White Paper

Secure Access with the BIG-IP System

Rapid growth of the mobile and remote workforce is driving organizations' need to support tens of thousands of concurrent users on a single appliance. To this end, F5 developed a high-performance, high-concurrency SSL VPN in BIG-IP Edge Gateway and BIG-IP Access Policy Manager (APM) to help enterprise IT migrate existing remote access solutions.

by Peter Silva
Technical Marketing Manager, Security

Contents

Introduction

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® 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, 35 percent of the worldwide workforce will be remote and therefore mobile—that's 1.2 billion people.[1] 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.

[1] IDC Report, "Market Analysis: Worldwide Mobile Worker Population 2009–2013 Forecast". December 2009, IDC #221309, Volume 1.

History of the FirePass SSL VPN

SSL VPNs Take Off

F5's first foray into the SSL VPN realm was with its 2003 purchase of uRoam and its flagship product, FirePass. Although the VPN and firewall market was still small, Infonetics Research predicted it would swell from $34 million in 2002 to $393 million by 2005. 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-ons 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 product. Over the years, FirePass has led 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.

In today's workplace, primary business resources, including data centers, applications, employees, and customers, are all shifting outside the traditional business perimeter. BIG-IP APM protects public-facing applications by providing policy-based, context-aware access to users while consolidating access infrastructure.

BIG-IP APM offers multi-gigabit per second SSL encryption throughput with HTTPS and supports hundreds of logins per second. A single high-end appliance with the BIG-IP APM module can scale to support tens of thousands of concurrent users and provide simplified access and control to users in hosted virtual desktop environments.

BIG-IP APM also enables organizations to manage access based on identity. It unifies remote, web, and application access. BIG-IP APM integrates with an organization's AAA (authentication, authorization, and accounting) servers to give users fast authentication and single sign-on to other applications within the infrastructure. Its powerful reporting engine gives administrators a holistic view of access, and application analytics offer unique insight into not only application behavior, but the user experience as well.

BIG-IP Edge Gateway

BIG-IP Edge Gateway is a standalone appliance that provides all the SSL VPN remote access security benefits of BIG-IP APM—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.

SharePoint:

	Competitor SSL VPN	BIG-IP Edge Gateway	Δ
First Access	211 seconds	114 seconds	1.9x
Repeat	47 seconds	16 seconds	2.9x

SAP:

	Competitor SSL VPN	BIG-IP Edge Gateway	Δ
Access	111 seconds	14 seconds	7.9x

Figure 1: When F5 tested a first-time user's attempt to download a 4 MB document (SharePoint) and a 27 MB Microsoft Office file (SAP), the result was faster portal file downloads with BIG-IP Edge Gateway.

BIG-IP Edge Gateway gives organizations unprecedented flexibility and agility to consolidate all their secure access methods on a single device.

Acceleration and optimization

With users and resources distributed around the world and often on the move, latency can also be a challenge. Ideally, users' requests would be addressed immediately—but this can be tricky with users and applications on opposite sides of the globe. Varying locations and networks can cause packet loss and poor performance, which can have a detrimental effect on application performance and user experience. It can sense and adjust to haphazard network conditions by adding compression and other optimizations to ensure a pleasant user experience. BIG-IP Edge Gateway combines remote access and optimization services on a single BIG-IP platform; these services can be used for data centers, POPs, remote sites hosting applications for mobile users, and remote branches accessing those applications.

Quality of service, particularly with VoIP, is another challenge for mobile and remote users. BIG-IP Edge Gateway offers a Datagram TLS (DTLS) mode for remote connections. TLS is the standard protocol used for securing TCP-based Internet traffic (also known as SSL); and DTLS is a protocol based on TLS that can secure the datagram transport. It is well-suited for securing and tunneling applications that are delay-sensitive. This solution reduces the required hardware in locations that may have delay-sensitive networks; provides effective application access management; and greatly improves user experience.

TMOS

BIG-IP Edge Gateway and BIG-IP APM run on F5's TMOS®, a modular operating system and the universal product platform shared by all BIG-IP products. With its application control plane architecture, TMOS provides intelligent control over the acceleration, security, and availability services applications require. TMOS establishes a virtual, unified pool of highly scalable, resilient, and reusable services that can dynamically adapt to changing conditions in data centers and virtual and cloud infrastructures.

TMOS also offers the flexibility and extensibility of F5 iRules® and iControl®. The iRules scripting language provides organizations with unprecedented ability to directly manipulate and manage any IP application traffic. iRules utilizes an easy-to-learn syntax that enables IT organizations to customize how they intercept, inspect, transform, and direct inbound or outbound application traffic. Using iRules, network professionals can:

- Deter newly discovered security threats.
- Halt phishing attacks.
- Stop spam email.
- Route traffic to specific servers, based on packet content.

With the iControl API, organizations can give their software the ability to control its own application traffic. Using iControl, application programmers have devised solutions that:

- Bring new servers online and offline dynamically, as needed.
- Give priority to critical traffic during sudden traffic bursts.
- Filter out unwanted traffic.
- Distribute software updates to individual servers without affecting overall service.
- Manage total delivery of all applications from a single console.

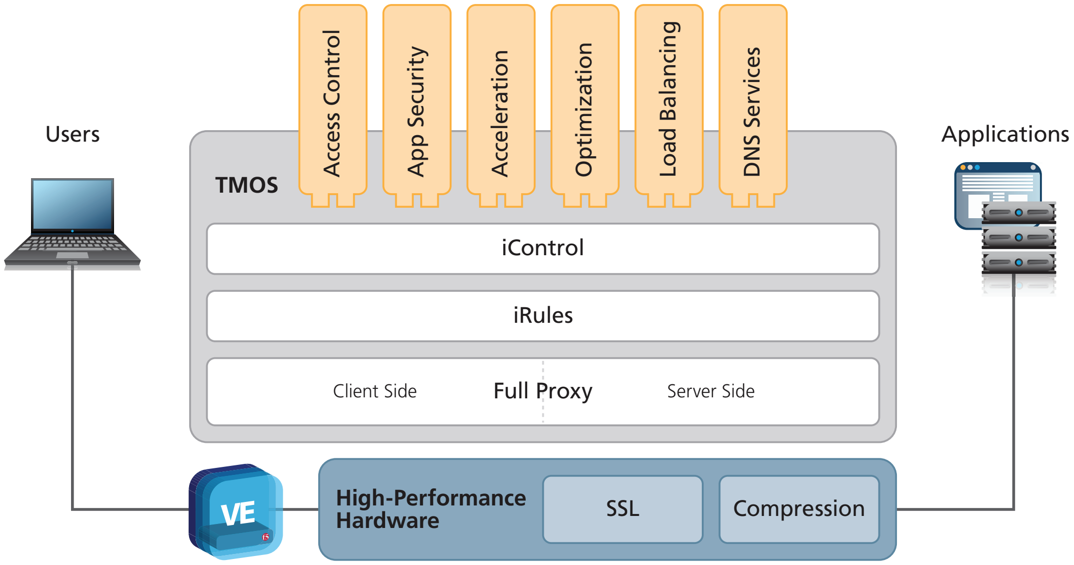


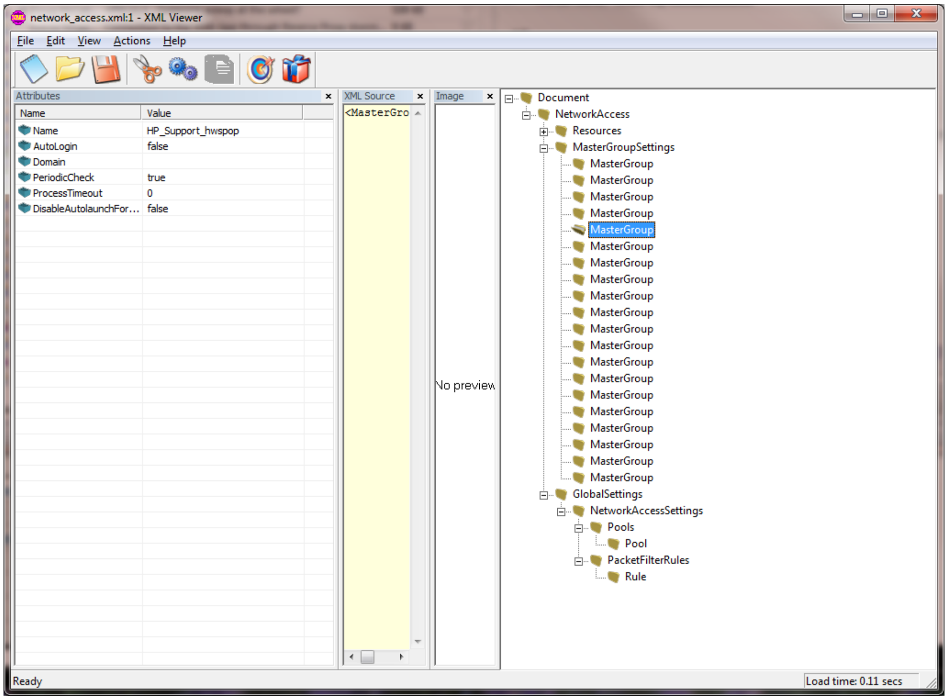
Figure 2: The TMOS operating system is the foundation of the BIG-IP system and a unified system for application delivery.

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.


network_access.xml:1 - XML Viewer
File Edit View Actions Help
Attributes
XML Source
Image
No preview
Ready
Load time: 0.11 secs

Name	Value
Name	HP_Support_hwspop
AutoLogin	false
Domain	
PeriodicCheck	true
ProcessTimeout	0
DisableAutolaunchFor…	false

```
<MasterGro
```

```
Document
  NetworkAccess
    Resources
    MasterGroupSettings
      MasterGroup
      MasterGroup
      MasterGroup
      MasterGroup
      MasterGroup
      MasterGroup
      MasterGroup
      MasterGroup
      MasterGroup
      MasterGroup
      MasterGroup
      MasterGroup
      MasterGroup
      MasterGroup
      MasterGroup
      MasterGroup
      MasterGroup
      MasterGroup
      MasterGroup
      MasterGroup
    GlobalSettings
      NetworkAccessSettings
        Pools
          Pool
        PacketFilterRules
          Rule
```

Figure 3: Exported FirePass XML file view.

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.

Conclusion

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. BIG-IP APM provides secure, context-aware, policy-based SSL VPN access control in a module that can be added to BIG-IP LTM. BIG-IP Edge Gateway provides all the benefits of BIG-IP APM but is a standalone appliance, and can also accelerate and optimize applications at the edge of the network—all in one efficient, scalable, and cost-effective solution. It centralizes and simplifies AAA management directly on the BIG-IP system. Both provide the scale, performance, and optimization needed for today's mobile workforce.

F5 Networks, Inc. 401 Elliott Avenue West, Seattle, WA 98119 888-882-4447 www.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