CloudFucius Says: AAA Important to the Cloud

Peter Silva, 2010-13-04

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.

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.

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.

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.

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.

And one from Confucius himself: *I hear and I forget. I see and I remember. I do and I understand.*

ps

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