

PenTest
magazine

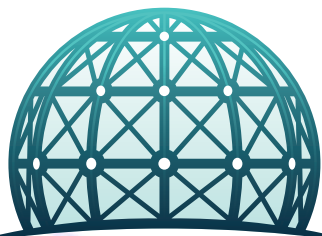
Free Article

6/2011

Securing Your Cloud

Radical Departures From Your Security

by Roy Feintuch



Dome9
SECURITY

Securing Your Cloud

Radical Departures From Your Security

You wouldn't leave your car unlocked in a public parking lot, so why are so many organizations leaving their servers unlocked in the cloud? Security is the number one concern for cloud adoption, but making your cloud impenetrable requires a radical departure from your typical security.

Security is the number one concern for cloud adoption, and a particular point of discussion among analysts and industry experts. Deployment of cloud applications is daunting when you consider the risks of having your applications, infrastructure, IP and private information in the cloud. Yet the cloud bears an abundance of benefits to today's enterprise – availability, agility, scalability, performance, and more. So, like every business decision, it's all about finding a balanced and acceptable risk, and it's finding that balance that most security professionals fail to do. That's because most people don't adequately understand the cloud, let alone know how best to secure it. Security in the cloud is as mysterious as the cloud itself. Who knows what all the vulnerabilities in the cloud might be? Its ambiguity presents significant risk. Yet, there are several things we do know, right off the bat: We must secure the cloud, including our applications and data used within it; and we must ensure that our security is simple and scalable – that our cloud security is as elastic as the infrastructure it protects.

You Can't Secure if You Can't Manage

First, when it comes to cloud security, elasticity and efficiency of management are as important as security

itself. The cloud is infinitely and immediately scalable. In the blink of an eye you can scale from one server to one hundred. In a world of automation (i.e., the cloud), if security is manual, it will not be sustainable. By themselves, most of today's cloud security services are, unfortunately, ill-equipped to efficiently scale, monitor and manage protection against vulnerabilities for cloud servers. This is critical when you consider how you make your cloud servers secure, because generally speaking security that's cumbersome and complex is security that goes unused. Thus, if security management is not automated, controls are discarded, mistakes are made, and servers and infrastructure are left vulnerable.

Traditional, on-premise security fails to cover the cloud. Nearly every facet of modern security was designed to defend from outside the perimeter, yet when you consider security in the cloud there is no perimeter to defend. In fact, the cloud is the *outside the perimeter* space that our traditional defenses were design to secure us from. Think about it: Gateway antivirus is at the corporate perimeter;

the corporate firewall is too. IDS/IPS is, again, at the gateway and protecting the perimeter-controlled infrastructure, etc., etc. Our modern security solutions

By themselves, most of today's cloud security services are, unfortunately, ill-equipped to efficiently scale, monitor and manage protection against vulnerabilities for cloud servers.

are designed to protect a legacy infrastructure – one where we have a physical corporate perimeter, with all of our infrastructure and applications safely secured therein. Conversely, however, the cloud is itself outside that perimeter, and one could argue whether the cloud itself has a perimeter and where it is – at the cloud, at the virtualization host, where? What's more, now too is our enterprise as we place more and more of our applications and data in it. Hence, as we've known for years due to mobility, the perimeter is eroding. With mobility our concern was how to protect our users who, if compromised, typically had a relatively low threat impact. Conversely, today, cloud is eroding the perimeter and what's left vulnerable is our core infrastructure and applications – a much more critical resource than a single endpoint, that has a tremendously high threat impact.

Security in the cloud is an imperative and requires an antithetical approach. If your applications, databases, and data are in the cloud, they're there for good reason – to drive your business. Since they are driving your business and are tremendously valuable, any potential vulnerability should be taken seriously and an abundance of caution and resource should be applied with respect to security. Securing your cloud resource, however, requires a reversal and perhaps even counterintuitive re-architecture of modern security theory. The cloud itself requires that security be applied not as a large, blanket overlay (the most similar approach to traditional security), but instead as a dynamic, object-oriented resource that allows you to automate application of security instantaneously across any new object that's added to (or removed from) your cloud. That's because the cloud itself is an object-oriented and tremendously elastic infrastructure. Security must be applied in conjunction with the architecture and utilization of the *thing* it's protecting. Thus, security in the cloud must be defined by each object (i.e., each server, application, and bit of data, and not a wide scope of infrastructure). This approach is reinforced when you consider that there are many clouds (e.g., AWS, Rackspace, Terremark, etc.), so there isn't any single area to build a moat-oriented approach around.

You Are Here; Now How Do you Get There

So where and how to start? Web application firewalls are growing tremendously in popularity, given that

Cloud server firewalls are the best place to stop attacks and prevent exploits of OS and application vulnerabilities. They're the first point of potential vulnerability at which any hacker would attempt to connect to and gain access to your application and data.

application hacking is now one of the largest attack vectors, but we'll save that for another article. But when it comes to securing the cloud, the first line of defense, and arguably the most effective, is the server firewall. Cloud server firewalls are the best place to stop attacks and prevent exploits of OS and application vulnerabilities. They're the first point of potential vulnerability at which any hacker would attempt to connect to and gain access to your application and data. That said, securing cloud servers can be very, very cumbersome and complex, and entail a laborious and manual process.

If you want to use your cloud, you need to be able to connect to and manage it. That means you need to punch (often many) holes in your cloud server firewall for administrative access, including SSH, Remote Desktop, and more. Opening and closing a firewall is typically done through the hosting or cloud service provider's management UI, and is done manually. On the face of it, this isn't a big deal. It sounds easy enough to do... you just need to do it time and time again with each new server you add to your cloud. If you have just a few servers this doesn't sound difficult, but if you have many it can be exhausting. Still, once you configure your server to have your administrative ports open, you're done, right? WRONG! What you've just done is expose your entire cloud server infrastructure to vulnerabilities and hackers.

It's worth repeating: You wouldn't leave your car unlocked in a public parking lot, so why would you leave your server ports open in the cloud? Remember, your cloud server is outside your corporate perimeter firewall. Before when your server was in your datacenter you could leave SSH open, but now your server is outside your perimeter, beyond the security you had in place. When you open SSH and Remote Desktop on your servers – so you can connect to and manage your infrastructure – you leave only a username and password on those open ports as a line of defense between hackers and your machines (note: some people use certificates instead of passwords, but that leads to other management problems such as certificate sharing or dealing with multiple or expired certificates). Anyone can SSH to your open port, and start punching in – most likely using a dictionary or brute force tool – usernames and passwords to gain access. This vulnerability must be managed.

So, to prevent unauthorized access and ensure your cloud infrastructure isn't vulnerable, you need to close all your administrative ports, and open them only when, for whom, for what, and for as long as you need access. This is, however, where that manual firewall management process fails you, because using the hosted or cloud service provider's UI to manually open ports to each and every cloud server you have every time someone needs to access and administer your servers is far too cumbersome and time-consuming. And remember, you have to close those ports as soon as access isn't needed, or you expose yourself to being vulnerable. You might try it for a while, but in very short order you're bound to forget to close a port, open the wrong one, or even give up and accept the risk that comes from leaving all SSH (or other administrative port) ports open by default, just to make your job easier. And the result, as we've outlined, is that anyone can leverage a brute force/dictionary tool to try to hack into any of your cloud infrastructure.

The SECRET Sauce to Cloud Security

The key to effective cloud security is like a two-sided coin – one side is security (of course) while the other is management. Most overlook the later, only to realize how critical management is when it's too late and they've given up on the first, security. Securing your cloud needs to offer protection that includes firewall security management as a first line of defense. Other technologies for applications and data services in your cloud follow on, but the first, most important act of vulnerability management is making sure your internal servers are internal, external services are exposed, and your server is less vulnerable to attack. Thus, the firewall and its effective management is the number one priority.

An effective cloud firewall and management solution must support multiple cloud platforms concurrently. That's because most organizations utilize more than one cloud. AWS, for example, is often used for development and applications, while Rackspace and Terremark are used for production environments. What's more, there are a variety of cloud servers and operating systems running in the cloud. Having separate management for each cloud and type of server defeats the purpose of easing management. For example, if you have cloud servers in both AWS EC2 and Rackspace, your cloud firewall management service should enable you to centrally manage secure access across your entire

multi-vendor, multi-OS cloud infrastructure with a persistent set of policies. In essence, your security management needs to operate at a higher plane than your infrastructure, or the security itself.

A cloud firewall management service makes security as flexible, or elastic, as the cloud. When you scale from one server to one hundred, your security must be applied in parallel, and your management and policy need to be updated and applied concurrently. The architecture of the firewall and security management service must be able to scale automatically with the infrastructure.

Perhaps most important to cloud security, management must be automated. It's impractical and unnecessary to manually manage cloud server firewalls, as described earlier on, and so a security management solution must automate application of policies, dynamically opening and closing cloud server firewalls on demand when, for whom, for what, and for as long as is needed.

Consider, for example, a developer who needs to SSH into an AWS EC2 Web server. Instead of directly SSHing into that Web server on an already-open port, the administrative port for SSH should be closed by default. The developer would first authenticate to the firewall management solution. If user is authenticated and authorized – that solution should dynamically open the port, just for that developer (e.g., access assigned to his IP address), for that protocol, port, and only for a specified time period. . At the end of the

period of time, the firewall management service should automatically terminate access and close the SSH port, to ensure the cloud server is secure. This automated provisioning remands control back to the users and does not inhibit workflow. More importantly, it ensures the cloud infrastructure has maximum, and efficient, security applied at all times.

Applying firewall security effectively in the cloud requires a flexible approach. Virtual or dedicated, Windows or Linux, public or private, Amazon or Rackspace... ensuring you have adequate coverage for the 31 flavors of cloud you're bound to use in your enterprise means you require a firewall management solution that provides sufficient coverage and flexibility. With some providers, such as AWS, management can be done through the virtualization layer and applied automatically to any new instance, managed through what's called Amazon Web Service Security Groups. If you're looking for both inbound and outbound security controls, however, you'll need an agent-based

Any cloud infrastructure investment should plan accordingly and invest in a security strategy that expects to span and support multiple types of clouds.

approach since even Amazon with its cutting-edge security management controls built into its virtualization layer does not offer outbound firewall management. An agent-based approach can manage both inbound and outbound traffic and span operating systems and cloud types. An agent-based approach is also critical since most hosting and cloud service providers do not offer security management at the virtualization layer, like Amazon. Thus, any cloud infrastructure investment should plan accordingly and invest in a security strategy that expects to span and support multiple types of clouds.

A Hot, Emerging Technology

Cloud firewall management, an emerging technology, is quickly growing in popularity among enterprise customers, as well as cloud hosting providers who are offering it as a value-added security service for subscribers. With first-of-its-kind multi-platform cloud server and security management that automates policy management, it enables administrators to:

- Keep ALL administrative ports on the server firewall closed without losing access and control
Most administrators forget that a vulnerability or hacker can use and exploit the same means of access to a cloud server that the administrator uses. It's critical that ports, especially those used for administration that are not related to the service or application delivery, be closed by default. To do this effectively, however, requires that while the port is closed by default, the administrator retains some means to connect to and manage that resource, without significant effort that would result in an adverse user experience or limitations on management.
- Dynamically open any port on demand – anytime, for anyone, and from anywhere
Security needs to be as flexible as the life of the everyday administrator requires. Cloud server administrators and developers often need to access their infrastructure on the road or at home, so it's critical that the firewall management service be flexible enough to provide the access securely, for anyone, at any time, and from anywhere. Leveraging a SaaS firewall management solution is one critical component that enables this kind of dynamic access, as does the ability to send and share access invitations with third parties, again – securely, so they too can support your cloud infrastructure.
- Send time- and location-based secure access invitations to third parties

You're likely not alone in managing your cloud and its applications and data. Colleagues, contactors, and other partners are often called upon to help manage your infrastructure, and that means they'll need to access your environment. Your firewall management solution should have a secure, yet simple workflow designed to make it easy for your support resources to get access. And that workflow should include automation, such as time-based invitations, location-based access restrictions (i.e., to ensure unauthorized users don't try to exploit access granted to a third party), and other advanced and automated capabilities to ensure you're productive but secure.

- Close ports automatically, so administrators don't have to manually reconfigure your firewall
One of the greatest supermarket inventions was the automated sliding door. It opens when you're coming, and it closes when you leave, automatically. Your firewall management service should do the same for your server access, only it must restrict who it provides access to, based on policy. Ensuring the door closes, automatically, is key because most people simply forget or don't bother to close the server access port (e.g., SSH) on their way out, resulting in cloud machines with unprotected administrative ports.
- Enable secure access of cloud servers without fear of getting locked out
The third leg of the cloud security stool – why many administrators do not close their administrative ports, is that they fear being locked out of their cloud servers. A cloud firewall management solution can ensure that you're never locked out, because its API or agent-based approach has a *man on the inside*, providing you with a deep yet secure hook into the server's firewall to remotely manage your configuration through the firewall management solution.

A key innovation in cloud server firewall management-as-a-service is the ability to provide secure access leasing – dynamically generated, time-based secure access to cloud servers, which enables customers to close all server administrative ports by default. Ports are opened via policy for any authorized user, but only for the time needed by the user. Once the time is up, the port is dynamically closed, ensuring that no vulnerabilities can penetrate through the firewall due to a port left open.

Another critical capability of cloud firewall management is the ability to segregate administration of machines for both policy management and access.

While some IT administrators may need access to a specific set of cloud servers, in many cases they do not need access (or should be prevented for security and compliance reasons) to others. A Web developer, for example, may require access to a Web server, while a DBA may need server access to the MySQL server. You should have controls, however, that enable you to provision security that prevents each from accessing the others' machines. That's where multi-administrator controls come in. With multi-administrator controls, you can segregate users to obtain or request access to a specific set of cloud servers, but not others. And you can set policy that restricts or allows access and/or the ability to manage firewall policy. For example, John, an IT Security Administrator, may be able to both access and manage firewall policy for both servers, but Michael, the DBA, can only get access (i.e., Michael cannot manage firewall policy). This granular level of control ensures you can delegate both administration and access controls (i.e., empower users to self-request/grant access) to the users themselves. What's more, you can do so knowing that their privileges are restricted by the cloud firewall management solution, and security is automated to a safe state (e.g., all ports are closed by default, and any open ports are closed after a specified time period) to ensure they don't make mistakes that might introduce vulnerabilities and compromise security.

With a cloud firewall service, the hosted cloud, VPS and dedicated servers are practically invisible to attackers. Additionally, there are no bandwidth or latency issues since remote clients are connected directly to the servers. This method eliminates all bandwidth, privacy, and latency problems. Since this approach uses the well-tested OS firewalls that are always enabled anyway, the impact on any machine is minimal.

Your Impenetrable Defense

A cloud firewall management service can be leveraged directly by an enterprise or delivered by a service provider. Service providers can bundle such capabilities directly into their offerings, or add it as a value-added security offering. Regardless of the approach, by deploying such a service organizations can dramatically improve their security for their cloud, applications, and the data. Alternatively, organizations can procure a cloud firewall management service directly from the provider. Either approach provides for provisioning

across cloud providers, since the solution operates at a higher level in the stack than either cloud infrastructure or the applied security.

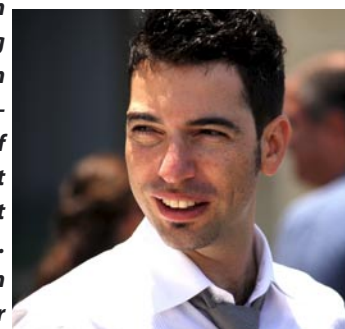
Making the cloud impenetrable is top of mind for every IT administrator wanting to migrate applications and other data to the cloud. As technologies continue to emerge to make this happen in a scalable, reliable, elastic, and flexible way, migration

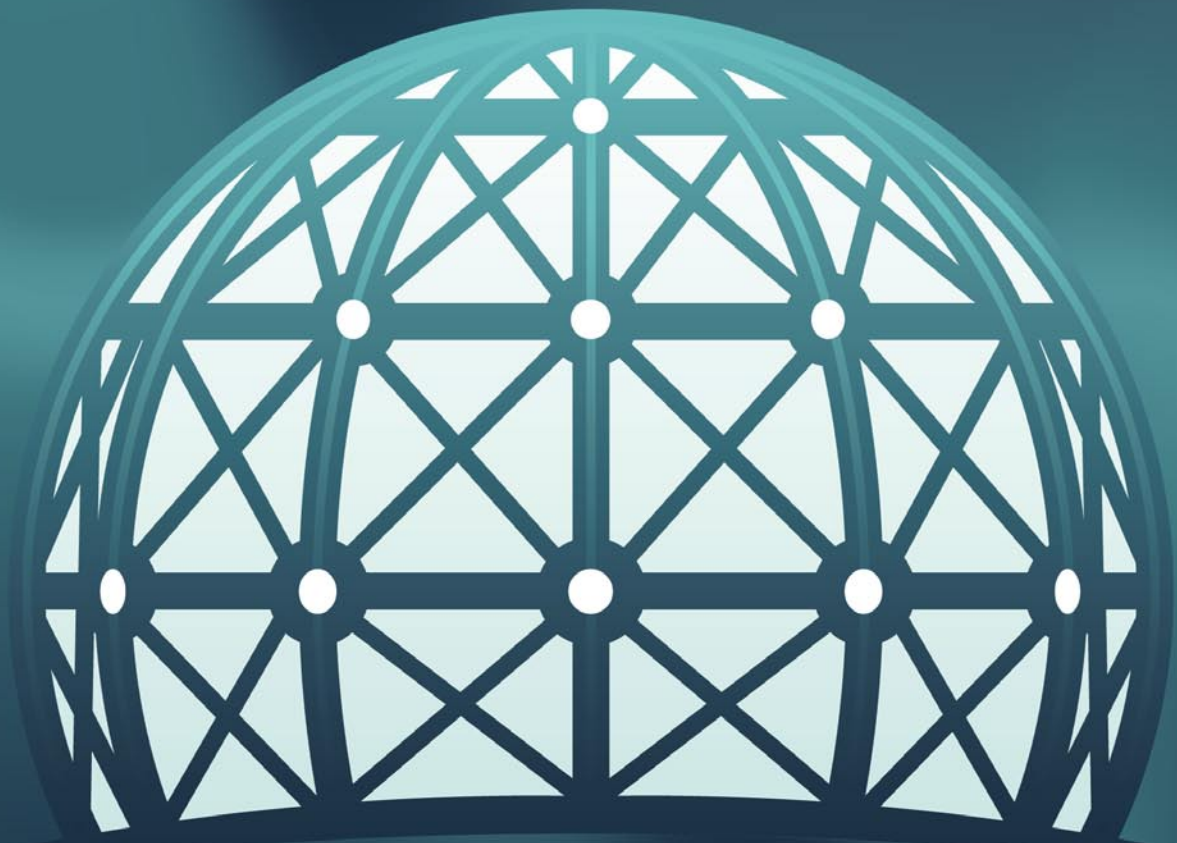
to the cloud will happen sooner rather than later. Why not manage vulnerabilities and provide the same protection that enterprises have grown to trust for on-premise networks, to secure information in the cloud? With a firewall management service helping to secure cloud firewalls, enterprises can be sure they've added another important layer of security for their information.

Making the cloud impenetrable is top of mind for every IT administrator wanting to migrate applications and other data to the cloud.

ROY FEINTUCH, CTO OF DOME9 SECURITY

Feintuch is a veteran technology leader having spent more than a decade in R&D at various Israeli high-tech startups. His area of expertise is the development of IT security management solutions and IP-video. Feintuch received his B.Sc. in Mathematics and Computer Science at BGU University in Israel.





Dome9

S E C U R I T Y

The world's first hosted and cloud server security management-as-a-service.

Centrally manage security policies for your cloud servers.
Any OS, any server, any time, from anywhere!

Visit Dome9.com to learn more.

Enter promo code **PTMAG2011** and sign up for **FREE!**