Cloud-based Firewall

Value to the ecosystem

Virtual firewall appliances play a critical role within the cloud infrastructure, mitigating security risks by implementing appropriate security controls for inter-virtual machine (VM) – or VM to physical and vice-versa – communication and providing the necessary isolation on an application, zone, domain or tenant basis.

Network-based security services were traditionally implemented by strategically placing physical "middle-boxes" across data centers and assuming the underlying network fabric would remain relatively static. However, new cloud architectures contain virtualized infrastructure, making the end-points (VMs) and the network fabric dynamic and subject to rapid change due to some triggering event, such as a failed compute/storage resource causing an automated response from the orchestration layer. This has created issues with the traditional network security approach, ranging from inflexible physical topologies, to firewalls becoming chokepoints, to loss of VM traffic visibility within the host, to name a few.

In a virtualized environment, network service functions such as firewalls can be rapidly deployed when and where needed – independent of physical locations or boundaries – and stitched together with other virtual or physical network services (e.g., load-balancers) though the network functions virtualization concept of "service chaining". This allows an agile, responsive and dynamic virtual environment to be created that scales based on events and configuration updates. It also ensures businesses can continue to monitor and enforce the same set of security controls and compliance requirements on the new virtual environment as they would with the traditional physical one.

Key Benefits:

1. Basic building block for any virtual network fabric in cloud infrastructure for securing applications – both externally (using VPNs) and internally (zone/app firewall).

2. Elasticity/scalability based on demand conditions and operator defined KPIs.

3. Self-healing of the firewall instances for high reliability and availability.

4. Complete visibility and security of the virtual environment

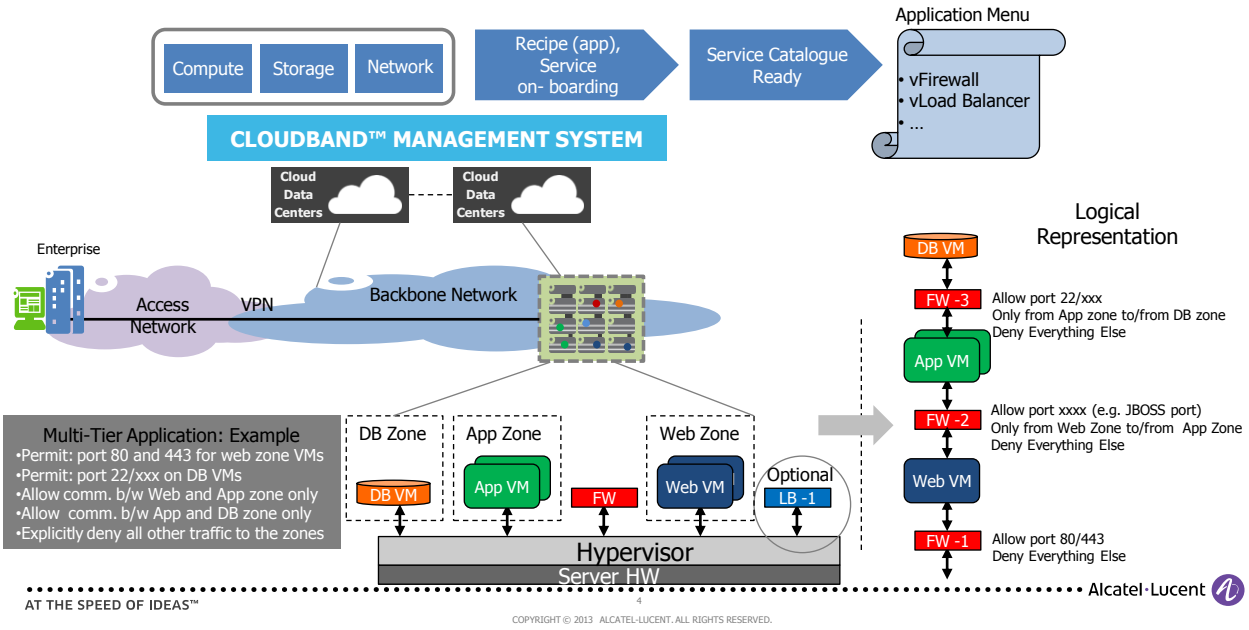
Solutions(s):

Virtual firewalls are one of the basic building blocks within cloud infrastructure, required for securing access to/from the virtual environment as well as the applications running within the environment. Deployed within the virtual environment network fabric , they enable access controls to be used between virtual machines and other points in the virtual and physical environment. They play a significant role at various security layers – e.g. tenant isolation and security in a shared, multi-tenant environment (e.g. using VPNs); between applications within a given tenant (Zone firewall); between VMs within a given application (application firewall) and so on. They are essential in creating multi-tier virtual network functions/applications within a host environment.

Virtual Firewall Integration with CloudBand:

Virtual firewall is deployed within CloudBand as an application appliance instance that can be used by other applications to create security controls between VMs within the application or across applications. There are two ways of using this virtual network function within CloudBand – it can be deployed as a standalone network function within a virtual network that is stitched together to form some higher level application/service or it can be deployed as a fully integrated network function within the framework of an application – e.g. a multi-tier web application. Independent of the deployment option, all applications are built by initially creating the necessary service templates called “recipes” using CloudBand’s cPaaS layer. The recipes essentially create the necessary service tiers for the application and manage the relationships between them, including all the scaling rules, healing rules, upgrades etc. The recipe is used to onboard the application onto CloudBand and make it available within the application/service catalogue for deployment.

The service provider/user can deploy the application by simply selecting the application from the application catalogue menu and providing any additional application-specific and/or operations-specific (business policy constraints) deployment parameters required. Upon deployment, the cPaaS manager monitors and controls the application activity as per the recipe definition/service template and the business policy constraints provided. CloudBand and cPaaS automatically provide all the underlying platform benefits to all deployed applications – such as elasticity, scalability, performance, reliability, availability, security and other common carrier-grade features – all without the need of deploying the applications on customized, proprietary hardware. Further, due to the cookie-cutter nature of the application template, deploying multiple instances requires little time or effort. The end result is the overall reduction in total cost of ownership for any deployed application – both in terms of Capex (since COTS hardware is employed) as well as Opex.



Firewall on CloudBand use case: simple multi-tier application deployment architecture

Firewall Cloudification Benefits: Operational Aspects

Attribute	Conventional	CloudBand
Appliance	Hardware appliance of software application on generic server (bare-metal) architected for peak capacity	Virtualized software appliance on cloud infrastructure architected for current capacity
Deployment	Site engineer investigates, deployment engineer installs, configures and provisions the system and monitors heath	Management and Orchestration system deploys new instance with standard configuration and automatically monitors health
Scale	Add new cards/blades/servers into the system hardware and perform re-configuration (re-architect with capacity planning)	Orchestration system adds additional instances of the appliance and automatically adds them to the load-balanced pool

Upgrade	Replace new upgraded blade with existing blade	Upgrade a new virtual instance and just switch traffic to it. Delete old instance
Operations	Hardware, OS, Application, Alarms	OS, Hypervisor, Application, Alarms
Multi-tenancy	Service partitioning of hardware based systems can be quite cumbersome – or deploy multiple, parallel hardware/software systems	Simply create a new service slice by deploying new application instance and service chain with other NFV components