Application Traffic Management

Overview

Traffic Management has long been an integral part of the enterprise network. Over the last seven years, Internet Traffic Management has grown from beyond just a means to route HTTP (Web) traffic to the most available web server; it now represents a way to intercept, inspect, transform, and direct that traffic for core business applications to the correct resource, based on specific business policies.

F5 Networks is pioneering a new category within the networking market called ***Application Traffic Management***. Application Traffic Management allows customers to apply all the benefits (high availability, scalability, security, and increased performance) delivered by traditional Internet Traffic Management to *any* IP-based application. Application Traffic Management is driven by four key markets:

- ***Enterprise Applications*** - the delivery of any application over IP (Internet Protocol) within the enterprise. These applications include nearly all Independent Software Vendors (ISVs) including Microsoft®, Oracle®, SAP®, BEA®, Siebel®, PeopleSoft®, IBM®, Sun®, and WebMethods®.

- ***Web Services*** - the ability to integrate different systems, applications, and organizations regardless of the hardware, operating system, application type or location, using SOAP, XML, and UDDI.

- ***Mobile Computing*** - the ability to deliver any application to any type of mobile device, at any time.

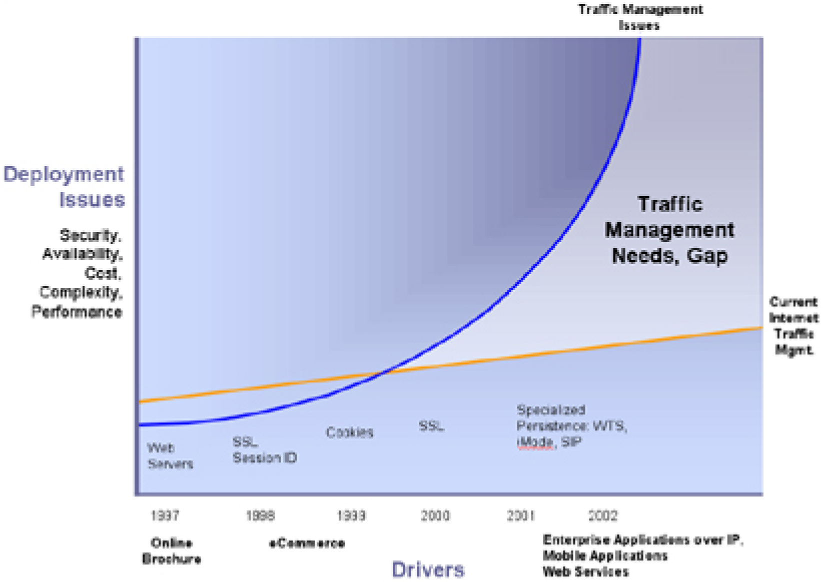
- ***Security*** - the ability to configure and enforce common application level security policies, and protect against application level attacks and threats.

This white paper focuses primarily on new technology in F5 Networks BIG-IP® product including the Universal Inspection Engine (UIE), iRules™, and the Dynamic Security Control Architecture (DSCA). UIE and iRules drive the BIG-IP product's ability to switch, persist, and filter any IP-based application or Web service based upon content encapsulated in a packet's header or payload. The Dynamic Security Control Architecture (DSCA) enforces, fortifies, and accelerates the secure delivery of application and Web services, which allows the BIG-IP to automatically respond to, act upon, and prevent changing security threats. The resulting benefits of these features are extremely significant, allowing the product to support the complex security and high availability requirements of today's Web services, enterprise and mobile applications -- making them simpler to implement and maintain. The result is a dramatic gain in operational efficiencies and cost-savings.

Challenge

The fundamental problem in the Internet Traffic Management industry is that enterprises and service providers cannot extend the benefits of traffic management to all of their IP-based applications. As businesses continue to deploy Web services and enterprise and mobile applications over IP (Internet Protocol), the same type of high availability, security, and flexibility that previously ensured success for web servers must be applied to ensure success in this more complex environment. The goal was to extend the flexibility of the current best-practice architectures to all back-office applications in order to achieve the same economies of scale and operational efficiencies.

The intelligence and flexibility needed to support all of these processes is staggering. F5 developed its Application Traffic Management products in order to support all of the different types of applications and services traversing the network, such as streaming media, Web services, video, voice, enterprise, and mobile applications.



Application traffic management bridges the gap between current internet traffic management devices and deployment and traffic management issues

The challenges in supporting these deployments include:

Ensuring Quality of Service (QoS) and manageability - Building application redundancy in multi-tier architectures creates the need for networking devices able to support each tier. Distributed applications and their differing platforms make for a complex environment. Business rules and policies for traffic must be easy to set and flexible.

Providing scalability - Existing IP-based applications and services are rapidly and constantly evolving, while new IP-based applications and services are still being introduced. Organizations must find a solution that can easily integrate new and evolving technologies without significant effort.

Enhancing security - One of the biggest challenges for enterprises is to stay on top of security issues. Organizations need a networking solution that can not only ensure the secure delivery of applications and Web services, but also accelerate transactions. A complete security solution includes comprehensive authentication, authorization, auditing, and payload parsing features that allow organizations to enforce their security policies at the edge of the network, before a session is allowed.

Saving costs while increasing ROI - An increasing number of enterprises are expanding their networks to include Web services and mobile connectivity, but with a close eye on costs. Without proper application traffic management, these new architectures can cost thousands of dollars, require expensive servers and special software implementation. Organizations are looking for a product that can help lower or eliminate special development costs and time, and reduce the level and quantity of hardware and applications they need to purchase.

Solution

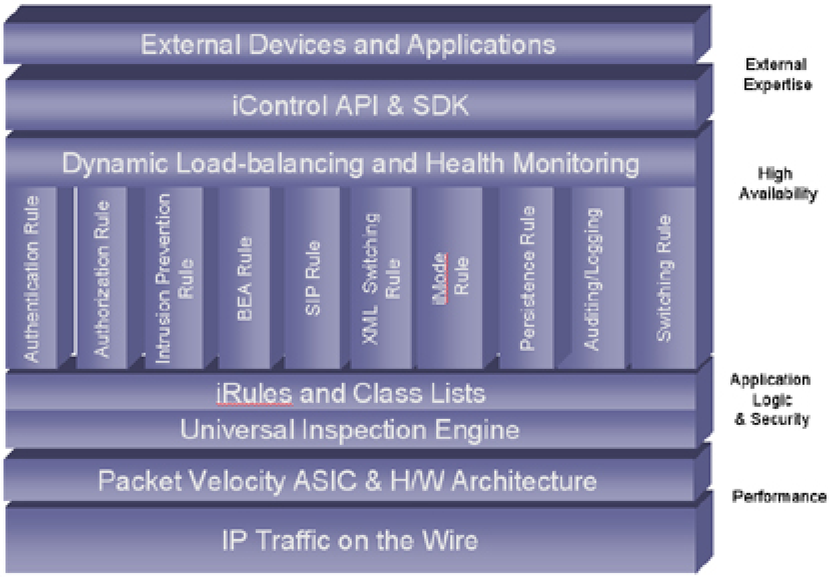
F5's BIG-IP product is the first application traffic management device on the market that can process any application or Web service, ensuring quick response times, reliable sessions, easy scalability, and application-level security -- all in a single network device.

Because of its unique, strategic placement in the network between the router and servers, the BIG-IP product is aware of everything within the ingress and egress traffic, and can react appropriately. The Universal Inspection Engine inspects any data in the HTTP and TCP data stream, and iRules allow administrators to apply new intelligence and business decisions to traffic management. With BIG-IP system's superior load balancing algorithms and advanced health checking capabilities, organizations have the most robust high availability solution on the market today. And to complete the solution, F5's iControl™ API/SDK overcomes the greatest challenges of integration - making it quick and easy to create intercommunication between 3rd party applications and the network via F5's products. The BIG-IP product includes three distinguishing characteristics that make it unlike any other application traffic management product: The Universal Inspection Engine, iRules, and Dynamic Security Control

Universal Inspection Engine and iRules

The Universal Inspection Engine enables the BIG-IP product to be the first completely adaptable application management solution that can switch and persist on all types of IP applications and their payloads. The Universal Inspection Engine is the means - iRules are the tools used to apply intelligence and business decisions to application traffic management.

Through the use of the UIE and iRules, organizations can use lower cost servers to manage the same traffic, and eliminate expensive options for resolving tough availability, security, and scalability challenges. The Universal Inspection Engine allows organizations to direct traffic with pinpoint accuracy, based on exacting business requirements. The UIE can handle of all the different application or protocol types, in a single, intelligent network device. For example, with the UIE and iRules, customers can read, switch, and filter on mobile phone numbers found in the payload of a packet, database operation types found in the IP stream, and XML payload information.



A look at application traffic management

iRules are a powerful yet simple tool for defining the application traffic that administrators wish to direct, filter, or persist on. iRules enhance the ability of an enterprise or service provider to customize their application switching to suit exact business needs. Individual iRules can be defined to optimize the handling of traffic - where and when to send it for the fastest response based on application type, category, and priority. For example, using UIE and iRules, organizations can segment database traffic based on whether it is a read or read/write operation, allowing them to save money by purchasing less expensive database servers for the read operations, or use a single database server for both read and read/write sections.

iRules can be created, deleted or altered through F5's standards-based iControl (an open

Application Programming Interface based on SOAP/XML with control that can be extended to third-party devices). With iControl, network flow can be tuned based upon the application or service conditions, helping to automate communications between 3rd party applications and the BIG-IP system, while eliminating the need for manual intervention.

Dynamic Security Control

The BIG-IP product also features the Dynamic Security Control Architecture (DSCA) to enforce, fortify, and accelerate the secure delivery of application and Web services. By combining the expertise of specialized security devices and applications and acting on their behalf, the BIG-IP product is the first solution that can automatically respond to, act upon, and prevent changing security threats - providing a coordinated and unified line of defense, while improving the performance of other security products in the network.

Using VLAN mirroring or clone pools, the BIG-IP device directs traffic to the appropriate security device without disrupting the flow of traffic for intrusion detection, mail scanning, virus checking and other application level security services. This is ideal for an organization that wants application-level security at a practical cost for daily activities like business-to-business transactions between multiple suppliers (firewalls alone do not offer an organization the level of security required between these suppliers). Using the BIG-IP product and DSCA, an organization can offload functions from the servers and applications themselves onto the BIG-IP product, which centralizes security control. The BIG-IP with DSCA can authenticate, authorize, enforce intrusion prevention, and prevent application attacks, as well as log and report all activity.

Through the iControl API, specialized security devices and applications can directly communicate their knowledge to the BIG-IP device by creating, deleting or editing iRules, which alter how the BIG-IP system handles traffic. For example, suppose an attack is detected at 3:00 AM and the administrator is alerted by pager. Using the DSCA, the intrusion detection system that identified the threat can notify the BIG-IP product to discard traffic from the source, which solves the problem automatically.

F5 Networks - Pioneering Application Traffic Management

F5 Networks is setting the rules and standards for Application Traffic Management. Previous solutions to business problems were only possible at a high, and in many cases, impractical cost. With the latest version of the BIG-IP application traffic management product, best practices architectures can be built quickly and inexpensively without having to make massive application architectural changes or buying expensive midrange or high-end servers. F5 Application Traffic Management is the solution for supporting the highly complex requirements involved with today's Web services, enterprise applications, and mobile applications.