

Evaluating the Security of Multi-Tenant Cloud Architecture

Cloud computing exists at the forefront of technology modernization, widely accepted as the obvious path toward IT efficiency, yet security concerns continue to be a significant hurdle for mainstream cloud adoption. Despite those concerns, the compelling economic and operational benefits drive more businesses to the cloud every day. As businesses evaluate opportunities to capitalize on the benefits of cloud computing, it's important to understand how the cloud architecture either increases/decreases vulnerability to potential threats. Although many of these same security concepts can be applied to on-premises private cloud models, this article focuses on evaluating the cloud provider controlled security versus business user controlled security within a public, multi-tenant cloud environment.

This whitepaper highlights security problems that exist within a majority of cloud infrastructures as most people know them today, and introduces an alternative configuration to achieve a more secure cloud architecture. With the information provided, IT professionals will have a cursory understanding of the difference between 'flat' and 'ideal' cloud architectures to better evaluate the achievable level of security. Once businesses know that the secure three-tier architecture trusted in the physical IT world can be replicated within the cloud environment, they know what to demand from cloud providers and can rest assured that cloud adoption will not change their existing business, infrastructure, security, or Service Level Agreement (SLA) models in the ways previously feared.

Scope

When it comes to cloud computing discussions (especially on the topic of security), unintentionally 'boiling of the ocean' often occurs. To properly frame this discussion, scope must be defined. This article will discuss security concerns as they apply to Infrastructure as a Service (IaaS). Specifically it will tackle IaaS as it is used in public cloud or otherwise shared environments, but strong parallels can be drawn to dedicated or private clouds. When using the generic term "cloud providers", this article is referring to providers like Amazon, Rackspace, OpSource and a multitude of smaller cloud providers that deliver IaaS services. These providers are not all the same, but they share one or more of the characteristics discussed in this article. This is the only place where cloud providers are identified by name.

Current Landscape

In January 2010, Gartner predicted that, “a fifth of enterprises will hold no IT assets by 2012”. Even at the time it was a bold prediction. As of March 2011 it is mistaken. The majority of companies spent 2010 dabbling in on-premise virtualization or simply watching from the sidelines to see how the market unfolds. There are many factors inhibiting adoption. One of the most commonly cited is general concern with the security model of various cloud providers. Apart from security concerns, many executives have anxiety about the impacts of cloud computing on existing business models. Both concerns are real, but they are not universal. Options exist that provide peace of mind for enterprise customers.

Architecture Concerns

In March of 2011 Context Information Security LTD (Context), released a whitepaper titled Assessing Cloud Node Security (<http://bit.ly/ezZrXP>). It contains the following quote:

In a traditional hosted environment any attacker from the Internet must start at the outer firewall and work their way through... But in the cloud all the systems within the virtualised network reside next to each other.

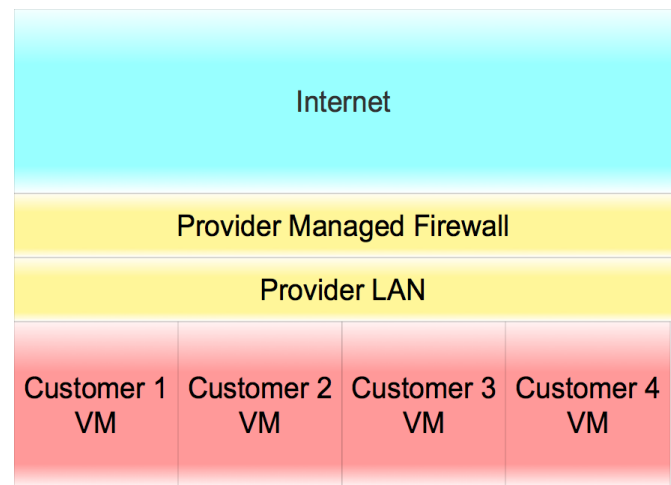


Figure 1 - Flat Cloud Architecture

According to Context, cloud providers are 'flat'. Figure 1 depicts a 'flat' cloud where the provider manages both the edge of the cloud and the network in which the virtual machines (VMs) reside. Essentially, this flat network provides no isolation between multiple tenants sharing the cloud. There are two major problems with this approach.

The first problem is that the provider-managed firewall is the security equivalent of a screen door. The provider must accommodate a huge variety of services for a multitude of customers. There is no way to control whether or not a customer will be building web servers, ftp servers or private web services that could span nearly any network port. Furthermore, Layer 7 (application-level) technologies are useless because the provider has almost no understanding of the underlying services exposed by the customers.

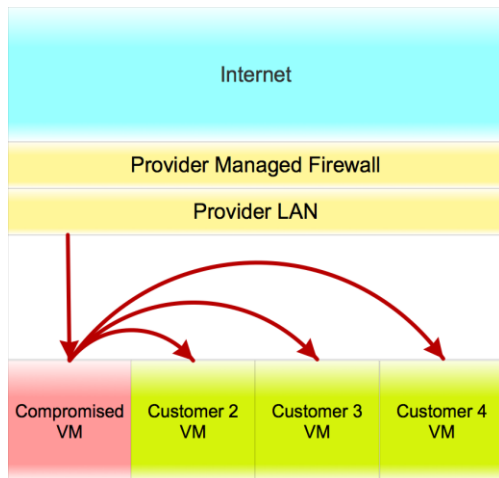


Figure 2 - Attack Vectors

Another major problem with this configuration involves the lack of isolation between VMs between customers (Figure 2). Since there is no isolation between clients, attacks are easily staged from within the same cloud by other tenants (intracloud attacks). A potential attacker may not have to know what he is looking for because the public nature of this network makes all traffic easily obtainable by others. Even more concerning is that if the attacker shares the cloud, an offensive can be launched directly at weaknesses in the customer's virtual machines. To defend against this, one must install a firewall directly on the virtual node itself. Unfortunately, this approach does not scale.

It should be noted here that there are other vectors of attack. There is always concern that attacks could be launched directly through the hypervisors that host the VMs. Furthermore the opportunity exists for attacks to be launched from the provider's side of the hypervisor. These concerns are legitimate and should be weighed when considering any cloud computing strategy. The threat is acknowledged here, but will not be discussed in detail.

Support for Custom Appliances

As previously mentioned, another looming security issue concerns the provider's inability to support customer provided images. The customers must choose from a limited list of pre-configured images that may or may not meet the security demands of the customer. Furthermore, the cloud consumer must trust the cloud provider to properly lock-down the virtual image so that it can be used securely. This references the previously stated concerns about isolation between multiple customers.

The only way to secure against this threat is to build a firewall on the device itself, but since this is a raw image, the software must be installed and configured each time a node is created. For environments where the end-users are deploying cloud infrastructure, the practice is difficult if not impossible to enforce without direct involvement from the security organization. It is also possible for some operating systems to be compromised even before these security measures can be implemented. This approach is both not scalable and undesirable.

Flat or Non-Existent User Hierarchies

The untenable nature of how cloud providers handle access and control of cloud computing environments can be even more challenging. Most, if not all, cloud providers extend their cloud services as a function of a single user account. In many cases there is no chain of custody or ability to empower administrative users to deploy their own resources with limited access and control. Giving another individual access to the cloud management console means giving total access to all user-managed systems.

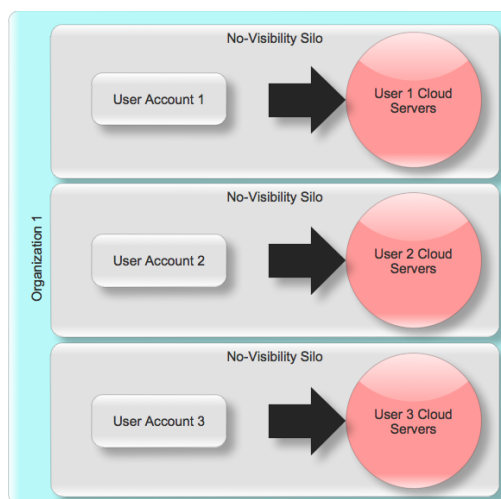


Figure 3 - Flat User Hierarchies

Most security administrators will bristle at the thought of losing audit-trail accountability through generic accounts. To empower multiple users, multiple accounts are absolutely required; however, there is no visibility or continuity between these silos in a flat user hierarchy. Even more vexing is the lack of accountability, visibility or control that can be managed from a higher vantage point. Today, almost all IT resources are provisioned through some form of internal supply chain. Services flow down this chain while usage flows back up. Most cloud computing models today threaten this eco-system.

Trust is Good, Control is Better

Trust is required to use the cloud—enterprises must trust their cloud provider with their business. This trust has been required since the advent of the co-location facility and continues onward through cloud computing. Trust is great if and when you can find it, but control provides peace of mind. If given the option to trust a service provider's firewall configuration or to retain complete control of the firewall product and configuration, security-minded organizations will choose the latter every time. Using the co-location facility example, trust was required, but a customer-managed firewall at the top of the rack was the rule. Why should cloud computing change this dynamic? Quite simply, it shouldn't. In fact, cloud computing should not change any of the following:

- The business model
- The security model
- The architecture model
- The service level agreement

It seems straight forward, but to date very few cloud providers see it that way. Either through technical inability, cost or unwillingness to accommodate multiple configurations, these cloud providers demand change to one or more of these aforementioned criteria. Regardless, these cloud models misrepresent core cloud consumers and cloud deliverables. These models consider the user to be a single individual and the deliverables to be virtual machines. The expectations of the enterprise customer deviate from this considerably. For the enterprise, the consumer of cloud is the organization and the deliverable is a dynamic workspace for creating complex infrastructure.

Meeting Enterprise Security Requirements

Since the beginning of distributed computing, 3-tier architecture has been the rule. This model should be familiar to nearly all of security experts and system architects. It creates a security model by creating independent computing layers designed to force intruders to penetrate multiple defense mechanisms before compromising the data. Since security is never absolute, these multiple layers create ample opportunity for security administrators to detect the attack and neutralize the threat before it becomes a calamity.

Not All Clouds are Flat

When providing IaaS to the enterprise, it might be surprising to hear that less security is sometimes better. Essentially, if the provider firewall services insufficiently support the enterprise use case, it calls to question whether or not there is any value at all in providing that service. This is another example of trust versus control. The enterprise customer wants to control the security of their cloud computing environment. When securing its border against the edge of the Internet, trust is not enough.

Sure, the enterprise customer may trust the provider, but the nature of threats from the Internet can never be completely understood. Furthermore, the customer wants to be free to act independently from their provider when it comes to securing the border. A better model is for the service provider to provide an unconfigured public facing LAN as a service with no inherent security. At first the concept of ‘no security’ seems counter intuitive, but if the cloud consumer can install a security device of their choosing and configuration, it goes much farther to meet the enterprise security requirement.

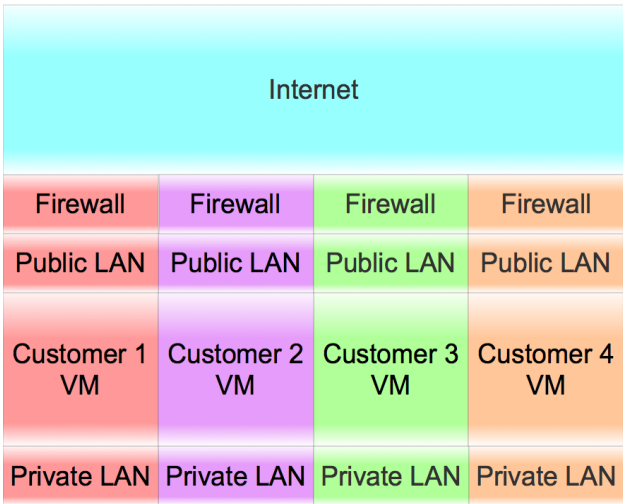


Figure 4 - Tiered Cloud Infrastructure

In this model, as shown in Figure 4, there are both public and private networks. It should be noted here that the public LAN is not shared among other cloud members. It is dedicated to that customer and defines a single broadcast domain with which no other customer can interfere. Of course the customer is free to create as many public servers as they wish, it is a best practice to secure the border with a single security device and control all access through this device. All other servers are created on one or more private networks that the enterprise controls. This is the way it has always been done and cloud computing should not change this simple practice.

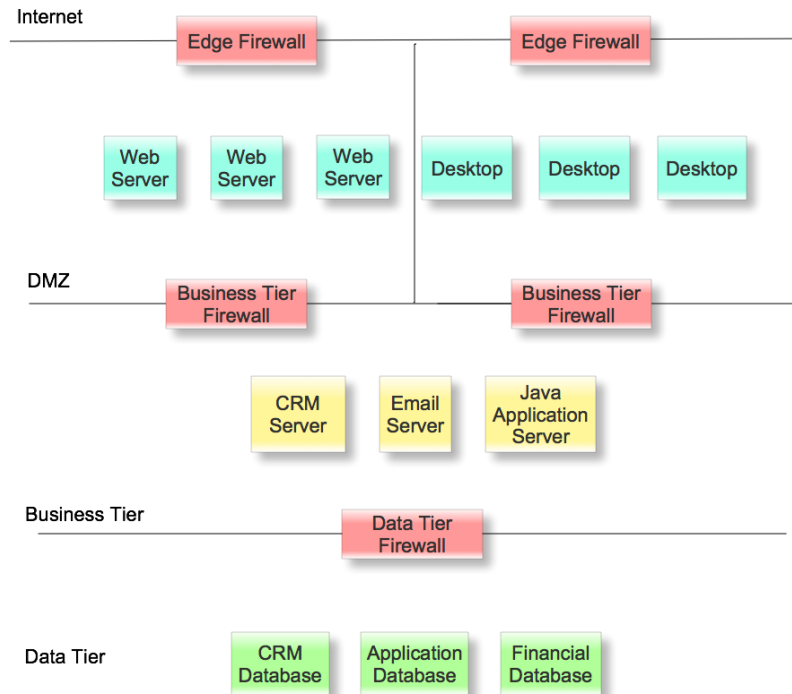


Figure 5 – n-Tier Architecture

When the cloud gives unfettered access to both public and private networks under the strict ownership of the customer, n-tier architecture is possible. Complex network topologies are now possible and the services can be exposed securely while other servers are strictly private in nature. Of course a cloud provider delivering this type of service will have provisions for accessing the consoles of the completely private servers. A typical setup in this type of environment will have separate, demilitarized segments for both web based applications and user desktops. Behind both of these network segments are more access control layers separating these tiers from the business.

The advantages of the tiered security model in the cloud are obvious, but there are additional benefits. Most importantly is the ability to have complete control over the edge security device. This means that any service can be controlled at whatever level the security model requires. For a service provider to manage a layer 7 firewall device in front of customer applications would be, at best, impractical. Creating layer 7 policies require intimate knowledge of the services that sit behind them. As a service provider managing a multi-tenant cloud, this level of knowledge is just not possible. Also, VPN tunnels and intelligent load-balancing can be implemented using the very same technologies used in the physical datacenter.

Custom Appliances

The ability to install and manage customer appliances defines another trait of the enterprise ready cloud. When an enterprise customer is able to bring their own appliance to the cloud, it can be pre-hardened to meet the security requirements of the customer. It makes even more sense to bring an appliance directly from the enterprise’s on-premises datacenter. Since the logical network can mimic the network topology of the enterprise datacenter, it becomes much simpler to use existing images as is. Once uploaded to the cloud, the user community can deploy the images as required by the business. Of course these images remain private to the enterprise customer that uploads the images. Because they are pre-built with roles, ACLs, and polices, direct intervention from the security team may not be required to implement a server.

Tiered User Hierarchy

As important as the architectural details are to the enterprise acceptance of cloud, the method in which users access the cloud can be even more challenging. As stated before, the typical cloud hierarchy is completely flat and featureless. In fact, the majority of cloud computing environments tie all infrastructure to a single user account. From an enterprise perspective this is simply not adequate.

Enterprises allocate computing resources through internal supply channels. Sometimes these supply channels are defined by high-level business relationships or compliance requirements, and other times those channels are a matrix across IT managed disciplines. Auditing and delegating control must be possible. Cloud computing user hierarchies support these relationships. Once complex business relationships are facilitated in the cloud, it becomes possible to align the cloud computing model with the business model.

Users Servers Networks ACLs Roles	Enterprise								
	Marketing Department		Security Department			IT Operations		Network Operations	
	Project 1	Project 2	IDS	Firewall	LDAP	Web Servers	Email	Routing	LANs

Figure 6 - Tiered User Hierarchy

Summary

Despite the security risks, compelling economic and operational benefits drive more businesses to the cloud every day. With an ever increasing pool of cloud vendors touting solution reliability and efficiency, businesses should look to cloud architecture as the 'telltale sign' of a more secure multi-tenant cloud offering. With technology advancing at lightning speed and sales-hype like blinding fog, understanding the security differences between 'flat' and 'ideal' multi-tenant cloud architectures provides a solid foundation for successful cloud computing strategies.

Business executives and IT professionals should be relieved to learn that cloud architecture today allows the virtual world to replicate the same three-tier architecture that secures our physical infrastructure today. In this 'ideal' cloud architecture, businesses no longer conform to cloud. Instead, the cloud adapts to accommodate existing business models, infrastructure models, security models, and Service Level Agreements (SLAs).

Armed with this critical insight, readers need not feel compelled to compromise business standards to gain cloud computing benefits. Know what's possible, know your options, and demand cloud vendors to deliver solutions that best suit the security and organizational requirements of your business. Knowledge is power, and cloud security can be the reward.