Ode to FirePass

Peter Silva, 2012-20-02

A decade ago, remote VPN access was a relatively new concept for businesses; it was available only to a select few who truly needed it, and it was usually over a dial-up connection. Vendors like Cisco, Check Point, and Microsoft started to develop VPN solutions using IPsec, one of the first transport layer security protocols, and RADIUS Server. At first organizations had to launch the modem and enter the pertinent information, but soon client software was offered as a package. This client software had to be installed, configured, and managed on the user's computer. As high-speed broadband became a household norm and SSL/TLS matured, the SSL VPN arrived, allowing secure connections via a browser-based environment. Client pre-installation and management hassles were eliminated; rather the masses now had secure access to corporate resources with just a few browser components and an appliance in the data center.

These early SSL VPNs, like the first release of F5's FirePass, offered endpoint checks and multiple modes of access depending on user needs. At the time, most SSL VPNs were limited in areas like overall performance, logins per second, concurrent sessions/users, and in some cases, throughput. Organizations that offered VPN extended it to executives, frequent travelers, and IT staff, and it was designed to provide separated access for corporate employees, partners, and contractors over the web portal. But these organizations were beginning to explore company-wide access since most employees still worked on-site.

Today, almost all employees have multiple devices, including smartphones, and most companies offer some sort of corporate VPN access. By 2015, 37.2 percent of the worldwide workforce will be remote and therefore mobile—that's 1.3 billion people. Content is richer, phones are faster, and bandwidth is available—at least via broadband to the home. Devices need to be authenticated and securely connected to corporate assets, making a high-performance Application Delivery Controller (ADC) with unified secure access a necessity. As FirePass is retired, organizations will have two ADC options with which to replace it: F5 BIG-IP Edge Gateway, a standalone appliance, and BIG-IP Access Policy Manager (APM), a module that can be added to BIG-IP LTM devices. Both products are more than just SSL VPNs—they're the central policy control points that are critical to managing dynamic data center environments.

A Little History

F5's first foray into the SSL VPN realm was with its 2003 purchase of uRoam and its flagship product, FirePass. Although still small, Infonetics Research predicted that the SSL VPN market will swell from around $25 million [in 2002] to $1 billion by 2005/6 and the old meta Group forecasted that SSL-based technology would be the dominant method for remote access, with 80 percent of users utilizing SSL by 2005/6. They were right—SSL VPN did take off.

Using technology already present in web browsers, SSL VPNs allowed any user from any browser to type in a URL and gain secure remote access to corporate resources. There was no full client to install—just a few browser control components or add-on to facilitate host checks and often, SSL-tunnel creation. Administrators could inspect the requesting computer to ensure it achieved certain levels of security, such as antivirus software, a firewall, and client certificates. Like today, there were multiple methods to gain encrypted access. There was (and still is) the full layer-3 network access connection; a port forwarding or application tunnel–type connection; or simply portal web access through a reverse proxy.

SSL VPNs Mature

With more enterprises deploying SSL VPNs, the market grew and FirePass proved to be an outstanding solution. Over the years, FirePass has lead the market with industry firsts like the Visual Policy Editor, VMware View support, group policy support, an SSL client that supported QoS (quality of service) and acceleration, and integrated support with third-party security solutions. Every year from 2007 through 2010, FirePass was an *SC Magazine Reader Trust* finalist for Best SSL VPN.

As predicted, SSL VPN took off in businesses; but few could have imagined how connected the world would really become. There are new types of tablet devices and powerful mobile devices, all growing at accelerated rates. And today, it's not just corporate laptops that request access, but personal smartphones, tablets, home computers, televisions, and many other new devices that will have an operating system and IP address.

As the market has grown, the need for scalability, flexibility, and access speed became more apparent. In response, F5 began including the FirePass SSL VPN functionality in the BIG-IP system of Application Delivery Controllers, specifically, BIG-IP Edge Gateway and BIG-IP Access Policy Manager (APM). Each a unified access solution, BIG-IP Edge Gateway and BIG-IP APM are scalable, secure, and agile controllers that can handle all access needs, whether remote, wireless, mobile, or LAN.

The secure access reigns of FirePass have been passed to the BIG-IP system; by the end of 2012, FirePass will no longer be available for sale. For organizations that have a FirePass SSL VPN, F5 will still offer support for it for several years. However those organizations are encouraged to test BIG-IP Edge Gateway or BIG-IP APM.

Unified Access Today

The accelerated advancement of the mobile and remote workforce is driving the need to support tens of thousands concurrent users. The bursting growth of Internet traffic and the demand for new services and rich media content can place extensive stress on networks, resulting in access latency and packet loss. With this demand, the ability of infrastructure to scale with the influx of traffic is essential. As business policies change over time, flexibility within the infrastructure gives IT the agility needed to keep pace with access demands while the security threats and application requirements are constantly evolving. Organizations need a high-performance ADC to be the strategic point of control between users and applications. This ADC must understand both the applications it delivers and the contextual nature of the users it serves.

BIG-IP Access Policy Manager

BIG-IP APM is a flexible, high-performance access and security add-on module for either the physical or virtual edition of BIG-IP Local Traffic Manager (LTM). BIG-IP APM can help organizations consolidate remote access infrastructure by providing unified global access to business-critical applications and networks. By converging and consolidating remote access, LAN access, and wireless connections within a single management interface, and providing easy-to-manage access policies, BIG-IP APM can help free up valuable IT resources and scale cost-effectively. BIG-IP APM protects public-facing applications by providing policy-based, context-aware access to users while consolidating access infrastructure.

BIG-IP Edge Gateway

BIG-IP Edge Gateway is a standalone appliance that provides all the benefits of BIG-IP APM—SSL VPN remote access security—plus application acceleration and WAN optimization services at the edge of the network—all in one efficient, scalable, and cost-effective solution.

BIG-IP Edge Gateway is designed to meet current and future IT demands, and can scale up to 60,000 concurrent users on a single box. It can accommodate all converged access needs, and on a single platform, organizations can manage remote access, LAN access, and wireless access by creating unique policies for each. BIG-IP Edge Gateway is the only ADC with remote access, acceleration, and optimization services built in. To address high latency links, technologies like intelligent caching, WAN optimization, compression, data deduplication, and application-specific optimization ensure the user is experiencing the best possible performance, 2 to 10 times faster than legacy SSL VPNs. BIG-IP Edge Gateway gives organizations unprecedented flexibility and agility to consolidate all their secure access methods on a single device.

FirePass SSL VPN Migration

A typical F5 customer might have deployed FirePass a few years ago to support RDP virtual desktops, endpoint host checks, and employee home computers, and to begin the transition from legacy IPsec VPNs. As a global workforce evolved with their smartphones and tablets, so did IT's desire to consolidate their secure access solutions. Many organizations have upgraded their FirePass controller functionality to a single BIG-IP appliance.

Migrating any system can be a challenge, especially when it is a critical piece of the infrastructure that global users rely on. Migrating security devices, particularly remote access solutions, can be even more daunting since policies and settings are often based on an identity and access management framework. Intranet web applications, network access settings, basic device configurations, certificates, logs, statistics, and many other settings often need to be configured on the new controller.

FirePass can make migrating to BIG-IP Edge Gateway or BIG-IP APM a smooth, fast process. The FirePass Configuration Export Tool, available as a hotfix (HF-359012-1) for FirePass v6.1 and v7, exports configurations into XML files. Device management, network access, portal access, and user information can also all be exported to an XML file. Special settings like master groups, IP address pools, packet filter rules, VLANS, DNS, hosts, drive mappings, policy checks, and caching and compression are saved so an administrator can properly configure the new security device. It's critical that important configuration settings are mapped properly to the new controller, and with the FirePass Configuration Export Tool, administrators can deploy the existing FirePass configurations to a new BIG-IP Edge Gateway device or BIG-IP APM module. A migration guide will be available shortly.

SSL VPNs like FirePass have helped pave the way for easy, ubiquitous remote access to sensitive corporate resources. As the needs of the corporate enterprise change, so must the surrounding technology tasked with facilitating IT initiates. The massive growth of the mobile workforce and their devices, along with the need to secure and optimize the delivery of rich content, requires a controller that is specifically developed for application delivery. Both BIG-IP Edge Gateway and BIG-IP APM offer all the SSL VPN functionality found in FirePass, but on the BIG-IP platform.

ps

Resources:

- 2011 Gartner Magic Quadrant for SSL VPNs
- F5 Positioned in Leaders Quadrant of SSL VPN Magic Quadrant
- SOL13366 - End of Sale Notice for FirePass
- SOL4156 - FirePass software support policy
- Secure Access with the BIG-IP System | (whitepaper)
- FirePass to BIG-IP APM Migration Service
- F5 FirePass to BIG-IP APM Migration Datasheet
- FirePass Wiki Home
- Audio Tech Brief - Secure iPhone Access to Corporate Web Applications
- In 5 Minutes or Less - F5 FirePass v7 Endpoint Security
- Pete Silva Demonstrates the FirePass SSL-VPN

Technorati Tags: F5, infrastructure 2.0, integration, cloud connect, Pete Silva, security, business, education, technology, application delivery, intercloud, cloud, context-aware, infrastructure 2.0, automation, web, internet

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