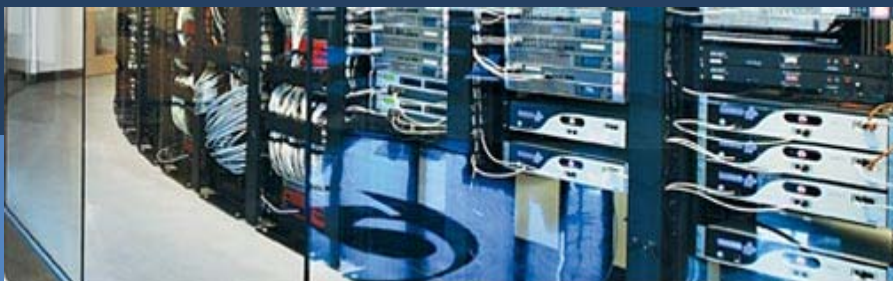




F5 BIG-IP[®] Edge Gateway[™]

**IT Agility that Drives
Business Forward**



**Richard Stienon
Chief Research Analyst**

Introduction

There are six factors that drive the ever changing information technology space:

- Growth in Users
- Bandwidth
- Processing Power
- Applications
- Mobility
- Security Threats

All of these trends have been shown to be exponential. Yet given these changes, products tend to lag giving rise to new innovation, new products, and new vendors. Invariably, the first generation of technology does not grow with the increasing demand for bandwidth, applications, and mobility, or the increasing exposure of IT infrastructure to new threats. Thus it is no surprise that secure remote access platforms are undergoing a revolution that has led to a next generation of products that meet those demands.

There were IPSec VPN concentrators that made possible secure connectivity for remote and mobile users using the same technology that enabled site to site encrypted tunnels. That first generation of products was conceived to facilitate access to corporate email and file systems. They were produced by Nortel and Cisco and other companies that are long gone such as TimeStep and FTP Software. But those devices relied on IPSec, a strong encrypted tunnel, which had enrollment, certificate management, and interoperability issues. It was much easier to just use the inherent simplicity of the SSL certificates in every browser. This gave birth to the first generation of SSL VPN remote access devices and a flurry of acquisitions that enabled most network security vendors to add SSL VPN for remote access to their product portfolios. One sign of the commoditization of SSL VPN solutions is that they are now bundled into

F5 Secure Accelerated Remote Access

- **BIG-IP® Edge Client™**
- **Smart Connection: location awareness and auto-connect**
- **Windows logon credential reuse**
- **Endpoint security and customization**

offerings from every UTM vendor which makes simple remote access available to the smallest organization

As technologies become features in all purpose appliances the more sophisticated applications for those technologies are often under served. This paper stresses that changes to corporate computing environments brought on by a move to private and public cloud delivery of services have created a need for a more robust secure remote access solutions. These purpose-built, dedicated devices fulfill a mission critical role by providing robust, always-on, connectivity with application acceleration and security.

Rise of Web Apps, Data Center, and the Cloud

Like all things digital there are overriding growth trends that drive demand for more and more functionality, reliability, resilience, throughput, security, manageability, and reporting, at all layers of IT infrastructure. What are the key drivers that demand innovation in secure remote access?

Growth of Applications

Increased use of hosted apps, either within the data center or in the cloud, is the primary driver for technology and new products in the secure remote access space. Enterprise computing has quickly transitioned to hosted central applications with a web front end accessed from anywhere via a web browser. As mission critical business functions make that transition a new focus on robust secure remote access is required to ensure always-on connectivity.

Third party applications including CRM (salesforce.com), supply chain management (ariba.com), financials (NetSuite.com) employee payroll, and bank treasury functions are replacing traditional in-house software. Distributed environments like Citrix Xenapp, Citrix Desktop, and VMWare View, create a desktop environment delivered from central servers yet they do

F5 Secure Accelerated Remote Access

- **Virtual keyboard support**
- **Protected workspace support and encryption**
- **Network, application, and content rewrite access**
- **Credential caching and proxying for SSO**

not provide desktop like performance. End users have to get access to these applications in a secure and reliable manner without administrators losing control of that access.

Increased Mobility

Teleworkers and mobile users are the other key driver. As devices proliferate (laptops, Blackberrys, iPhones, iPads) there is more demand for centrally administered and monitored access to the proliferation of applications and data they need to conduct every day business. In addition to the proliferation of devices the mobile workforce is encountering an increasingly complex network where access from public hot spots, home broadband, 4G networks, and any combination of those is required. This drives the need for improvements in the way connections are made, authenticated, secured, and optimized. Mobile users familiar with a LAN like experience in the office are requesting a better user experience spurring the need for application acceleration technology with remote access.

Increased Threats

As critical applications and the data they work with get moved into the cloud they become subject to targeted attacks from cyber criminals, malicious insiders, and even state sponsored espionage. Controlling access to that information – always critical– becomes even more important as they are moved to cloud environments.

F5 Secure Accelerated Remote Access

- **Advanced Visual Policy Editor**
- **Comprehensive remote access authentication**
- **External logon page support**
- **Authorization – dynamic L4 and L7 ACL policy enforcement**

Next Gen SSL VPN

The next generation of secure remote access appliances has to be built with the following capabilities because of the rising tide of applications and the move to the cloud.

Robust Authentication and Connectivity from Anywhere in the World

An increasingly mobile workforce means that access must be easy from anywhere in the world and that low latency and high bandwidth cannot be assumed. That means that next gen secure remote access solutions will take steps to ensure that getting connected is simple, reliable, and automatic. The end-user interaction with the SSL client has to be minimal to avoid help desk calls and a frustrated user base. If the organization has deployed SSL appliances globally the employee on the move should automatically connect to the nearest device that provides the lowest latency and best throughput.

Acceleration

Application response must be accelerated to improve performance. Just securing a connection with SSL or IPSec is not enough to support user demand for LAN like performance. Stand alone web application acceleration appliances are being deployed today in front of data centers to improve performance in remote offices in the same way IPSec devices were deployed to provide VPN tunnels. But the mobile user also needs that acceleration. Application acceleration between the end point and the data center, or multiple data centers, will vastly improve the end user experience and contribute to overall business productivity.

Management/Policy

Granular policy controls for each user and group must be easy to configure and control. Policies that change based on geo-location, time of day, and context have to be monitored and attempted violations tracked and logged for advanced reporting. Layer 7 ACLs (Access Control Lists) give the security administrators another control point where they can determine who has access to which applications, even down to controlling who can use

F5 Secure Accelerated Remote Access

- **Group policy support and integration**
- **Geolocation agent in Visual Policy Editor**
- **Integration with Oracle Access Manager**
- **Acceleration/optimization services**

particular components of applications. In this way engineering cannot see HR functions, and sales people are restricted just to the access they need.

Dynamic Connectivity

Other features that enhance the ease of use are the ability to roam between networks, be it various Wi-Fi access points, multiple broadband connections, or LAN segments while maintaining active sessions. Automatic connection that does not require user participation takes the decision process out of the user's hands and allows additional security controls to be put in place including routing of web requests to third party apps in the cloud.

AAA Integration and Web Single Sign On

Quick and easy integration with existing authentication mechanisms is required with next gen remote access solutions; including Radius, and Windows Domains. Control of the web layer will give administrators additional ability to protect the end user as well as corporate data. Web single sign on can be easily accomplished. The user provides their login credentials and is granted access to internal resources as well as those third party apps. Strong authentication via tokens can be invoked at initial connection and stronger passwords can be used for common third party applications through proxying. This gives administrators better revocation control as well. When an employee departs a company, revoking their remote access credentials will prevent them from accessing their salesforce.com account for instance.

F5 Secure Accelerated Remote Access

- **Dynamic data compression, D-TLS (Datagram-based TLS) and application QoS**
- **Client-side traffic shaping for Windows**
- **Asymmetric and symmetric network and application acceleration**
- **Support for CIFS and MAPI acceleration**

Conclusion

Early deployments of standalone appliances that aggregated IPSec or SSL VPN are not sufficient to meet the demands of a rapidly evolving network eco-system. As cloud based mission critical applications grow so too will the enterprise demands for robust remote connectivity.

The next generation of secure remote access solutions will be built on robust network gear delivered by vendors with experience in high availability, redundancy, application performance enhancement, and manageability. The solutions will scale to handle thousands of end users and provide them with transparent ease of use while securing their access and accelerating application performance.

This white paper was produced with the sponsorship of F5

References:

F5 Tech Demo The BIG-IP® Edge Client™

<http://devcentral.f5.com/weblogs/dctv/archive/2010/02/22/f5-tech-demo-the-big-ip-edge-client.aspx>

F5 Optimizes User Experience and Secure Access with New Solution for VMware View™ 4.5

<http://www.f5.com/news-press-events/press/2010/20100831a.html>

Unified Access and Optimization with F5 BIG-IP Edge Gateway

<http://www.f5.com/pdf/white-papers/unified-access-edge-wp.pdf>

BIG-IP Edge Gateway product overview

<http://www.f5.com/pdf/products/big-ip-edge-gateway-overview.pdf>

F5 Secure Accelerated Remote Access

- **Caching, compression, and data de-duplication**
- **L7 Rate Shaping™**
- **BIG-IP® Global Traffic Manager™ integration**
- **iRules™**