F5 makes an even bigger BIG-IP with version 11

Analyst: Wendy Nather Eric Hanselman

28 Jul, 2011

F5 recently announced release 11 of its TMOS (Traffic Management Operating System), which forms the underlying platform for its products (BIG-IP runs TMOS, and both are in v11). The release contains numerous major enhancements, such as multi-way clustering between BIG-IP devices to create a pool of application-delivery services, and an open application logging engine. However, one of the most interesting developments is its new iApp technology, which uses templates (much as its iRules did for network traffic management) to standardize and provision the underlying network services associated with a given application. This ties the network (and security) configurations more closely to the application configurations, and that leads us to think of one word: devops.

The 451 Take

The release of version 11 kicks it up a notch in breadth of functionality, offering a unique level of integration. F5 was smart to build on the success of its network-level iRules by adding iApp, which consists of a language and templates that specify the network-level configuration needed to support a deployed application. This not only supports movements like devops – bridging the traditional gap between software development and network operations – but also edges F5 closer to competition with other application performance management players like IBM's Tivoli, CA Technologies, BMC and Hewlett-Packard. F5's hardware platform offers significant performance; the longer-term question is where specialized hardware will play a role as the world gets cloudier.

Copyright 2011 - The 451 Group

Version 11 of F5's BIG-IP introduces its Application Control Plane architecture, in which the device's application-delivery services are managed in a dynamic pool. This allows the services that provide availability, security and optimization to be configured and allocated on demand more quickly than before. F5's new ScaleN architecture allows the BIG-IP devices to be clustered in multiple combinations across networks and distributed sites, and manages them in a virtualized fashion. This abstraction makes it easier to identify and administer all the network services that a given application depends on, so that whole services can failover from one BIG-IP cluster to another. It also treats network users and resources as virtualized objects, regardless of their actual locations, so that the administrator can apply policies to them that are more abstracted and persistent.

Application provisioning

This growing abstraction of network services to match server virtualization characteristics was an obvious next step for application-delivery control. However, F5 knew the power of its iRules scripting language, which has acquired a development community of its own (F5's DevCentral website encourages collaboration and sharing of iRules code), and it has taken a powerful step in applying that concept to application-layer resource management. The company's new iApp capability allows the administrator to create a template for provisioning network resources that a given application needs. In a manually administered environment, deploying an application generally means that a software team installs and configures the actual code on the assigned servers, and a separate network team has to figure out what network services to configure to support it.

For example, a large enterprise application might require network access from specific ports to other ports on other servers; it would also need access to domain name services (DNS), Simple Mail Transfer Protocol services for sending email notifications, Internet routing and proxying services, authentication and authorization services, backup services, and database connectivity. It might be calling any number of Web services from other parts of the enterprise, logging to a specific device, and using load balancing and SSL acceleration from BIG-IP itself. Each of these requires network-level settings that developers generally don't track or administer themselves, and an application deployment can be slowed down if the requirements aren't fully communicated to the network or security teams. With an iApp template, all of the requirements are kept in one place, which makes them easier to apply consistently; improves change control; and speeds up the failover, troubleshooting and provisioning processes. Applications today aren't terribly fluid, but the iApp capability certainly helps to grease the skids.

F5's version 11 comes with a number of prebuilt iApp templates for well-known commercial applications, such as Microsoft Exchange, BEA Software's WebLogic, Oracle Application Server, SAP and IBM WebSphere. It is also encouraging users to share iApp templates on its DevCentral site in the same way that iRules are being shared today. IApp creates a bridge between the application and network management in a way that we consider to be a significant boost to the devops movement, in which developers and operations work more closely together to improve software delivery to the business. We expect that both development and operations will find the templates useful for solidifying the application rollout process, and it may also provide a better bridge between the enterprise application owners and cloud providers: Being able to say, 'Here, just use this template to configure the services we need,' is much more straightforward than delivering a spreadsheet of settings grouped by network addresses and server names.

Identity management

The new release also includes enhancements for single sign-on with identity management. An F5 device can take a user's credentials and verify them with an identity management system (a number of different authentication types are supported), and then, based on the results, pass them on to different applications without further prompting to the user. This can speed user interaction with different applications and improve security by not delivering users to applications to which they're not allowed access.

Application protections

Two new Web application inspection functions are included in v11 for Ajax and JSON objects. This will help F5 secure a more complete set of Web applications and seal another attack path for customers that are consolidating content through their Web applications. In version 11, WhiteHat Security's Sentinel Web vulnerability-assessment offerings are more easily integrated at the user-interface level, as well as on the back end; the vulnerabilities identified with Sentinel can be funneled to F5's Application Security Manager for blocking until they're remediated.

Availability protections

Given the number of recent highly publicized denial-of-service (DoS) attacks, customers may also be attracted to version 11's improved capabilities that can assist with availability when services are under attack. F5's Application Security Manager has DoS-filtering capabilities, and v11 adds the ability for the Global Traffic Manager (GTM) to handle DNS queries. As more organizations have implemented application DoS protections, attackers have shifted to taking down name servers, to

prevent users from reaching the servers hosting applications. GTM can now proxy DNS requests, allowing DNS performance to scale to levels that most DNS servers are unable to achieve. It's not providing a real DNS server, but it can insulate your DNS infrastructure and help it withstand an attack. It supports 'anycast' addressing and IPv6, which will help it fit in higher-capacity environments.

F5 has also added flexibility in internal load management to allow users to balance application load across multiple F5 systems. In the spring, its Clustered Multiprocessing functionality added the ability to virtualize the underlying hardware to allow more flexibility in how processing resources are assigned to applications. In v11, users can take this virtualization a step further and move applications to different chassis. This is accompanied by a change in licensing to allow customers to only pay for licenses for processors in a VIPRION chassis that are currently running an application. Idle processors don't need to have an active license.

Competition

With its enhanced VPN capabilities, F5 is stepping up its competitive posture with traditional VPN gateway products from the likes of Juniper and Citrix. For customers who require high capacity access management or want to include it with their ADC (application delivery controller) infrastructure, the power of the larger VIPRION systems may be attractive.

In a broader sense, F5 is competing with service offerings from content delivery networks, such as those provided by Akamai, and native ADC capabilities in cloud offerings. Against each of these, F5's strength has been the scale of its hardware platform and the breadth of its functionality. In a virtualized environment, scale will become less important. F5's move to more fully embrace virtual instances of its products will give them more traction in large enterprise and cloud deployments. As F5 embraces more operational control over the application layer – even if it's all based in the network – we see it encroaching on enterprise operations management suites such as IBM Tivoli (which has an interesting Application Dependency Discovery Manager, or TADDM). CA is also big in operational management, as are HP and BMC. F5 still has a disadvantage compared to the others, however, since it does not have visibility into or control over the actual processes and data resources running on the servers – if it doesn't happen across the network, BIG-IP won't know about it. Application delivery – meaning delivery across the network – is important, but it's by no means the whole picture when it comes to overall application performance management.

On the WAF side, F5 is still giving Imperva a run for its money, and is up against consolidated

vendors like Zeus Technology (which bought the distributed art of defence WAF), Crosscheck Networks (Forum Sentry), Bayshore Networks, NSFOCUS, ActivNetworks, Cisco, Barracuda Networks and Radware. There are 'WAF plus more' technologies available from Trustwave, eEye Digital Security, StillSecure, Sophos (Astaro), Deny All, Mykonos Software and Trustifier's ryū (Qualys has started its open source IronBee project, but still has a ways to go before it can be monetized). In the XML and SOA security arenas, there are vendors such as Intel (which has its Service Expressway Gateway, along with offering single-sign-on support), Layer 7 Technologies and IBM (whose DataPower is getting increasingly integrated with its Network IPS and Tivoli Access Manager).

Reproduced by permission of The 451 Group; © 2011. This report was originally published within 451 Research's Market Insight Service. For additional information on 451 Research or to apply for trial access, go to: www.451research.com