewall solutions protect the entire network infrastructure and scale to perform under the most demanding conditions. Operators benefit from these solutions' intelligence, flexibility for enhancement, and simplification of network security in the increasingly threatening landscape—with a common platform to deliver applications and improve responsiveness. BIG-IP Application Security Manager (ASM) enhances security for applications by providing comprehensive web security and L7 DDoS protection.

SDN and NFV Solutions

With F5 solutions, service providers can move to software-defined networking (SDN) and NFV architectures for greater agility. They can deploy applications and services across multiple hybrid network architectures and evolving NFV environments using both F5 purpose-built, carrier-grade chassis and VNFs. The fully virtualized, carrier-grade F5 network architecture reduces operator dependency on inflexible hardware and enables a more dynamic, flexible, and agile network. Operators can rapidly test and deliver a variety of personalized services while managing rapid growth and increasing efficiency and security.

F5 solutions also help generate new revenues through services such as parental controls, enhanced security, shared data plans, application-based charging, VoLTE, URL filtering, and content insertion.

About F5

F5 (NASDAQ: FFIV) provides solutions for an application world. F5 helps organizations seamlessly scale cloud, data center, and SDN deployments to successfully deliver applications to anyone, anywhere, at any time. F5 solutions broaden the reach of IT through an open, extensible framework and a rich partner ecosystem of leading technology and data center orchestration vendors. This approach lets customers pursue the infrastructure model that best fits their needs over time. The world's largest businesses, service providers, government entities, and consumer brands rely on F5 to stay ahead of cloud, security, and mobility trends. For more information, go to f5.com.

WE MAKE APPS

FASTER. SMARTER. SAFER.

US Headquarters: 401 Elliott Ave W, Seattle, WA 98119 | 888-882-4447 // Americas: info@f5.com // Asia-Pacific: apacinfo@f5.com // Europe/Middle East/Africa: emeainfo@f5.com // Japan: f5j-info@f5.com

 GUIDE-MWC-196823413