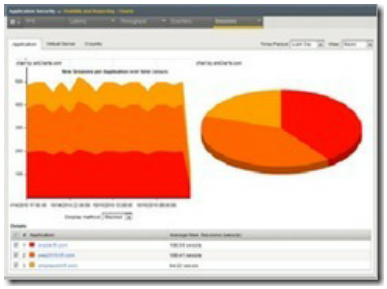
Dynamic Application Control and Attack Protection

Peter Silva, 2011-26-07

If you've perused any media outlet of late, the barrage of cyber threats are unrelenting and protecting your networks and applications continues to be a never ending task. Organizations are making significant investments in IT security to improve their attack protection but still need to control costs and keep the systems running efficiently. Since these attacks are targeting multiple layers of the infrastructure, both the network and applications, it is increasingly difficult to properly reduce the risk of exposure. Siloes of protection and network firewalls alone cannot do the trick. Add to that, the dynamic nature of today's infrastructures especially with cloud environments, makes the job even tougher. Federal mandates and standards for government agencies, contractors and the public sector adds to an organization's growing list of concerns. DNS can be vulnerable to attacks; interactive Web 2.0 applications can be vulnerable; and IT needs analytics and detailed reporting to understand what's happening within their dynamic data center. On top of that, IPv6 is now a reality and v6 to v4 translation services are in demand.



F5's most recent release, BIG-IP v11, delivers a unified platform that helps protect Web 2.0 applications and data, secure DNS infrastructures, and establish centralized application access and policy control. In BIG-IP v10, F5 offered the Application Ready Solution Templates to reduce the time, effort, and application-specific knowledge required of administrators to optimally deploy applications. With BIG-IP v11, F5 introduces iApp, a template-driven system that automates application deployment. iApp helps reduce human error by enabling an organization's IT department to apply preconfigured, approved security policies and repeat and reuse them with each application deployment. Also iApp analytics provides real-time visibility into application performance, which helps IT staff identify the root cause of security and performance issues quickly and efficiently.

For DNS, BIG-IP GTM has offered a DNSSEC solution since v10 and with v11, we've added DNS Express, a high-speed authoritative DNS delivery solution. DNS query response performance can be improved as much as 10x. DNS Express offloads existing DNS servers and absorbs the flood of illegitimate DNS requests during an attack—all while supporting legitimate queries. It's critical to have the ability to protect and scale the DNS infrastructure when a DoS or DDoS attacks occur, since DNS is just as vulnerable as the web application or service that is being targeted.

For interactive web applications, BIG-IP ASM v11 can parse JSON (JavaScript Object Notation) payloads and protect AJAX (Asynchronous JavaScript and XML) applications that use JSON for data transfer between the client and server. AJAX, which is a mix of technologies, is becoming more pervasive since it allows developers to deliver content without having to load the entire HTML page in which the AJAX objects are embedded. Unfortunately, poor AJAX code can allow an attacker to modify the application and prevent a user from seeing their customized content, or even initiate an XSS attack. Additionally, some developers are also using JSON payloads, a lightweight data-interchange format that is understandable by most modern programming languages and used to exchange information between browser and server. If JSON is insecure and carrying sensitive information, there is the potential for data leakage. BIG-IP ASM can enforce the proper security policy and can even display an embedded blocking alert message. Very few WAF vendors are capable of enforcing JSON (other than the XML Gateways), and no other vendor can display an embedded blocking alert message. F5 is the only WAF vendor that fully supports AJAX, which is becoming more and more common even within enterprises.

Also with v11, BIG-IP ASM is now available in a Virtual Edition (BIG-IP ASM VE), either as a stand-alone appliance or an add-on module for BIG-IP Local Traffic Manager Virtual Edition (LTM VE). BIG-IP ASM VE delivers the same functionality as the physical edition and helps companies maintain compliance, including PCI DSS, when they deploy applications in the cloud. If an organization discovers an application vulnerability, BIG-IP ASM VE can quickly be deployed in a cloud environment, enabling organizations to immediately virtually patch vulnerabilities until the development team can permanently fix the application. Additionally, organizations are often unable to fix applications developed by third parties, and this lack of control prevents many of them from considering cloud deployments. But with BIG-IP ASM VE, organizations have full control over securing their cloud infrastructure.

After about 5 years of IPv4 depletion stories, it finally seems to be coming soon and IPv6 is starting to be deployed. Problem is that most enterprise networks are not yet ready to handle IPv4 and IPv6 at the same time. BIG-IP v11 provides advanced support for IPv6 with built-in DNS 6-to-4 translation services and the ability to direct traffic to any server in mixed (IPv4 and IPv6) environments. This gives organizations the flexibility to support IPv6 devices today while transitioning their backend servers to IPv6 over time.

Many more new features are available across all F5 solutions including BIG-IP APM which added support for site-to-site IPsec tunnels, AppTunnels, Kerberos ticketing, enhanced virtual desktops, Android and iOS clients, and multi-domain single sign-on. These are just a few of the many new enhancements available in BIG-IP v11.

ps

Resources:

- The BIG-IP v11 System
- F5 Delivers on Dynamic Data Center Vision with New Application Control Plane Architecture
- F5's Enhanced BIG-IP Security Solutions Thwart Multilayer Cyber Attacks
- ABLE Infrastructure: The Next Generation – Introducing v11
- The Evolution To IT as a Service Continues … in the Network
- iApp Wiki on DevCentral

Whitepapers:

- High-Performance DNS Services in BIG-IP Version 11
- Symmetric Optimization in the Cloud with BIG-IP WOM VE
- Secure, Optimized Global Access to Corporate Resources
- Maximizing the Strategic Point of Control in the Application Delivery Network
- Application Security in the Cloud with BIG-IP ASM
- F5 iApp: Moving Application Delivery Beyond the Network
- Simplifying Single Sign-On with F5 BIG-IP APM and Active Directory
- BIG-IP Virtual Edition Products,The Virtual ADCs Your Application Delivery Network Has Been Missing

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

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com