Securing the Cloud

Cloud computing has become another key resource for IT deployments, but there is still fear of securing applications and data in the cloud. With F5 devices, you can keep your most precious assets safe, no matter where they live.

White Paper

by Peter Silva

Introduction

While companies certainly see a business benefit to a pay-as-you-go model for computing resources, security concerns seem always to appear at the top of surveys regarding cloud computing. These concerns include authentication, authorization, accounting (AAA) services; encryption; storage; security breaches; regulatory compliance; location of data and users; and other risks associated with isolating sensitive corporate data. Add to this array of concerns the potential loss of control over your data, and the cloud model starts to get a little scary. No matter where your applications live in the cloud or how they are being served, one theme is consistent: You are hosting and delivering your critical data at a third-party location, not within your four walls, and keeping that data safe is a top priority.

Proceeding into the Cloud with Caution

Most early adopters began to test hosting in the cloud using non-critical data. Performance, scalability, and shared resources were the primary focus of initial cloud offerings. While this is still a major attraction, cloud computing has matured and established itself as yet another option for IT, more data—including sensitive data—is making its way to the cloud. The problem is that you really don't know where in the cloud the data is at any given moment. IT departments are already anxious about the confidentiality and integrity of sensitive data; hosting this data in the cloud highlights not only concerns about protecting critical data in a third-party location but also role-based access control to that data for normal business functions.

Organizations are beginning to realize that the cloud does not lend itself to static security controls. Like all other elements within cloud architecture, security must be integrated into a centralized, dynamic control plane. In the cloud, security solutions must have the capability to intercept all data traffic, interpret its context, and then make appropriate decisions about that traffic, including instructing other cloud elements how to handle it. The cloud requires the ability to apply global policies and tools that can migrate with, and control access to, the applications and data as they move from data center to cloud—and as they travel to other points in the cloud.

Cloud computing is a style of computing in which dynamically scalable and often virtualized resources are provided as a service. Users need not have knowledge of, expertise in, or control over the technology infrastructure in the "cloud" that supports them. Furthermore, cloud computing employs a model for enabling available, convenient, and on-demand network access to a shared pool of configurable computing resources for example, networks, servers, storage, applications, services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

F5 Networks Cloud Survey, August 2009

The Role of Application Delivery

Generally speaking, F5 solutions all focus on application delivery. Given that the ultimate goal of any cloud, regardless of model or location, is to deliver applications in the most efficient, agile, and secure way possible, F5 solutions are relevant when it comes to building out cloud infrastructure. This is particularly true since application delivery requires the same strategic points of control that the dynamic control plane of cloud architecture necessitates, and it must provide the same capability to intercept, interpret, and instruct.

While a cloud certainly requires a variety of components (many of which are not within F5's domain) to create an environment capable of providing scalability, the infrastructure solutions that pertain to application delivery are germane to F5's area of expertise. These infrastructure solutions provide the scalability, extensibility, adaptability, manageability, security, mobility, and real-time performance required in the dynamic control plane.

F5's focus on providing intelligent and strategic points of control utilizing proxies (intercept), policies (interpret/instruct), and services (interpret/instruct) in a unique, modularized delivery infrastructure is well suited to handling the high-volume traffic associated with cloud computing. F5 solutions can be deployed on a wide range of hardware platforms, offering flexibility in overall capacity and performance that enables mid- and large-size organizations, as well as service providers, to choose an application delivery or data solution that is tailored to meet the unique needs of the organization.

The F5-Secured Cloud

While you might equate the F5 BIG-IP Local Traffic Manager (LTM) Application Delivery Controller with advanced load balancing, it also inspects all inbound and outbound application content. Additionally, BIG-IP LTM is a powerful security tool that thwarts network- and application-based protocol attacks. Out of the box, BIG-IP LTM protects both the applications being delivered from it and the network to which it is attached. And, BIG-IP LTM offers a unified approach to security solutions, which include, but are not limited to, packet filtering, port lockdown, denial of service (DoS) attack protection, network/administrative isolation, protocol validation, rate shaping, SSL termination, and more.

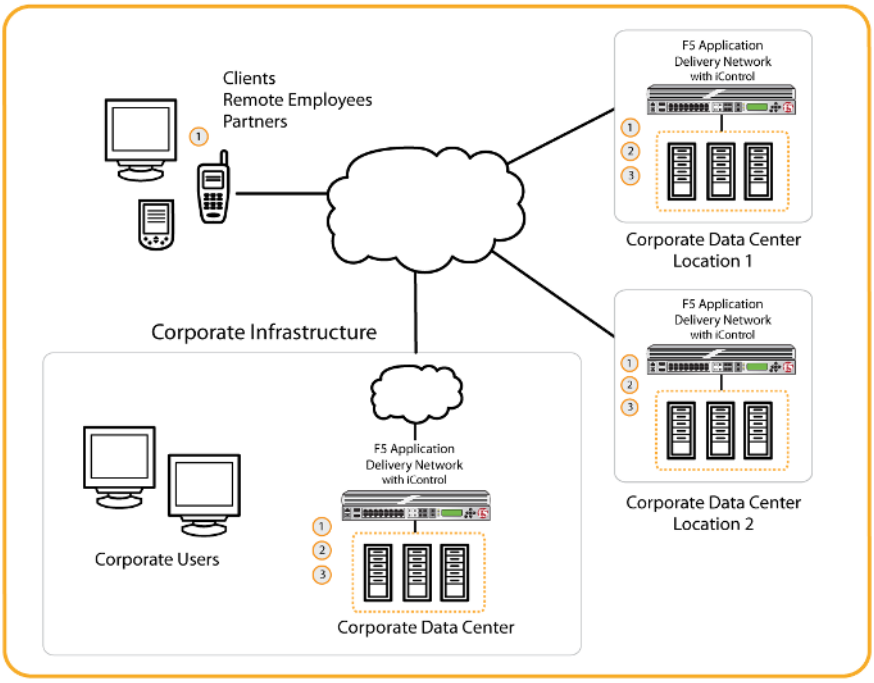
While this is an impressive list of security advantages, there are attacks that cannot be detected by either network devices or the application itself, and, increasingly, thieves are going after the application data via web-based attacks. Since layer 7 DoS attacks, XSS, SQL injections, and brute-force attacks can easily compromise a web application, additional security measures must be put in place.

F5 BIG-IP Application Security Manager (ASM), a web application firewall, not only protects against common vulnerabilities such those listed in the OWASP Top 10, but it also tightens control over the data with fine-grained policies. BIG-IP ASM Application Security templates for many popular applications enable you to quickly deploy application security with the optimal settings. With BIG-IP ASM, the ability to control who has access to the data, the type of data available, and if the data can be exchanged, as well as the ability to obtain detailed logs and reporting, helps you meet regulatory compliance mandates—even in the cloud. BIG-IP ASM offers additional protections such as scrubbing of social security numbers, credit card numbers, and the content in other custom fields; as well as masking sensitive data, selective encryption of server cookies and password fields, directory-level or file-type restrictions, and resource cloaking to hide your IIS server's version information.

One of the biggest areas of concern for both cloud vendors and customers alike is strong authentication, authorization, and encryption of data to and from the cloud.

Users and administrators alike need to be authenticated—with strong or two- factor authentication—to ensure that only authorized personnel are able to access data. And, the data itself needs to be segmented to ensure there is no leakage to other users or systems. Most experts agree that AAA services along with secure, encrypted tunnels to manage your cloud infrastructure should be at the top of the basic cloud services offered by vendors. Since data can be housed at a distant location where you have less physical control, logical control becomes paramount, and enforcing strict access to raw data and protecting data in transit (such as uploading new data) becomes critical to the business. Lost, leaked, or tampered data can have devastating consequences.

Here too, F5 can help both the vendor and customer with solutions like BIG-IP Edge Gateway and BIG-IP Access Policy Manager (APM). BIG-IP Edge Gateway uses SSL technology to bring together access security, acceleration, and application availability services to enable context-aware, policy-controlled, secure, and optimized access to applications. BIG-IP APM is a flexible, high-performance access and security platform; with it you can manage access to networks and applications by implementing solid security policies. By bringing these services together and driving user and group identity into the network, policy and service levels can be set based on identity and location. Access based on context makes the Internet, and the cloud, a faster, more predictable, and more secure network for the enterprise, which is especially beneficial for mobile users and IT administrators.



1. Secure remote access technology provides contextual, secure access to cloud-based applications with minimal client management overhead.
2. Web application firewalls provide the means to centralize application security, improving performance and securing applications against myriad threats in the cloud.

   Network-side scripting offers an agile, immediate method of addressing security vulnerabilities on an on-demand basis, requiring little or no downtime and no changes to the application.
3. Administrative domains isolate configuration and management for fine-grained control over access to cloud computing infrastructure.

   VLAN support offers application traffic isolation for improved security of application data, utilizing shared resources.

Figure 1: The F5-secured cloud offers comprehensive protection from client to cloud.

Mobile users who are scattered around the globe need fast, secure access to applications; IT administrators need to manage cloud architecture and cloud applications. BIG-IP Edge Gateway and BIG-IP APM are packed with security features to meet the needs of both mobile users and IT administrators.

Secure services based on SSL VPN offer endpoint security, giving IT administrators the ability to see who is accessing the organization and what the endpoint device's posture is to validate against the corporate access policy. Strong AAA services, L4 and L7 user Access Control Lists, and integrated application security help protect corporate assets and maintain regulatory compliance. Availability services give administrators global traffic management capabilities to direct users to the best site based on location, L2-L4 switching, integrated routing, and an IPv6 gateway. Acceleration services offer asymmetric and symmetric network and application acceleration along with caching, compression, and de-duplication for superior user experience.

Users connecting through BIG-IP Edge Gateway will receive their applications fast no matter where they are with a multi-gigabit per second SSL encryption throughput with HTTP and HTTPS at BIG-IP LTM speeds. Client-side services enable users to access corporate network and applications dynamically when mobile with the smart connection access intelligence system. Smart connection access, which is bundled with BIG-IP Edge Gateway, gives roaming users instant secure access by letting them know when they are not connected to the corporate domain. Smart connection access also provides application acceleration through traffic shaping for dynamic, adaptable compression. With client-side traffic shaping, administrators can give priority to particular protocols, like Server Message Block (SMB), ensuring both file transfers and VoIP traffic can get through.

With the integrated iSessions enabled by BIG-IP WAN Optimization Module, IT departments can connect with their cloud environment through an optimized, encrypted tunnel. Because maintaining control over data in the cloud is paramount, some organizations like to “house” their data at the corporate data center and have the cloud access it when requested. This process can certainly have performance implications but here, too, the secure, optimized iSessions tunnel provides the pipe from the data to the cloud. Symmetric, adaptive compression enables the tunnel to use the best compression ratio for the bandwidth available and adjusts the data stream to better use bandwidth, CPU, and compression rates. The branch office also benefits from the acceleration services. Whether for back-up scenarios or just keeping information up to date, symmetric data de-duplication only updates the changes to the data (rather than transferring the entire file), thus saving bandwidth. There is also support for CIFs and MAPI acceleration, and hardware-accelerated (SSL and compression) and L7 rate shaping, including QoS mode.

Managing the cloud has always been a challenge for IT departments. A central control point of access for both web access management and SSO makes policy-based access control over resources for context-aware networking quick to deploy and easy to manage. BIG-IP Edge Gateway policies can be imported and exported, web applications are secure and accelerated and offers modes for remote access, internal LAN control, and public and private wireless.

Conclusion

Cloud computing, while quickly evolving, can offer IT departments a powerful alternative for delivering applications. Cloud computing promises scalable, on-demand resources; flexible, self-serve deployment; lower TCO; faster time to market; and a multitude of service options that can host your entire infrastructure, be a part of your infrastructure, or simply serve a single application.

No matter how far into the cloud you are, or if it is a public, private, or hybrid cloud, F5 solutions can help make your cloud infrastructure or deployment more secure, reliable, and resilient. Secure remote access technology provides contextual, secure access to cloud-based applications; web application firewalls provide the means to centralize application security; network-side scripting offers an agile, immediate method of addressing security vulnerabilities on an on-demand basis, all helping to keep the cloud dynamic, fluid and secure.. IT administrators can isolate configuration and management for fine-grained control over access to cloud computing infrastructure and can isolate application traffic for improved security of application data that uses shared resources.

Securing the cloud with F5 includes a set of flexible, unified solutions—each with its own expertise to address your specific cloud application delivery needs.

F5 Networks, Inc.
401 Elliott Avenue West, Seattle, WA 98119
888-882-4447 www.f5.com

Americas
info@f5.com

Asia-Pacific
apacinfo@f5.com

Europe/Middle-East/Africa
emeainfo@f5.com

Japan
f5j-info@f5.com