Dome9: Closing the (Cloud) Barn Door

Lori MacVittie, 2011-13-09

Ever hear the saying, "Closing the barn door after the horse has already left?" It's not a good thing, and Dome9 aims to make sure you close the (cloud) barn door before the horse bolts – not after.

An interesting* side-effect of deploying applications in public cloud computing environments is the fact that access to management functions is often accessible, necessarily, to any one. We rely instead on credentials and API keys to prevent unauthorized access and, given that we really can't do much more than that based on the external constraints placed upon us by the environment that, as we say, is that.

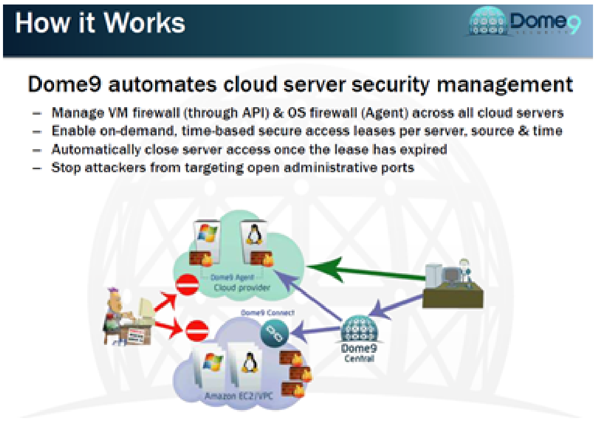
In a more controlled environment, such as our own data center, we'd take precautions to secure access to any administrative or management-enabling service – whether of the OS, the application, or the network. Using techniques such as firewall rules to IP-restricted management networks, we'd make sure to eliminate even the remote possibility that someone could hijack, compromise, or brute force their way in to what are certainly restricted operational functions. We would, to keep with the theme, close the barn door ***before*** the horse bolted, not after. Proactive, not reactive, measures is the foundation of successful security strategies.

In the cloud, however, we are more limited in our choices of how to secure these potential avenues of attack and given the complexity inherent in not only deploying but managing such choices in the cloud, we tend to close the barn door only ***after*** the horse has bolted; when a serious risk becomes reality and thus forces our hand. Deploying a firewall** in a cloud computing environment is of course an option, albeit a topologically challenging one at worst and an operationally frustrating one at best. Unless you can force consistent IPs across servers in a cloud computing environment, this will continue to be a challenge for any IP-coupled system – whether routing, switching, or security related.

So we deploy an application, perhaps complete with an administrative GUI – on a secured port, of course – in the cloud. But we don't restrict access to that port and thus leave the security of the application to whatever defenses are inherent to the application, most of which rarely include protection against brute force password attacks.

Dome9 aims to change that paradigm completely. Like its competitor, CloudPassage, it is a security management-as-a-service solution. Unlike its competition it employs a more flexible, time-based approach to managing access to applications and services hosted in cloud-computing environments.

IF YOUR INNER DEVELOPER SCREAMS …



How it Works

Dome9 automates cloud server security management

- Manage VM firewall (through API) & OS firewall (Agent) across all cloud servers
- Enable on-demand, time-based secure access leases per server, source & time
- Automatically close server access once the lease has expired
- Stop attackers from targeting open administrative ports

After a briefing with Dome9 on their impending solution, my inner developer was screaming. Loudly. With respect to security solutions, that generally means it's a good one. The primal developer-scream started when Dome9 explained the basics of how it worked, which in a nutshell is to employ a deny-all (negative) security approach to access and allow authorized access for a specific time interval before slamming the barn door shut again.

[Back in the day we used 14.4 baud modems to dial into a mainframe on the college campus to complete COBOL coding assignments. Having had more than one of those sessions interrupted by call waiting or someone in the house picking up the phone or static in the line, you can probably understand why I had the reaction I did. But I digress…]

Dome9 accomplishes this on-demand open and closing of ports either through the VM firewall (API) or via the OS' firewall (agent). The Dome9 agent supports “all major distributions of Linux and Windows.” Currently the list comprises CentOS 6.0 and Ubuntu, including CentOS/RHEL 5.x and 6.0, Debian 6, and Windows 2008 R2, 2008, 2003 R2 and 2003, both 32 & 64bit. Dome9 Connect (API) is available at launch to manage Amazon EC2/VPC and Cloud.com, with OpenStack and vCloud coming later this month. UDP and TCP are both supported, with the expected full range of ports capable of management via Dome9, e.g. all the usual suspects including RDP, SSH, FTP, and SQL.

The ability to manage across all cloud servers allows a consistent application of access security policies from a centralized location. The administrator can grant access to any managed port with the click of a button. With a couple extra clicks the admin can specify a time period (15 min, 1 hour, 6 hours) and a scope (individual IP or all IP addresses). Further customization of policies can be accomplished at the group level, e.g. “web servers”, “application servers”, “databases”. Essentially, administrators can create security zones and delegate access and security management across them.

Dome9 offers the ability to open/close ports on-demand in a self-service style interface, with additional capabilities to support third-party users via an invitation-style mechanism. Invitations are time-limited, i.e. they expire, and also include the basic time limitation on usage, once the invitation is activated.

The service also includes the ability to manage multiple administrators, including ability to limit administrations in their ability to access, manage, and add servers as well as AWS security groups.

Is it important to note that LEASES ALWAYS EXPIRE. Today, there is an option to terminate a lease before it would otherwise expire, but no way to extend one. That capability is one that may be included in future versions. It, in addition to the ability to specify more granular time limitations on leases, is necessary, I think, to not only ensure that leases aren’t simply always passed out for the maximum amount of time but to prevent the inevitable angst coming from application developers and administrators who may be bitten by an expiring lease. The always-expiring leases are an excellent way to ensure that ports are closed when not in use, eliminating completely one avenue of attack, but security impeding other IT functions has long been a source of contention across teams. There simply must be some way to ensure that security controls are adhered to without becoming overly burdensome, lest the benefits of mitigating the risk are lost to the negative consequences of lost productivity in other areas.

Available today, Dome9 is a monthly subscription service with pricing starting at $20 per server per month, based on the number of servers and admins. A free, 14-day full-featured trial is available. Also available is a free, personal use plan, which includes support for one server with one administrator. You can check it out at their web site.

THE POSSIBILITIES

The basic premise of Dome9 is fairly simple, and the solution elegant. It’s easy to use, not unpleasing to the eye, and at least in demonstrations does exactly what it’s supposed to do.

What catches my eye about solutions like Dome9 and CloudPassage is the possibilities of expanding beyond server virtualization and into the network. There are other components, after all, that perform access related functions that also suffer similar management impedance from IP-based configuration and management that would benefit from such systems. Those able to be managed via an API, infrastructure 2.0 capable devices, should be easily enough incorporated into such management-as-a-service systems as to provide the same security benefits as is afforded applications and servers.

More difficult, perhaps, would be the inclusion in operational automation solutions, which are increasingly accomplished via scripts and frameworks like Puppet and Chef. The ability to integrate an automated “open this port” action through Chef to allow boot time configuration via SSH would be a good first step and something vendors in this nascent market should keep in mind moving forward.

* I use “interesting” in the same sense as used in the Chinese curse, “May you live in interesting times”

** This begs the question what, if anything, secures access to the security service in a cloud environment

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