F5 White Paper

Unified Access and Optimization with F5 BIG-IP Edge Gateway

Integrating security, availability, and application acceleration services to enable context-aware networking.

by Peter Silva
Technical Marketing Manager

Contents

Introduction

The 1987 movie Planes, Trains and Automobiles follows Neal Page as he tries to get home for Thanksgiving by any means possible and despite all the setbacks he encounters along with way. Del Griffith, the jovial shower curtain salesman who tags along with Neal, only adds to the incidents that make the trip long, hard, and full of delays. Now, more than 20 years later, the title could be Planes, Trains, Automobiles, Buses, Coffee Shops, Airports, and Everywhere Else, which would aptly describe all the different locations, devices, and networks people use to get "home," or, in other words, connect to their corporate network. Just as Del inhibits Neal from easily reaching his "home network," quality of service, network threats, slow connections, and complex deployments challenge our access to our "home enterprise" networks.

The mobile workforce is expected to increase from 758.6 million in 2006 to 1.0 billion in 2011, a figure that represents 24.8 to 30.4 percent of the worldwide workforce[i] and approximately 50 to 60 million teleworkers solely in the United States. Employers disperse their workers all over the globe with a variety of trusted and un-trusted devices that are used to request access to corporate resources from different types of networks. Users need fast, secure, and reliable access to the corporate infrastructure. Simultaneously, IT departments struggle with multi-vendor access solutions and systems, enforcement of policies, regulation of access, security threats and vulnerabilities, and ensuring that the right user is connecting to the proper applications based on context. If all that weren't enough, IT departments also need to ensure that content is delivered quickly, reliably, and securely—while keeping management and maintenance costs in line. The enterprise needs unified and converged access and policy management in a globally distributed environment, for wireless and public connections. Managed service providers (MSPs) need to differentiate themselves by offering their customers a customized look and feel for their service offerings and MSPs need to virtualize their environments to maximize investment.

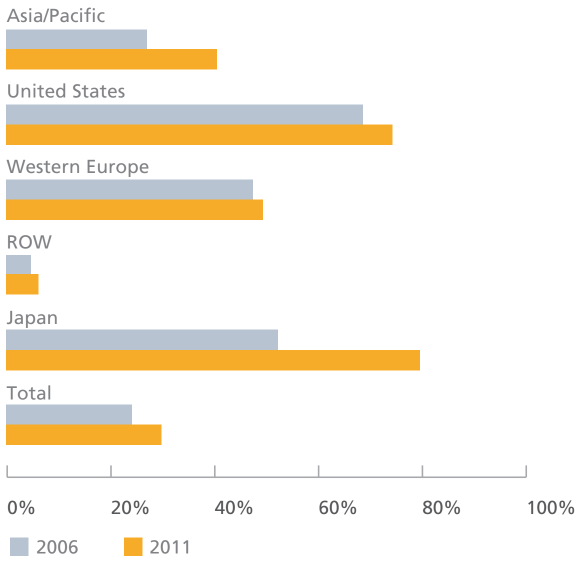

Figure 1. Worldwide mobile workforce penetration by region, 2006 and 2011.

The days of expensive, single-point products that only provide an isolated solution are waning, and customers are now looking to consolidate their deployments for easier management and better return on investment (ROI) and total cost of ownership (TCO). Unified, optimized, and secure access is what customers need.

The Enterprise

Access Challenges

Enterprises have long struggled with single-point, multi-vendor security solutions for remote, LAN, or wireless access modes. They will deploy IPsec or a SSL VPN for remote teleworkers, Network Access Control (NAC) for LAN-based control, and WiFi Protected Access (WPA) or other wireless encryption for their WiFi access points. With multiple, varying application entry points, it can be difficult to maintain a consistent security policy across all access points and expensive to manage multiple systems. Current IPsec solutions might only be available for certain endpoint devices and usually require a pre-installed client and configuration to work properly. SSL VPN, while advantageous for quick deployments and endpoint checks, can be limited in performance once you reach a certain threshold. NAC solutions don't adequately protect important corporate applications or data since they typically just authenticate the user and might only assign a particular network segment. Different users need to access different, and often restricted, corporate resources; yet, L2-L3 access control lists (ACLs) inherently do not control access to applications, and wireless access points are often wide open for connection by any user. If the WiFi access point does use security, it's usually the same 802.1x technology as NAC, so many of the same pitfalls can still haunt IT departments.

IT organizations can also find it difficult to control the endpoint security posture of the different types of machines requesting access to applications. Companies are sharing more data as part of their value chain, and having access to sensitive partner resources is critical to that exchange of information. While corporate-issued, trusted machines must abide by a mandated security policy, partners, contractors, and other business associates might not have the same requirements or restrictions when they are requesting access. Additionally, it might be difficult or forbidden to push security policies to non-corporate devices. Users want seamless access and ease of use without having to employ multiple solutions. Support costs can escalate when users are frustrated; business can suffer when workers are unable to complete their tasks. And, ultimately, the corporate network is not completely secure.

Global Distribution

When users are all over the world, globally distributed access across several data centers can help solve access and availability requirements, but both the user base and IT administrators still need a solution that is easy to use and simple to manage. At the same time, the worldwide strain on budgets is forcing customers to reduce the number of data centers while still offering fast and secure application performance to the global user base. Content delivery networks (CDNs) can place certain objects at the edge of the network for fast access, but the cost of entry for using a traditional CDN can be prohibitive for small-to-medium-size businesses. There are also security and control concerns with traditional CDNs because some content is shared, which can be perceived as a potential risk to the business. The asymmetric acceleration used in CDNs does little to impress first-time visitors: large media (video/audio/ISO) files are being distributed and requested more than ever over both HTTP and FTP, and there are few things more frustrating than waiting on a file to slowly make its way to your desktop, especially if it is critical and you need it now. Lastly, depending on the location and network of both your users and the applications they use, issues like latency, packet loss and poor performance can have a detrimental effect on the user experience.

Managed Service Providers

Many small-to-medium-size businesses might not have the resources to manage their own secure access deployments, so they turn, instead, to MSPs. A good number of MSPs offer remote access solutions, and while they have moved away from offering IPsec due to the deployment challenges, they still offer a SSL VPN solution. Customization is important to both MSPs and customers alike: MSPs need to differentiate their offerings while providing the customer with their unique company logo, color scheme, host names, and more—with which customers are familiar and comfortable.

MSPs also need virtualization functionality to maximize their investment. The ability to host multiple customers on the same unit, with the segregation needed for security, can provide the economies of scale necessary for ROI.

Secure and Accelerated Access

Productive Users with Fast, Secure, and Consolidated Access

The ability to converge and consolidate all three access modes—remote, LAN, wireless—on a single management interface and provide easy-to-manage access policies saves money and frees up valuable IT resources. With F5® BIG-IP® Edge Gateway™, secure, consolidated, speedy access with readily managed policies on the same device is now a reality. BIG-IP Edge Gateway supports any endpoint that has a browser and provides the security and performance equivalent to or greater than IPsec. BIG-IP Edge Gateway uses SSL technology and brings together access security, acceleration, and application availability services to enable context-aware, policy-controlled, secure access to applications that provides LAN speed performance for remote users. The built-in SSL VPN provides access that is robust, easy to deploy and manage, and secure without the performance drawbacks of traditional SSL VPNs. Adding to this, an integrated client provides a broader and less expensive solution to policy-based access management and improved application performance for remote users. Its ability to support up to 40,000 users with flexible access control, dynamic policy enforcement, centralized policy management, integrated endpoint security checking, and integrated application acceleration makes BIG-IP Edge Gateway perfect for any deployment scenario.

BIG-IP Edge Gateway increases the security of applications by driving identity and access management into the network, and it drives down bandwidth costs by optimizing access to applications. By bringing these services together and driving user and group identities into the network, policy and service levels can be set based on role. This makes the Internet and cloud computing faster, more predictable, and more secure for the enterprise.

The BIG-IP Edge Gateway protects applications with L4 and L7 ACLs to control network access and application access at a fine-grain level. The BIG-IP Edge Gateway is application aware, which enables you to control access down to the specific path within an application, securing areas that might otherwise have role-based restricted access. F5's endpoint inspection can be added into any access control decision and is managed with the unique Visual Policy Editor (VPE). The VPE is a human readable flowchart used for end-to-end policy definition. Implementing a complex security policy on a remote access product can be difficult to accomplish accurately, and, as a result, administrators will often either decide not to implement a policy or spend inordinate amounts of time doing it. With VPE, both of these issues are addressed, leading to better security and higher productivity.

The BIG-IP Edge Gateway VPE adds full control over creating and managing policies that govern authentication, authorization, and resource management. With the tremendous and ongoing growth in the number of telecommuters and mobile users, it is critical that organizations ensure that endpoint devices are secure and compliant. BIG-IP Edge Gateway accomplishes this with a group policy enforcement feature that provides policy-based endpoint security to any remote user, inside or outside a Microsoft Active Directory domain for a fully integrated endpoint solution. A choice of templates is also available to suit many particular policy requirements. These pre-built templates are unique and can benefit enterprises that must comply with regulatory or industry requirements such as PCI, HIPAA, or GLBA. You can also initiate a protected workspace or virtual desktop to limit data loss prevention by ensuring no files or data are left behind on a PC or device.

To streamline secure access, the new BIG-IP Edge Client™ solution can automatically detect when a VPN connection is required via the smart connection technology feature on BIG-IP Edge Client without user intervention. When users disconnect from their primary work domain—for example, when users need to unplug their laptops to work elsewhere—and connect to an open WiFi signal, the BIG-IP Edge Client smart connection technology feature will automatically detect that users are no longer on a trusted network and will immediately initiate an encrypted tunnel. Automatic detection saves users time and frustration since they can continue whatever they were doing securely and without manual intervention.

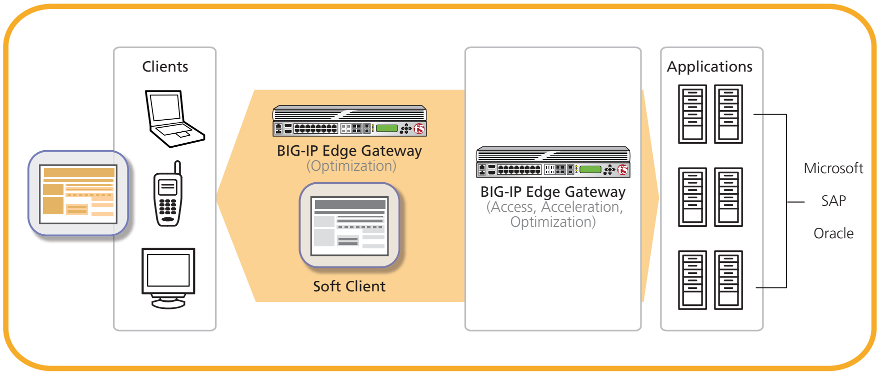

Figure 2. BIG-IP Edge Gateway combines symmetric, asymmetric, and client-based acceleration.

Global Solution

Today, with users who are spread around the world, connecting with mobile devices on over-the-air networks or sitting in branch offices that may have limited or varying bandwidth, application performance is not always acceptable. Depending on the network and location, network latency is always a concern—especially in emerging markets. The BIG-IP Edge Gateway integrated WAN optimization and web acceleration minimizes the impact of latency without building a data center or co-locating equipment in a particular region. BIG-IP Edge Gateway optimization services can be used for data centers, POPs, remote sites hosting applications for mobile users, and for remote branches accessing those applications.

Quality of service, particularly with VoIP, is another challenge facing mobile and remote users. BIG-IP Edge Gateway offers a solution with a Datagram TLS (DTLS) mode for remote connections. TLS is the standard protocol used for securing TCP-based Internet traffic (also known as SSL). DTLS is a protocol based on TLS that is capable of securing the datagram transport. DTLS is well suited for securing applications that are delay sensitive (and hence use datagram transport), tunneling applications such as VPNs, and applications that tend to run out of file descriptors or socket buffers. Combining the remote access and optimization services onto a single BIG-IP platform reduces the hardware necessary in these locations, minimizing risk and consolidating infrastructure. Access to applications is effectively managed, while the performance of multiple applications is greatly improved.

BIG-IP Edge Gateway is also integrated with BIG-IP® Global Traffic Manager™ (GTM), so as individual BIG-IP Edge Gateway devices reach certain thresholds, BIG-IP GTM can load balance users to the next best BIG-IP Edge Gateway (without users noticing) and provide emergency capability when needed. Disaster recovery, business continuity, and workforce continuity accomplished all in one unit!

MSPs' Perfect Match

For small-to-medium-size companies with limited IT resources, a MSP can be a great resource in accomplishing IT-intensive or complex deployments. Since there are many MSPs to choose from, each must differentiate themselves by offering unique services. With BIG-IP Edge Gateway, MSPs can virtualize each customer environment to create multiple virtual BIG-IP Edge Gateway instances and customize all the user-facing content, including logon pages, errors, end pages, and more. Segmenting customers keeps sensitive information in the right hands and helps administrators tailor the offerings for their users. For instance, virtual routing and VPE permit a unique and separate access policy for each end customer. Not only can MSPs offer remote access services to their customers, but data center and cloud providers can also deploy these services as part of their own infrastructure, enabling segmented access to and management of each customer's unique environment. While many MSPs do offer portals through which customers can remotely manage their equipment, BIG-IP Edge Gateway can offer greater security. For example, after the customer authenticates, you can create an encrypted tunnel so they can be directly connected to their system environment. A unique customer portal can also be created offering strong authentication over and above simple HTTP or form-based authentication over the Internet. In addition, if the customer also has a BIG-IP device running v 10.1, encrypted and optimized tunnels can be created between the provider's and customer's BIG-IP deployment to allow the customer to upload data directly to its environment over a secure, optimized tunnel. Acceleration technology in BIG-IP Edge Gateway helps MSPs differentiate services—access or access and acceleration—depending on the packages they offer.

Conclusion

We've come a long way since Neal's fateful trip 22 years ago but the goal is still the same—connect back home. While we now carry devices that help us stay in contact with friends, family, business associates, trusted networks, and needed applications, challenges still exist. BIG-IP Edge Gateway offers a unique set of features, market-leading capacity and performance, enticing TCO, and ROI value. BIG-IP Edge Gateway integrates with existing enterprise infrastructure and applications while simultaneously providing authentication, authorization, and access to networks, applications and portals. The comprehensive endpoint security helps make corporate compliance easier. Dynamic access using asymmetric and symmetric acceleration and optimized sessions with caching, compression, and de-duplication gives users the highest performance available in the market. Scalability, acceleration, optimization, performance and reliability, and support for a wide range of clients, applications, and infrastructure give IT departments the management and consolidation features needed for critical environments.

BIG-IP Edge Gateway is a game changer in the secure connectivity market, providing the next generation of highly scalable integrated remote access and advanced acceleration capabilities. BIG-IP Edge Gateway brings together necessary edge services, remote access, site-to-site security, WAN optimization, and web acceleration. BIG-IP Edge Gateway gives you secure, accelerated, and highly available applications around the world—whether at home on the road.

.

[i] Source: IDC: Worldwide Mobile Worker Population 2007-2011 Forecast

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
info.asia@f5.com

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

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